A Reduction Theorem for Store Buffers

Ernie Cohen\(^1\), Norbert Schirmer\(^2\),\(^*\)

\(^1\) Microsoft Corp., Redmond, WA, USA
\(^2\) German Research Center for Artificial Intelligence (DFKI) Saarbrücken, Germany

ecohen@amazon.com, norbert.schirmer@web.de

Abstract. When verifying a concurrent program, it is usual to assume that memory is sequentially consistent. However, most modern multiprocessors depend on store buffering for efficiency, and provide native sequential consistency only at a substantial performance penalty. To regain sequential consistency, a programmer has to follow an appropriate programming discipline. However, naïve disciplines, such as protecting all shared accesses with locks, are not flexible enough for building high-performance multiprocessor software.

We present a new discipline for concurrent programming under TSO (total store order, with store buffer forwarding). It does not depend on concurrency primitives, such as locks. Instead, threads use ghost operations to acquire and release ownership of memory addresses. A thread can write to an address only if no other thread owns it, and can read from an address only if it owns it or it is shared and the thread has flushed its store buffer since it last wrote to an address it did not own. This discipline covers both coarse-grained concurrency (where data is protected by locks) as well as fine-grained concurrency (where atomic operations race to memory).

We formalize this discipline in Isabelle/HOL, and prove that if every execution of a program in a system without store buffers follows the discipline, then every execution of the program with store buffers is sequentially consistent. Thus, we can show sequential consistency under TSO by ordinary assertional reasoning about the program, without having to consider store buffers at all.

\(^*\) Work funded by the German Federal Ministry of Education and Research (BMBF) in the framework of the Verisoft XT project under grant 01 IS 07 008.
1 Introduction

When verifying a shared-memory concurrent program, it is usual to assume that each memory operation works directly on a shared memory state, a model sometimes called atomic memory. A memory implementation that provides this abstraction for programs that communicate only through shared memory is said to be sequentially consistent. Concurrent algorithms in the computing literature tacitly assume sequential consistency, as do most application programmers.

However, modern computing platforms typically do not guarantee sequential consistency for arbitrary programs, for two reasons. First, optimizing compilers are typically incorrect unless the program is appropriately annotated to indicate which program locations might be concurrently accessed by other threads; this issue is addressed only cursorily in this report. Second, modern processors buffer stores of retired instructions. To make such buffering transparent to single-processor programs, subsequent reads of the processor read from these buffers in preference to the cache. (Otherwise, a program could write a new value to an address but later read an older value.) However, in a multiprocessor system, processors do not snoop the store buffers of other processors, so a store is visible to the storing processor before it is visible to other processors. This can result in executions that are not sequentially consistent.
The simplest example illustrating such an inconsistency is the following program, consisting of two threads T0 and T1, where x and y are shared memory variables (initially 0) and r0 and r1 are registers:

\[
\begin{align*}
T0 & \quad T1 \\
 x &= 1; & y &= 1; \quad r0 &= y; & r1 &= x;
\end{align*}
\]

In a sequentially consistent execution, it is impossible for both r0 and r1 to be assigned 0. This is because the assignments to x and y must be executed in some order; if x (resp. y) is assigned first, then r1 (resp. r0) will be set to 1. However, in the presence of store buffers, the assignments to r0 and r1 might be performed while the writes to x and y are still in their respective store buffers, resulting in both r0 and r1 being assigned 0.

One way to cope with store buffers is make them an explicit part of the programming model. However, this is a substantial programming concession. First, because store buffers are FIFO, it ratchets up the complexity of program reasoning considerably; for example, the reachability problem for a finite set of concurrent finite-state programs over a finite set of finite-valued locations is in PSPACE without store buffers, but undecidable (even for two threads) with store buffers. Second, because writes from function calls might still be buffered when a function returns, making the store buffers explicit would break modular program reasoning.

In practice, the usual remedy for store buffering is adherence to a programming discipline that provides sequential consistency for a suitable class of architectures. In this report, we describe and prove the correctness of such a discipline suitable for the memory model provided by existing x86/x64 machines, where each write emerging from a store buffer hits a global cache visible to all processors. Because each processor sees the same global ordering of writes, this model is sometimes called total store order (TSO) [2].

The concurrency discipline most familiar to concurrent programs is one where each variable is protected by a lock, and a thread must hold the corresponding lock to access the variable. (It is possible to generalize this to allow shared locks, as well as variants such as split semaphores.) Such lock-based techniques are typically referred to as coarse-grained concurrency control, and suffice for most concurrent application programming. However, these techniques do not suffice for low-level system programming (e.g., the construction of OS kernels), for several reasons. First, in kernel programming efficiency is paramount, and atomic memory operations are more efficient for many problems. Second, lock-free concurrency control can sometimes guarantee stronger correctness (e.g., wait-free algorithms can provide bounds on execution time). Third, kernel programming requires taking into account the implicit concurrency of concurrent hardware activities (e.g., a hardware TLB racing to use page tables while the kernel is trying to access them), and hardware cannot be forced to follow a locking discipline.

A more refined concurrency control discipline, one that is much closer to expert practice, is to classify memory addresses as lock-protected or shared. Lock-protected addresses are used in the usual way, but shared addresses can be accessed using atomic operations provided by hardware (e.g., on x86 class architectures, most reads and writes are atomic). The main restriction on these accesses is that if a processor does a shared write and a

---

3 Before 2008, Intel [9] and AMD [1] both put forward a weaker memory model in which writes to different memory addresses may be seen in different orders on different processors, but respecting causal ordering. However, current implementations satisfy the stronger conditions described in this report and are also compliant with the latest revisions of the Intel specifications [10]. According to Owens et al. [15] AMD is also planning a similar adaptation of their manuals.

4 This atomicity isn’t guaranteed for certain memory types, or for operations that cross a cache line.
subsequent shared read (possibly from a different address), the processor must flush the 
store buffer somewhere in between. For example, in the example above, both \( x \) and \( y \) 
would be shared addresses, so each processor would have to flush its store buffer between 
its first and second operations.

However, even this discipline is not very satisfactory. First, we would need even more 
rules to allow locks to be created or destroyed, or to change memory between shared and 
protected, and so on. Second, there are many interesting concurrency control primitives, 
and many algorithms, that allow a thread to obtain exclusive ownership of a memory 
address; why should we treat locking as special?

In this report, we consider a much more general and powerful discipline that also guar-
antees sequential consistency. The basic rule for shared addresses is similar to the discipline 
above, but there are no locking primitives. Instead, we treat ownership as fundamental. 
The difference is that ownership is manipulated by nonblocking ghost updates, rather than 
an operation like locking that have runtime overhead. Informally the rules of the discipline 
are as follows:

– In any state, each memory address is either shared or unshared. Each memory address 
is also either owned by a unique thread or unowned. Every unowned address must be 
shared. Each address is also either read-only or read-write. Every read-only address is 
unowned.
– A thread can (autonomously) acquire ownership of an unowned address, or release 
ownership of a address that it owns. It can also change whether an address it owns is 
shared or not. Upon release of an address it can mark it as read-only.
– Each memory access is marked as volatile or non-volatile.
– A thread can perform a write if it is sound. It can perform a read if it is sound and 
clean.
– A non-volatile write is sound if the thread owns the address and the address is unshared.
– A non-volatile read is sound if the thread owns the address or the address is read-only.
– A volatile write is sound if no other thread owns the address and the address is not 
marked as read-only.
– A volatile read is sound if the address is shared or the thread owns it.
– A volatile read is clean if the store buffer has been flushed since the last volatile write. 
Moreover, every non-volatile read is clean.
– For interlocked operations (like compare and swap), which have the side effect of the 
store buffer getting flushed, the rules for volatile accesses apply.

Note first that these conditions are not thread-local, because some actions are allowed 
only when an address is unowned, marked read-only, or not marked read-only. A thread can 
ascertain such conditions only through system-wide invariants, respected by all threads, 
along with data it reads. By imposing suitable global invariants, various thread-local disci-
plines (such as one where addresses are protected by locks, conditional critical reasons, 
or monitors) can be derived as lemmas by ordinary program reasoning, without need for 
meta-theory.

Second, note that these rules can be checked in the context of a concurrent program 
without store buffers, by introducing ghost state to keep track of ownership and sharing 
and whether the thread has performed a volatile write since the last flush. Our main result 
is that if a program obeys the rules above, then the program is sequentially consistent when 
executed on a TSO machine.

Consider our first example program. If we choose to leave both \( x \) and \( y \) unowned (and 
hence shared), then all accesses must be volatile. This would force each thread to flush the 
store buffer between their first and second operations. In practice, on an x86/x64 machine,
this would be done by making the writes interlocked, which flushes store buffers as a side effect. Whichever thread flushes its store buffer second is guaranteed to see the write of the other thread, making the execution violating sequential consistency impossible.

However, couldn’t the first thread try to take ownership of \( x \) before writing it, so that its write could be non-volatile? The answer is that it could, but then the second thread would be unable to read \( x \) volatile (or take ownership of \( x \) and read it non-volatile), because we would be unable to prove that \( x \) is unowned at that point. In other words, a thread can take ownership of an address only if it is not racing to do so.

Ultimately, the races allowed by the discipline involve volatile access to a shared address, which brings us back to locks. A spinlock is typically implemented with an interlocked read-modify-write on an address (the interlocking providing the required flushing of the store buffer). If the locking succeeds, we can prove (using for example a ghost variable giving the ID of the thread taking the lock) that no other thread holds the lock, and can therefore safely take ownership of an address “protected” by the lock (using the global invariant that only the lock owner can own the protected address). Thus, our discipline subsumes the better-known disciplines governing coarse-grained concurrency control.

To summarize, our motivations for using ownership as our core notion of a practical programming discipline are the following:

1. the distinction between global (volatile) and local (non-volatile) accesses is a practical requirement to reduce the performance penalty due to necessary flushes and to allow important compiler optimizations (such as moving a local write ahead of a global read),
2. coarse-grained concurrency control like locking is nothing special but only a derived concept which is used for ownership transfer (any other concurrency control that guarantees exclusive access is also fine), and
3. we want that the conditions to check for the programming discipline can be discharged by ordinary state-based program reasoning on a sequentially consistent memory model (without having to talk about histories or complete executions).

Overview In Section 2 we introduce preliminaries of Isabelle/HOL, the theorem prover in which we mechanized our work. In Section 3 we informally describe the programming discipline and basic ideas of the formalization, which is detailed in Section 4 where we introduce the formal models and the reduction theorem. In Section 5 we give some details of important building blocks for the proof of the reduction theorem. To illustrate the connection between a programming language semantics and our reduction theorem, we instantiate our framework with a simple semantics for a parallel WHILE language in Section 6. Finally we conclude in Section 7.

2 Preliminaries

The formalization presented in this paper is mechanized and checked within the generic interactive theorem prover Isabelle [16]. Isabelle is called generic as it provides a framework to formalize various object logics declared via natural deduction style inference rules. The object logic that we employ for our formalization is the higher order logic of Isabelle/HOL [12].

This article is written using Isabelle’s document generation facilities, which guarantees a close correspondence between the presentation and the actual theory files. We distinguish formal entities typographically from other text. We use a sans serif font for types and constants (including functions and predicates), e.g., \texttt{map}, a slanted serif font for free variables, e.g., \texttt{x}, and a slanted sans serif font for bound variables, e.g., \texttt{x}. Small capitals
are used for data type constructors, e.g., Foo, and type variables have a leading tick, e.g., 'a. HOL keywords are typeset in type-writer font, e.g., \texttt{let}.

To group common premises and to support modular reasoning Isabelle provides locales \cite{4,5}. A locale provides a name for a context of fixed parameters and premises, together with an elaborate infrastructure to define new locales by inheriting and extending other locales, prove theorems within locales and interpret (instantiate) locales. In our formalization we employ this infrastructure to separate the memory system from the programming language semantics.

The logical and mathematical notions follow the standard notational conventions with a bias towards functional programming. We only present the more unconventional parts here. We prefer curried function application, e.g., \( f \ a \ b \) instead of \( f(a, b) \). In this setting the latter becomes a function application to one argument, which happens to be a pair.

Isabelle/HOL provides a library of standard types like Booleans, natural numbers, integers, total functions, pairs, lists, and sets. Moreover, there are packages to define new data types and records. Isabelle allows polymorphic types, e.g., 'a list is the list type with type variable 'a. In HOL all functions are total, e.g., \( \texttt{nat} \Rightarrow \texttt{nat} \) is a total function on natural numbers. A function update is \( f(y := v) = (\lambda x. \text{if } x = y \text{ then } v \text{ else } f \ x) \). To formalize partial functions the type 'a option is used. It is a data type with two constructors, one to inject values of the base type, e.g., \( \lfloor x \rfloor \), and the additional element \( \bot \). A base value can be projected with the function \texttt{the}, which is defined by the sole equation \( \texttt{the} \lfloor x \rfloor = x \). Since HOL is a total logic the term \texttt{the} \( \bot \) is still a well-defined yet un(der)specified value. Partial functions are usually represented by the type 'a ⇒ 'b option, abbreviated as 'a ⇒ 'b. They are commonly used as maps. We denote the domain of map \( m \) by \( \texttt{dom} m \). A map update is written as \( m(a \mapsto v) \). We can restrict the domain of a map \( m \) to a set \( A \) by \( m|_A \).

The syntax and the operations for lists are similar to functional programming languages like ML or Haskell. The empty list is \( [] \), with \( x \# xs \) the element \( x \) is 'consed' to the list \( xs \). With \( xs \odot ys \) list \( ys \) is appended to list \( xs \). With the term \texttt{map} \( f \ xs \) the function \( f \) is applied to all elements in \( xs \). The length of a list is \( |xs| \), the \( n \)-th element of a list can be selected with \( xs[n] \) and can be updated via \( xs[n := v] \). With \texttt{dropWhile} \( P \ xs \) the prefix for which all elements satisfy predicate \( P \) are dropped from list \( xs \).

Sets come along with the standard operations like union, i.e., \( A \cup B \), membership, i.e., \( x \in A \) and set inversion, i.e., – \( A \).

Tuples with more than two components are pairs nested to the right.

## 3 Programming discipline

For sequential code on a single processor the store buffer is invisible, since reads respect outstanding writes in the buffer. This argument can be extended to thread local memory in the context of a multiprocessor architecture. Memory typically becomes temporarily thread local by means of locking. The C-idiom to identify shared portions of the memory is the \texttt{volatile} tag on variables and type declarations. Thread local memory can be accessed non-volatilely, whereas accesses to shared memory are tagged as volatile. This prevents the compiler from applying certain optimizations to those accesses which could cause undesired behavior, e.g., to store intermediate values in registers instead of writing them to the memory.

The basic idea behind the programming discipline is, that before gathering new information about the shared state (via reading) the thread has to make its outstanding changes to the shared state visible to others (by flushing the store buffer). This allows to sequentialize the reads and writes to obtain a sequentially consistent execution of the global system. In this sequentialization a write to shared memory happens when the write
instruction exits the store buffer, and a read from the shared memory happens when all preceding writes have exited.

We distinguish thread local and shared memory by an ownership model. Ownership is maintained in ghost state and can be transferred as side effect of write operations and by a dedicated ghost operation. Every thread has a set of owned addresses. Owned addresses of different threads are disjoint. Moreover, there is a global set of shared addresses which can additionally be marked as read-only. Unowned addresses — addresses owned by no thread — can be accessed concurrently by all threads. They are a subset of the shared addresses. The read-only addresses are a subset of the unowned addresses (and thus of the shared addresses). We only allow a thread to write to owned addresses and unowned, read-write addresses. We only allow a thread to read from owned addresses and from shared addresses (even if they are owned by another thread).

All writes to shared memory have to be volatile. Reads from shared addresses also have to be volatile, except if the address is owned (i.e., single writer, multiple readers) or if the address is read-only. Moreover, non-volatile writes are restricted to owned, unshared memory. As long as a thread owns an address it is guaranteed that it is the only one writing to that address. Hence this thread can safely perform non-volatile reads to that address without missing any write. Similar it is safe for any thread to access read-only memory via non-volatile reads since there are no outstanding writes at all.

Recall that a volatile read is clean if it is guaranteed that there is no outstanding volatile write (to any address) in the store buffer. Moreover every non-volatile read is clean. To regain sequential consistency under the presence of store buffers every thread has to make sure that every read is clean, by flushing the store buffer when necessary. To check the flushing policy of a thread, we keep track of clean reads by means of ghost state. For every thread we maintain a dirty flag. It is reset as the store buffer gets flushed. Upon a volatile write the dirty flag is set. The dirty flag is considered to guarantee that a volatile read is clean.

Table 1a summarizes the access policy and Table 1b the associated flushing policy of the programming discipline. The key motivation is to improve performance by minimizing the number of store buffer flushes, while staying sequentially consistent. The need for flushing the store buffer decreases from interlocked accesses (where flushing is a side-effect) over volatile accesses to non-volatile accesses. From the viewpoint of access rights there is no difference between interlocked and volatile accesses. However, keep in mind that some interlocked operations can read from, modify and write to an address in a single atomic step of the underlying hardware and are typically used in lock-free algorithms or for the implementation of locks.

<table>
<thead>
<tr>
<th>(a) Access policy</th>
<th>(b) Flushing policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>shared (read-write)</td>
<td>shared (read-only)</td>
</tr>
<tr>
<td>unowned vR, vW</td>
<td>vR, R unreachable</td>
</tr>
<tr>
<td>owned by other vR</td>
<td>unreachable</td>
</tr>
</tbody>
</table>

(v)olatile, (R)ead, (W)rite
all reads have to be clean

flush (before)
interlocked as side effect
vR if not clean
R, vW, W never
4 Formalization

In this section we go into the details of our formalization. In our model, we distinguish the plain ‘memory system’ from the ‘programming language semantics’ which we both describe as a small-step transition relation. During a computation the programming language issues memory instructions (read / write) to the memory system, which itself returns the results in temporary registers. This clean interface allows us to parameterize the program semantics over the memory system. Our main theorem allows us to simulate a computation step in the semantics based on a memory system with store buffers by \( n \) steps in the semantics based on a sequentially consistent memory system. We refer to the former one as store buffer machine and to the latter one as virtual machine. The simulation theorem is independent of the programming language.

We continue with introducing the common parts of both machines. In Section 4.1 we describe the store buffer machine and in Section 4.2 we then describe the virtual machine. The main reduction theorem is presented in 4.3.

Addresses \( a \), values \( v \) and temporaries \( t \) are natural numbers. Ghost annotations for manipulating the ownership information are the following sets of addresses: the acquired addresses \( A \), the unshared (local) fraction \( L \) of the acquired addresses, the released addresses \( R \) and the writable fraction \( W \) of the released addresses (the remaining addresses are considered read-only). These ownership annotations are considered as side-effects on volatile writes and interlocked operations (in case a write is performed). Moreover, a special ghost instruction allows to transfer ownership. The possible status changes of an address due to these ownership transfer operations are depicted in Figure 1. Note that ownership of an address is not directly transferred between threads, but is first released by one thread and then can be acquired by another thread. A memory instruction is a datatype with the following constructors:

- **Read volatile** \( a \ t \) for reading from address \( a \) to temporary \( t \), where the Boolean \( \text{volatile} \) determines whether the access is volatile or not.
- **Write volatile** \( a \ sop A L R W \) to write the result of evaluating the store operation \( \text{sop} \) at address \( a \). A store operation is a pair \( (D,f) \), with the domain \( D \) and the function \( f \). The function \( f \) takes temporaries \( \theta \) as a parameter, which maps a temporary to a value. The subset of temporaries that is considered by function \( f \) is specified by the domain \( D \). We consider store operations as valid when they only depend on their domain:

\[
\text{valid-sop} \equiv \forall D \ f \ \theta. \ sop = (D,f) \land D \subseteq \text{dom} \ \theta \implies f \ \theta = f (\theta|_{D})
\]
Again the Boolean volatile specifies the kind of memory access.

- RMW a t sop cond ret A L R W, for atomic interlocked ‘read-modify-write’ instructions (flushing the store buffer). First the value at address a is loaded to temporary t, and then the condition cond on the temporaries is considered to decide whether a store operation is also executed. In case of a store the function ret, depending on both the old value at address a and the new value (according to store operation sop), specifies the final result stored in temporary t. With a trivial condition cond this instruction also covers interlocked reads and writes.
- FENCE, a memory fence that flushes the store buffer.
- GHOST A L R W for ownership transfer.

4.1 Store buffer machine

For the store buffer machine the configuration of a single thread is a tuple \((p, is, θ, sb)\) consisting of the program state \(p\), a memory instruction list \(is\), the map of temporaries \(θ\) and the store buffer \(sb\). A global configuration of the store buffer machine \((ts, m)\) consists of a list of thread configurations \(ts\) and the memory \(m\), which is a function from addresses to values.

We describe the computation of the global system by the non-deterministic transition relation \(\triangleright_{sb} (ts, m) \triangleright_{sb} (ts', m')\) defined in Figure 2.

\[
\begin{align*}
\text{if } i < |ts| & \quad ts[i] = (p, is, θ, sb) \quad θ ⊢ p \rightarrow_p (p', is') \\
& (ts, m) \triangleright_{sb} (ts[i := \{p', is' @ θ, θ, sb\}], m) \\
\text{if } i < |ts| & \quad ts[i] = (p, is, θ, sb) \quad (is, θ, sb, m) \triangleright_{m} (is', θ', sb', m') \\
& (ts, m) \triangleright_{sb} (ts[i := \{p, is', θ', sb'\}], m') \\
\text{if } i < |ts| & \quad ts[i] = (p, is, θ, sb) \quad (m, sb) \rightarrow_{sb} (m', sb') \\
& (ts, m) \triangleright_{sb} (ts[i := \{p, is, θ, sb'\}], m')
\end{align*}
\]

Fig. 2: Global transitions of store buffer machine

A transition selects a thread \(ts[i] = (p, is, θ, sb)\) and either the ‘program’ the ‘memory’ or the ‘store buffer’ makes a step defined by sub-relations.

The program step relation is a parameter to the global transition relation. A program step \(θ ⊢ p \rightarrow_p (p', is')\) takes the temporaries \(θ\) and the current program state \(p\) and makes a step by returning a new program state \(p'\) and an instruction list \(is'\) which is appended to the remaining instructions.

A memory step \((is, θ, sb, m) \rightarrow_{m} (is', θ', sb', m')\) of a machine with store buffer may only fill its store buffer with new writes.

In a store buffer step \((m, sb) \rightarrow_{sb} (m', sb')\) the store buffer may release outstanding writes to the memory.

The store buffer maintains the list of outstanding memory writes. Write instructions are appended to the end of the store buffer and emerge to memory from the front of the list. A read instructions is satisfied from the store buffer if possible. An entry in the store buffer is of the form \(\text{WRITE}_{sb} \text{ volatile a sop} \text{ v for an outstanding write (keeping the volatile flag), where operation sop evaluated to value v}.\)

As defined in Figure 3 a write updates the memory when it exits the store buffer.
\[(m, \text{Write}_{\text{ab}} \text{ volatile } v \text{ A L R W } \neq \text{ sb}) \rightarrow_{\text{sb}} (m(a := v), \text{ sb})\]

Fig. 3: Store buffer transition

\[
\begin{align*}
\nu &= (\text{case buffered-val sb a of } ⊥ \Rightarrow m a | [\nu'] \Rightarrow \nu') \\
(\text{Read volatile a t # is, } &\emptyset, \text{ sb, m}) \xrightarrow{\nu} (\text{is, } \emptyset(t \mapsto v), \text{ sb, m}) \\
\text{sb'} &= \text{sb} \oplus (\text{Write}_{\text{ab}} \text{ volatile a (D, f) (}\emptyset) \text{ A L R W}) \\
(\text{Write volatile a (D, f) A L R W } &\neq \text{ is, } \emptyset, \text{ sb, m}) \xrightarrow{\emptyset} (\text{is, } \emptyset, \text{ sb}', \text{ m}) \\
\neg \text{cond (}\emptyset(t \mapsto m a)) &\quad \emptyset' = \emptyset(t \mapsto m a) \\
(\text{RMW a t (D, f) cond ret A L R W } &\neq \text{ is, } [], \text{ m}) \xrightarrow{\emptyset} (\text{is, } \emptyset', [], \text{ m}) \\
\text{cond (}\emptyset(t \mapsto m a)) &\quad \emptyset' = \emptyset(t \mapsto \text{ ret (m a)} ((\emptyset(t \mapsto m a)))) \\
(\text{RMW a t (D, f) cond ret A L R W } &\neq \text{ is, } [], \text{ m}) \xrightarrow{\emptyset} (\text{is, } \emptyset', [], \text{ m'}) \\
(\text{Fence } &\neq \text{ is, } [], \text{ m}) \xrightarrow{\emptyset} (\text{is, } \emptyset, [], \text{ m}) \\
(\text{Ghost A L R W } &\neq \text{ is, } \emptyset, \text{ sb, m}) \xrightarrow{\emptyset} (\text{is, } \emptyset, \text{ sb, m})
\end{align*}
\]

Fig. 4: Memory transitions of store buffer machine

The memory transition are defined in Figure 4. With \textbf{buffered-val sb a} we obtain the value of the last write to address a which is still pending in the store buffer. In case no outstanding write is in the store buffer we read from the memory. Store operations have no immediate effect on the memory but are queued in the store buffer instead. Interlocked operations and the fence operation require an empty store buffer, which means that it has to be flushed before the action can take place. The read-modify-write instruction first adds the current value at address a to temporary t and then checks the store condition \textit{cond} on the temporaries. If it fails this read is the final result of the operation. Otherwise the store is performed. The resulting value of the temporary t is specified by the function \textit{ret} which considers both the old and new value as input. The fence and the ghost instruction are just skipped.

4.2 Virtual machine

The virtual machine is a sequentially consistent machine without store buffers, maintaining additional ghost state to check for the programming discipline. A thread configuration is a tuple \((p, \text{ is, } \emptyset, \text{ D, } \text{ O})\), with a dirty flag \text{ D} indicating whether there may be an outstanding volatile write in the store buffer and the set of owned addresses \textit{O}. The dirty flag \text{ D} is considered to specify if a read is clean: for all volatile reads the dirty flag must not be set. The global configuration of the virtual machine \((ts, m, S)\) maintains a Boolean map of shared addresses \textit{S} (indicating write permission). Addresses in the domain of mapping \textit{S} are considered shared and the set of read-only addresses is obtained from \textit{S} by: \text{read-only } \textit{S} \equiv \{a. \text{ S a } = [\text{False}]\}

According to the rules in Fig 5 a global transition of the virtual machine \((ts, m, S) \Rightarrow ts', m', S'\) is either a program or a memory step. The transition rules for its memory system are defined in Figure 6. In addition to the transition rules for the virtual machine we introduce the \textit{safety} judgment \(\textit{Os, i }\vdash (\text{is, } \emptyset, m, \text{ D, } \text{ O, } S) \\sqrt{\textit{y}}\) in Figure 7, where \textit{Os} is the list of ownership sets obtained from the thread list \textit{ts} and \textit{i} is the index of the current
\[
i < |ts| \quad ts[i] = (p, is, \emptyset, D, O) \quad \varnothing \vdash p \rightarrow_p (p', is')
\]

\[
(t, m, S) \Rightarrow (ts[i := (p', is' @ is', \emptyset, D, O)], m, S)
\]

\[
i < |ts| \quad ts[i] = (p, is, \emptyset, D, O) \quad \text{(is, } \emptyset, D, O, S) \xrightarrow{\varnothing \tau_m} (is', \emptyset', D', O', S')
\]

\[
(t, m, S) \Rightarrow (ts[i := (p, is', \emptyset', D', O')], m', S')
\]

Fig. 5: Global transitions of virtual machine

\[
(\text{Read volatile a } \# \text{ is, } \emptyset, x, m, ghst) \xrightarrow{\varnothing \tau_m} (is, \emptyset(t \mapsto m a), x, m, ghst)
\]

\[
(\text{Write False a } (D, f) \text{ A L R W } \# \text{ is, } \emptyset, x, m, ghst) \xrightarrow{\varnothing \tau_m} (is, \emptyset, x, m(a := f \emptyset), ghst)
\]

\[
ghst = (D, O, S) \quad ghst' = (\text{True, } O \cup A - R, S \oplus W R \ominus A L)
\]

\[
(\text{Write True a } (D, f) \text{ A L R W } \# \text{ is, } \emptyset, x, m, ghst) \xrightarrow{\varnothing \tau_m} (is, \emptyset, x, m(a := f \emptyset), ghst')
\]

\[
\neg \text{ cond } (\emptyset(t \mapsto m a)) \quad ghst = (D, O, S) \quad ghst' = (\text{False, } O, S)
\]

\[
(\text{RMW a t } (D, f) \text{ cond ret A L R W } \# \text{ is, } \emptyset, x, m, ghst) \xrightarrow{\varnothing \tau_m} (is, \emptyset', x, m', ghst')
\]

\[
\text{cond } (\emptyset(t \mapsto m a)) \quad \emptyset' = \emptyset(t \mapsto \text{ret } (m a) (f (\emptyset(t \mapsto m a)))) \quad ghst = (D, O, S) \quad ghst' = (\text{False, } O \cup A - R, S \oplus W R \ominus A L)
\]

\[
(\text{RMW a t } (D, f) \text{ cond ret A L R W } \# \text{ is, } \emptyset, x, m, ghst) \xrightarrow{\varnothing \tau_m} (is, \emptyset', x, m', ghst')
\]

\[
\text{(Fence } \# \text{ is, } \emptyset, x, m, ghst) \xrightarrow{\varnothing \tau_m} (is, \emptyset, x, m, ghst')
\]

\[
ghst = (D, O, S) \quad ghst' = (D, O \cup A - R, S \oplus W R \ominus A L)
\]

\[
(\text{Ghost A L R W } \# \text{ is, } \emptyset, x, m, ghst) \xrightarrow{\varnothing \tau_m} (is, \emptyset, x, m, ghst')
\]

Fig. 6: Memory transitions of the virtual machine
thread. Safety of all reachable states of the virtual machine ensures that the programming discipline is obeyed by the program and is our formal prerequisite for the simulation theorem. It is left as a proof obligation to be discharged by means of a proper program logic for sequentially consistent executions. In the following we elaborate on the rules of

\[
\begin{align*}
\forall a \in O \vee a \in \text{read-only} S \lor \text{volatile} \land a \in \text{dom } S. & \quad \text{volatile} \rightarrow \neg D \\
\text{OS}, i \vdash (\text{Write volatile} a t \# is, \emptyset, m, D, O, \emptyset) \lor \\
\text{OS}, i \vdash (\text{Write} \text{False} a (D, f) A L R W \# is, \emptyset, m, D, O, \emptyset) \lor \\
\forall j \in |OS|. i \neq j \rightarrow a \notin OS[j] \lor \exists \text{ read-only } S \\
\text{OS}, i \vdash (\text{Write True} a (D, f) A L R W \# is, \emptyset, m, D, O, \emptyset) \lor \\
\neg \text{cond} (\emptyset t \rightarrow \emptyset m a) \quad a \notin \text{ dom } S \lor O \\
\text{OS}, i \vdash (\text{RMW} a t (D, f) \text{ cond ret} A L R W \# is, \emptyset, m, D, O, \emptyset) \lor \\
\forall j \in |OS|. i \neq j \rightarrow a \notin OS[j] \lor \exists \text{ read-only } S \\
\text{OS}, i \vdash (\text{RMW} a t (D, f) \text{ cond ret} A L R W \# is, \emptyset, m, D, O, \emptyset) \lor \\
\text{OS}, i \vdash (\text{Fence} \# is, \emptyset, m, D, O, \emptyset) \lor \\
\text{OS}, i \vdash (\text{Ghost} A L R W \# is, \emptyset, m, D, O, \emptyset)
\end{align*}
\]

Fig. 7: Safe configurations of a virtual machine

Figures 6 and 7 in parallel. To read from an address it either has to be owned or read-only or it has to be volatile and shared. Moreover the read has to be clean. The memory content of address \(a\) is stored in temporary \(t\). Non-volatile writes are only allowed to owned and unshared addresses. The result is written directly into the memory. A volatile write is only allowed when no other thread owns the address and the address is not marked as read-only. Simultaneously with the volatile write we can transfer ownership as specified by the annotations \(A, L, R\) and \(W\). The acquired addresses \(A\) must not be owned by any other thread and stem from the shared addresses or are already owned. Reacquiring owned addresses can be used to change the shared-status via the set of local addresses \(L\) which have to be a subset of \(A\). The released addresses \(R\) have to be owned and distinct from the acquired addresses \(A\). After the write the new ownership set of the thread is obtained by adding the acquired addresses \(A\) and releasing the addressing \(R, O \cup A - R\). The released addresses \(R\) are augmented to the shared addresses \(S\) and the local addresses \(L\) are removed. We also take care about the write permissions in the shared state: the released addresses in set \(W\) as well as the acquired addresses are marked writable: \(S \oplus W R \ominus A L\). The auxiliary ternary operators to augment and subtract addresses from the sharing map are defined as follows:

\[
S \oplus W R \equiv \lambda a. \text{ if } a \in R \text{ then } [a \in W] \text{ else } S a \\
S \ominus A L \equiv \lambda a. \text{ if } a \in L \text{ then } \bot \text{ else } S a \text{ of } \bot \Rightarrow \bot \mid \text{writable} \Rightarrow [a \in A \lor \text{writable}]
\]

The read-modify-write instruction first adds the current value at address \(a\) to temporary \(t\) and then checks the store condition \(\text{cond}\) on the temporaries. If it fails this read is
the final result of the operation. Otherwise the store is performed. The resulting value of
the temporary $t$ is specified by the function $\text{ret}$ which considers both the old and new value
as input. As the read-modify-write instruction is an interlocked operation which flushes
the store buffer as a side effect the dirty flag $D$ is reset. The other effects on the ghost
state and the safety sideconditions are the same as for the volatile read and volatile write,
respectively.

The only effect of the fence instruction in the system without store buffer is to reset
the dirty flag.

The ghost instruction $\text{Ghost} A L R W$ allows to transfer ownership when no write is
involved i.e., when merely reading from memory. It has the same safety requirements as
the corresponding parts in the write instructions.

### 4.3 Reduction

The reduction theorem we aim at reduces a computation of a machine with store buffers
to a sequential consistent computation of the virtual machine. We formulate this as a
simulation theorem which states that a computation of the store buffer machine $(ts_{sb},
m')$ can be simulated by a computation of the virtual machine $(ts, m, S)$
$\Rightarrow^* (ts', m', S')$. The main theorem only considers computations that start in an initial
configuration where all store buffers are empty and end in a configuration where all store
buffers are empty again. A configuration of the store buffer machine is obtained from a
virtual configuration by removing all ghost components and assuming empty store buffers.

This coupling relation between the thread configurations is written as $ts_{sb} \sim ts$. Moreover,
the precondition $\text{initial}_v$ $ts S$ ensures that the ghost state of the initial configuration of
the virtual machine is properly initialized: the ownership sets of the threads are distinct,
an address marked as read-only (according to $S$) is unowned and every unowned address
is shared. Finally with $\text{safe-reach} (ts, m, S)$ we ensure conformance to the programming
discipline by assuming that all reachable configuration in the virtual machine are safe
(according to the rules in Figure 7).

**Theorem 1 (Reduction).**

$$(ts_{sb}, m) \Rightarrow^* (ts_{sb}', m') \land \text{empty-store-buffers} ts_{sb}' \land ts_{sb} \sim ts \land \text{initial}_v ts S \land
\text{safe-reach} (ts, m, S) \rightarrow
\exists ts' S'. (ts, m, S) \Rightarrow^* (ts', m', S') \land ts_{sb}' \sim ts'$$

This theorem captures our intuition that every result that can be obtained from a com-
putation of the store buffer machine can also be obtained by a sequentially consistent
computation. However, to prove it we need some generalizations that we sketch in the
following sections. First of all the theorem is not inductive as we do not consider arbitrary
intermediate configurations but only those where all store buffers are empty. For interme-
diate configurations the coupling relation becomes more involved. The major obstacle is
that a volatile read (from memory) can overtake non-volatile writes that are still in the
store-buffer and have not yet emerged to memory. Keep in mind that our programming
discipline only ensures that no volatile writes can be in the store buffer the moment we do
a volatile read, outstanding non-volatile writes are allowed. This reordering of operations
is reflected in the coupling relation for intermediate configurations as discussed in the
following section.

### 5 Building blocks of the proof

A corner stone of the proof is a proper coupling relation between an intermediate configu-
ration of a machine with store buffers and the virtual machine without store buffers. It
allows us to simulate every computation step of the store buffer machine by a sequence of steps (potentially empty) on the virtual machine. This transformation is essentially a sequentialization of the trace of the store buffer machine. When a thread of the store buffer machine executes a non-volatile operation, it only accesses memory which is not modified by any other thread (it is either owned or read-only). Although a non-volatile store is buffered, we can immediately execute it on the virtual machine, as there is no competing store of another thread. However, with volatile writes we have to be careful, since concurrent threads may also compete with some volatile write to the same address. At the moment the volatile write enters the store buffer we do not yet know when it will be issued to memory and how it is ordered relatively to other outstanding writes of other threads. We therefore have to suspend the write on the virtual machine from the moment it enters the store buffer to the moment it is issued to memory. For volatile reads our programming discipline guarantees that there is no volatile write in the store buffer by flushing the store buffer if necessary. So there are at most some outstanding non-volatile writes in the store buffer, which are already executed on the virtual machine, as described before. One simple coupling relation one may think of is to suspend the whole store buffer as not yet executed instructions of the virtual machine. However, consider the following scenario. A thread is reading from a volatile address. It can still have non-volatile writes in its store buffer. Hence the read would be suspended in the virtual machine, and other writes to the address (e.g. interlocked or volatile writes of another thread) could invalidate the value. Altogether this suggests the following refined coupling relation: the state of the virtual machine is obtained from the state of the store buffer machine, by executing each store buffer until we reach the first volatile write. The remaining store buffer entries are suspended as instructions. As we only execute non volatile writes the order in which we execute the store buffers should be irrelevant. This coupling relation allows a volatile read to be simulated immediately on the virtual machine as it happens on the store buffer machine.

From the viewpoint of the memory the virtual machine is ahead of the store buffer machine, as leading non-volatile writes already took effect on the memory of the virtual machine while they are still pending in the store buffer. However, if there is a volatile write in the store buffer the corresponding thread in the virtual machine is suspended until the write leaves the store buffer. So from the viewpoint of the already executed instructions the store buffer machine is ahead of the virtual machine. To keep track of this delay we introduce a variant of the store buffer machine below, which maintains the history of executed instructions in the store buffer (including reads and program steps). Moreover, the intermediate machine also maintains the ghost state of the virtual machine to support the coupling relation. We also introduce a refined version of the virtual machine below, which we try to motivate now. Essentially the programming discipline only allows races between volatile (or interlocked) operations. By race we mean two competing memory accesses of different threads of which at least one is a write. For example the discipline guarantees that a volatile read may not be invalidated by a non-volatile write of another thread. While proving the simulation theorem this manifests in the argument that a read of the store-buffer machine and the virtual machine sees the same value in both machines: the value seen by a read in the store buffer machine stays valid as long as it has not yet made its way out in the virtual machine. To rule out certain races from the execution traces we make use of the programming discipline, which is formalized in the safety of all reachable configurations of the virtual machine. Some races can be ruled out by continuing the computation of the virtual machine until we reach a safety violation. However, some cannot be ruled out by the future computation of the current trace, but can be invalidated by a safety violation of another trace that deviated from the current one at some point.
in the past. Consider two threads. Thread 1 attempts to do a volatile read from address
a which is currently owned (and not shared) by thread 2, which attempts to do a non-
volatile write on a with value 42 and then release the address. In this configuration there
is already a safety violation. Thread 1 is not allowed to perform a volatile read from an
address that is not shared. However, when Thread 2 has executed his update and has
released ownership (both are non-volatile operations) there is no safety violation anymore.
Unfortunately this is the state of the virtual machine when we consider the instructions of
Thread 2 to be in the store buffer. The store buffer machine and the virtual machine are
out of sync. Whereas in the virtual machine Thread 1 will already read 42 (all non-volatile
writes are already executed in the virtual machine), the non-volatile write may still be
pending in the store buffer of Thread 2 and hence Thread 1 reads the old value in the
store buffer machine. This kind of issues arise when a thread has released ownership in
the middle of non-volatile operations of the virtual machine, but the next volatile write
of this thread has not yet made its way out of the store buffer. When another thread
races for the released address in this situation there is always another scheduling of the
virtual machine where the release has not yet taken place and we get a safety violation.
To make these safety violations visible until the next volatile write we introduce another
ghost component that keeps track of the released addresses. It is augmented when an ghost
operation releases an address and is reset as the next volatile write is reached. Moreover,
we refine our rules for safety to take these released addresses into account. For example, a
write to an released address of another thread is forbidden. We refer to these refined model
as delayed releases (as no other thread can acquire the address as long as it is still in the
set of released addresses) and to our original model as free flowing releases (as the effect
of a release immediate takes place at the point of the ghost instruction). Note that this
only affects ownership transfer due to the GHOST instruction. Ownership transfer together
with volatile (or interlocked) writes happen simultaneously in both models.

Note that the refined rules for delayed releases are just an intermediate step in our
proof. They do not have to be considered for the final programming discipline. As sketched
above we can show in a separate theorem that a safety violation in a trace with respect
to delayed releases implies a safety violation of a (potentially other) trace with respect
to free flowing releases. Both notions of safety collas in all configurations where there
are no released addresses, like the initial state. So if all reachable configurations are safe
with respect to free flowing releases they are also safe with respect to delayed releases.
This allows us to use the stricter policy of delayed releases for the simulation proof. Before
continuing with the coupling relation, we introduce the refined intermediate models for
delayed releases and store buffers with history information.

5.1 Intermediate models

We begin with the virtual machine with delayed releases, for which the memory transitions
\((is, \varnothing, m, D, O, R, S) \xrightarrow{\text{gu}} (is', \varnothing', m', D', O', R', S')\) are defined Figure 8. The additional
ghost component \(R\) is a mapping from addresses to a Boolean flag. If an address is in the
domain of \(R\) it was released. The boolean flag is considered to figure out if the released
address was previously shared or not. In case the flag is True it was shared otherwise not.
This subtle distinction is necessary to properly handle volatile reads. A volatile read from
an address owned by another thread is fine as long as it is marked as shared. The released
addresses \(R\) are reset at every volatile write as well as interlocked operations and the fence
instruction. They are augmented at the ghost instruction taking the sharing information
into account:

\[
\text{aug} \ (\text{dom} \ S) \ R \ R' =
\]
\[(\text{READ volatile a } t \# \text{ is}, \varnothing, m, \text{ghost}) \overset{\text{dom}}{\Rightarrow} (\text{is}, \varnothing(t \mapsto m a), m, \text{ghost})\]

\[(\text{WRITE False a (D, f) A L R W } \# \text{ is}, \varnothing, m, \text{ghost}) \overset{\text{dom}}{\Rightarrow} (\text{is}, \varnothing, m(a := f \varnothing), \text{ghost})\]

\[\text{ghost} = (D, O, R, S) \quad \text{ghost}') = (\text{True, } O \cup A - R, \text{empty, } S \oplus_w R \oplus_A L)\]

\[(\text{RMW a t (D, f) cond ret A L R W } \# \text{ is}, \varnothing, m, \text{ghost}) \overset{\text{dom}}{\Rightarrow} (\text{is}, \varnothing', m', \text{ghost}')\]

\[\text{cond} (\varnothing(t \mapsto m a)) \quad \varnothing' = \varnothing(t \mapsto (m a) (f (\varnothing(t \mapsto m a)))) \quad m' = m(a := f (\varnothing(t \mapsto m a)))\]

\[\text{ghost} = (D, O, R, S) \quad \text{ghost}' = (\text{False, } O \cup A - R, \text{empty, } S \oplus_w R \oplus_A L)\]

\[(\text{Fence # is}, \varnothing, m, D, O, R, S) \overset{\text{dom}}{\Rightarrow} (\text{is}, \varnothing, m, \text{False, } O, \text{empty, } S)\]

\[\text{ghost} = (D, O, R, S) \quad \text{ghost}' = (D, O \cup A - R, \text{aug (dom S)} R \text{R, } S \oplus_w R \oplus_A L)\]

Fig. 8: Memory transitions of the virtual machine with delayed releases

\[(\lambda a. \text{if } a \in R \text{ then case } R \ a \to \bot \Rightarrow [a \in \text{dom } S] \mid [s] \Rightarrow [s \wedge a \in \text{dom } S])\]

else \( R \ a)\]

If an address is freshly released \((a \in R \text{ and } R \ a = \bot)\) the flag is set according to \(\text{dom S}\). Otherwise the flag becomes \([\text{False}]\) in case the released address is currently unshared. Note that with this definition \(R \ a = [\text{False}]\) stays stable upon every new release and we do not lose information about a release of an unshared address.

The global transition \((ts, m, s) \overset{\text{dom}}{\Rightarrow} (ts', m', s')\) are analogous to the rules in Figure 5 replacing the memory transitions with the refined version for delayed releases.

The safety judgment for delayed releases \(\text{O}_s, \text{R}_s, i, j \to (is, \varnothing, m, D, O, S) \) is defined in Figure 9. Note the additional component \(\text{R}_s\) which is the list of release maps of all threads. The rules are strict extensions of the rules in Figure 7: writing or acquiring an address \(a\) is only allowed if the address is not in the release set of another thread \((a \notin \text{dom } \text{R}_s[i,j])\); reading from an address is only allowed if it is not released by another thread while it was unshared \((\text{R}_s[j], a \neq [\text{False}]\).

For the store buffer machine with history information we not only put writes into the store buffer but also record reads, program steps and ghost operations. This allows us to restore the necessary computation history of the store buffer machine and relate it to the virtual machine which may fall behind the store buffer machine during execution. Altogether an entry in the store buffer is either a

- \(\text{READ}^\text{sb} \ \text{volatile a } t \ v\), recording a corresponding read from address \(a\) which loaded the value \(v\) to temporary \(t\), or \(a\)
- \(\text{WRITE}^\text{sb} \ \text{volatile a sop } v\) for an outstanding write, where operation \(\text{sop}\) evaluated to value \(v\), or of the form
- \(\text{PROC}^\text{sb} p p' \text{is}'\), recording a program transition from \(p\) to \(p'\) which issued instructions \(\text{is}'\), or of the form
- \(\text{GHOST}^\text{sb} A L R W\), recording a corresponding ghost operation.

As defined in Figure 10 a write updates the memory when it exits the store buffer, all other store buffer entries may only have an effect on the ghost state. The effect on the ownership
Fig. 9: Safe configurations of a virtual machine (delayed-releases)

\( \neg \text{volatile} \rightarrow (\forall j < |O_s|, i \neq j \rightarrow a \notin \text{dom } R_{s[j]} ) \)
\( \text{volatile} \rightarrow \neg D \)

\( a \in O \lor a \in \text{read-only } S \lor \text{volatile } \land a \in \text{dom } S \quad \forall j < |O_s|, i \neq j \rightarrow R_{s[j]} a \neq |\text{False}| \)

\( \neg \text{volatile} \rightarrow (\forall j < |O_s|, i \neq j \rightarrow a \notin \text{dom } R_{s[j]} ) \)

\( \text{volatile} \rightarrow \neg D \)

\( (m, \text{Write}_{ab} \text{False} a \text{ sop } v A L R W \# sb, O, R, S) \rightarrow_{ab} (m(a := v), sb, O, R, S) \)

\( \text{O'} = O \cup A - R \quad S' = S \oplus_W R \ominus_A L \)

\( (m, \text{Write}_{ab} \text{True} a \text{ sop } v A L R W \# sb, O, R, S) \rightarrow_{ab} (m(a := v), sb, O', \text{empty}, S') \)

\( (m, \text{Read}_{ab} \text{volatile } a v \# sb, O, R, S) \rightarrow_{ab} (m, sb, O, R, S) \)

\( (m, \text{Prog}_{ab} \text{ p p' is } \# sb, O, R, S) \rightarrow_{ab} (m, sb, O, R, S) \)

\( \text{O'} = O \cup A - R \quad R' = \text{aug } (\text{dom } S) R R \quad S' = S \oplus_W R \ominus_A L \)

\( (m, \text{Ghost}_{ab} A L R W \# sb, O, R, S) \rightarrow_{ab} (m, sb, O', R', S') \)

Fig. 10: Store buffer transitions with history
information is analogous to the corresponding operations in the virtual machine. The memory transitions defined in Figure 11 are straightforward extensions of the store buffer transitions of Figure 11 augmented with ghost state and recording history information in the store buffer. Note how we deal with the ghost state. Only the dirty flag is updated when the instruction enters the store buffer, the ownership transfer takes effect when the instruction leaves the store buffer. The global transitions \((ts_{sbh}, m, S) \xrightarrow{ab} (ts_{sbh}', m', S')\)

\[
v = \text{(case buffered-val sb a of } \bot \Rightarrow m a \mid [v'] \Rightarrow v') \quad sb' = sb @ [\text{Read}_{ab} \text{ volatile a t v}]
\]

\[
(\text{Read} \text{ volatile a t # is}, \vartheta, sb, m, ghst) \xrightarrow{ab_m} (is, \vartheta(t \mapsto v), sb', m, ghst)
\]

\[
sb' = sb @ [\text{Write}_{ab} \text{ False a (D, f) (f } \vartheta) \text{ A L R W}]
\]

\[
(\text{Write} \text{ False a (D, f) A L R W # is}, \vartheta, sb, m, ghst) \xrightarrow{ab_m} (is, \vartheta, sb', m, ghst)
\]

\[
glhst = (D, O, R, S) \quad ghst' = (\text{True}, O, \emptyset, S)
\]

\[
(\text{Write} \text{ True a (D, f) A L R W # is}, \vartheta, sb, m, ghst) \xrightarrow{ab_m} (is, \vartheta, sb', m, ghst')
\]

\[
\neg \text{ cond } (\vartheta(t \mapsto m a)) \quad ghst = (D, O, R, S) \quad ghst' = (\text{False}, O, \emptyset, S)
\]

\[
(\text{RMW} \text{ a t (D, f) cond ret A L R W # is}, \vartheta, \emptyset, m, ghst) \xrightarrow{ab_m} (is, \vartheta(t \mapsto m a), \emptyset, m, ghst')
\]

\[
\text{cond } (\vartheta(t \mapsto m a)) \quad \vartheta' = \vartheta(t \mapsto \text{ret (m a) (f (} \vartheta(t \mapsto m a)\text{)))) \quad m' = m(a := f (} \vartheta(t \mapsto m a)\text{)))}
\]

\[
glhst = (D, O, R, S) \quad ghst' = (\text{False}, O \cup A \rightarrow R, \emptyset, S \oplus W R \times A L)
\]

\[
(\text{Fence} \# is, \vartheta, \emptyset, m, D, O, R, S) \xrightarrow{ab_m} (is, \vartheta, \emptyset, m, \text{False}, O, \emptyset, S)
\]

\[
(\text{Ghost} \ A L R W \# is, \vartheta, sb, m, G) \xrightarrow{ab_m} (is, \vartheta, sb @ [\text{Ghost}_{ab} \ A L R W, m, G])
\]

Fig. 11: Memory transitions of store buffer machine with history

are analogous to the rules in Figure 2 replacing the memory transitions and store buffer transistions accordingly.

5.2 Coupling relation

After this introduction of the immediate models we can proceed to the details of the coupling relation, which relates configurations of the store buffer machine with history and the virtual machine with delayed releases. Remember the basic idea of the coupling relation: the state of the virtual machine is obtained from the state of the store buffer machine, by executing each store buffer until we reach the first volatile write. The remaining store buffer entries are suspended as instructions. The instructions now also include the history entries for reads, program steps and ghost operations. The suspended reads are not yet visible in the temporaries of the virtual machine. Similar the ownership effects (and program steps) of the suspended operations are not yet visible in the virtual machine. The coupling relation between the store buffer machine and the virtual machine is illustrated in Figure 12. The threads issue instructions to the store buffers from the right and the instructions emerge from the store buffers to main memory from the left. The dotted line illustrates the state of the virtual machines memory. It is obtained from the memory of the store buffer machine by executing the purely non-volatile prefixes of the store buffers. The remaining entries of the store buffer are still (suspended) instructions in the virtual machine.

18
Consider the following configuration of a thread $t_{s_{bh}[j]}$ in the store buffer machine, where $i_k$ are the instructions and $s_k$ the store buffer entries. Let $s_v$ be the first volatile write in the store buffer. Keep in mind that new store buffer entries are appended to the end of the list and entries exit the store buffer and are issued to memory from the front of the list.

$$t_{s_{bh}[j]} = (p, [i_1, \ldots, i_n], \vartheta, [s_1, \ldots, s_v, s_{v+1}, \ldots, s_m], D, O, R)$$

The corresponding configuration $t_{[j]}$ in the virtual machine is obtained by suspending all store buffer entries beginning at $s_v$ to the front of the instructions. A store buffer READ$_{sb}$ / WRITE$_{sb}$ / GHOST$_{sb}$ is converted to a READ / WRITE / GHOST instruction. We take the freedom to make this coercion implicit in the example. The store buffer entries preceding $s_v$ have already made their way to memory, whereas the suspended read operations are not yet visible in the temporaries $\vartheta'$. Similar, the suspended updates to the ownership sets and dirty flag are not yet recorded in $O', R'$ and $D'$. 

$$t_{[j]} = (p, [s_v, s_{v+1}, \ldots, s_m, i_1, \ldots, i_n], \vartheta', D', O', R')$$

This example illustrates that the virtual machine falls behind the store buffer machine in our simulation, as store buffer instructions are suspended and reads (and ghost operations) are delayed and not yet visible in the temporaries (and the ghost state). This delay can also propagate to the level of the programming language, which communicates with the memory system by reading the temporaries and issuing new instructions. For example the control flow can depend on the temporaries, which store the result of branching conditions. It may happen that the store buffer machine already has evaluated the branching condition by referring to the values in the store buffer, whereas the virtual machine still has to wait. Formally this manifests in still undefined temporaries. Now consider that the program in the store buffer machine makes a step from $p$ to $(p', is')$, which results in a thread configuration where the program state has switched to $p'$, the instructions $is'$ are appended and the program step is recorded in the store buffer:

$$t_{s_{bh}[j]} = (p', [i_1, \ldots, i_n] @ is', \vartheta, [s_1, \ldots, s_v, \ldots, s_m, \text{ProG}_sb \ p \ p' \ is'] D, O, R)$$

The virtual machine however makes no step, since it still has to evaluate the suspended instructions before making the program step. The instructions $is'$ are not yet issued and the program state is still $p$. We also take these program steps into account in our final coupling relation $(t_{s_{bh}}, m_{sbh}, S_{sbh}) \sim (ts, m, S)$, defined in Figure 13. We denote the already simulated store buffer entries by $\text{execs}$ and the suspended ones by $\text{suspends}$. The function $\text{instrs}$ converts them back to instructions, which are a prefix of the instructions of the virtual
machine. We collect the additional instructions which were issued by program instructions but still recorded in the remainder of the store buffer with function \textit{prog-instrs}. These instructions have already made their way to the instructions of the store buffer machine but not yet on the virtual machine. This situation is formalized as \textit{insts suspends} @ \textit{is}$_{\text{sbh}}$ = \textit{is} @ \textit{prog-instrs suspends}, where \textit{is} are the instructions of the virtual machine. The program state of the virtual machine is either the same as in the store buffer machine or the first program state recorded in the suspended part of the store buffer. This state is selected by \textit{hd-prog}. The temporaries of the virtual machine are obtained by removing the suspended reads from \textit{θ}. The memory is obtained by executing all store buffers until the first volatile write is hit, excluding it. Thereby only non-volatile writes are executed, which are all thread local, and hence could be executed in any order with the same result on the memory. Function \textit{exec-all-until-volatile-write} executes them in order of appearance. Similarly the sharing map of the virtual machine is obtained by executing all store buffers until the first volatile write via the function \textit{share-all-until-volatile-write}. For the local ownership set \textit{O}_{\text{sbh}} the auxiliary function \textit{acquire} calculates the outstanding effect for the already simulated parts of the store buffer. Analogously \textit{release} calculates the effect for the released addresses \textit{R}_{\text{sbh}}.

\section{5.3 Simulation}

Theorem 2 is our core inductive simulation theorem. Provided that all reachable states of the virtual machine (with delayed releases) are safe, a step of the store buffer machine (with history) can be simulated by a (potentially empty) sequence of steps on the virtual machine, maintaining the coupling relation and an invariant on the configurations of the store buffer machine.

\textbf{Theorem 2 (Simulation).}

\[
(t_{\text{sbh}}, m_{\text{sbh}}, S_{\text{sbh}}) \xrightarrow{\text{h}} (t_{\text{sbh}}', m_{\text{sbh}}', S_{\text{sbh}}') \land (t_{\text{sbh}}, m_{\text{sbh}}, S_{\text{sbh}}) \sim (ts, m, S) \land \text{safe-reach-delayed} \land \text{invariant } t_{\text{sbh}} S_{\text{sbh}} m_{\text{sbh}} \rightarrow \text{invariant } t_{\text{sbh}}' S_{\text{sbh}}' m_{\text{sbh}}' \land (\exists ts' S' m' (ts, m, S) \xrightarrow{\text{h}} (ts', m', S') \land (t_{\text{sbh}}', m_{\text{sbh}}', S_{\text{sbh}}') \sim (ts', m', S'))
\]

In the following we discuss the invariant \textit{ts}_{\text{sbh}} S_{\text{sbh}} m_{\text{sbh}}, where we commonly refer to a thread configuration \textit{ts}_{\text{sbh}}[i] = (p, \textit{is}, \textit{θ}, \textit{sh}, \textit{D}, \textit{O}, \textit{R}) for \( i < |ts_{\text{sbh}}| \). By outstanding references we refer to read and write operations in the store buffer. The invariant is a conjunction of several sub-invariants grouped by their content:

\[
invariant t_{\text{sbh}} S_{\text{sbh}} m_{\text{sbh}} \equiv \text{ownership-inv } S_{\text{sbh}} t_{\text{sbh}} \land \text{sharing-inv } S_{\text{sbh}} t_{\text{sbh}} \land
\]

Fig. 13: Coupling relation
Ownership. (i) For every thread all outstanding non-volatile references have to be owned or refer to read-only memory. (ii) Every outstanding volatile write is not owned by any other thread. (iii) Outstanding accesses to read-only memory are not owned. (iv) The ownership sets of every two different threads are distinct.

Sharing. (i) All outstanding non volatile writes are unshared. (ii) All unowned addresses are shared. (iii) No thread owns read-only memory. (iv) The ownership annotations of outstanding ghost and write operations are consistent (e.g., released addresses are owned at the point of release). (v) There is no outstanding write to read-only memory.

Temporaries. Temporaries are modeled as an unlimited store for temporary registers. We require certain distinctness and freshness properties for each thread. (i) The temporaries referred to by read instructions are distinct. (ii) The temporaries referred to by reads in the store buffer are distinct. (iii) Read and write temporaries are distinct. (iv) Read temporaries are fresh, i.e., are not in the domain of $\theta$.

Data dependency. Data dependency means that store operations may only depend on previous read operations. For every thread we have: (i) Every operation $(D, f)$ in a write instruction or a store buffer write is valid according to $\text{valid-sop} (D, f)$, i.e., function $f$ only depends on domain $D$. (ii) For every suffix of the instructions of the form WRITE volatile $a (D, f) A L R W \#$ is the domain $D$ is distinct from the temporaries referred to by future read instructions in is. (iii) The outstanding writes in the store buffer do not depend on the read temporaries still in the instruction list.

History. The history information of program steps and read operations we record in the store buffer have to be consistent with the trace. For every thread: (i) The value stored for a non volatile read is the same as the last write to the same address in the store buffer or the value in memory, in case there is no write in the buffer. (ii) All reads have to be clean. This results from our flushing policy. Note that the value recorded for a volatile read in the initial part of the store buffer (before the first volatile write), may become stale with respect to the memory. Remember that those parts of the store buffer are already executed in the virtual machine and thus cause no trouble. (iii) For every read the recorded value coincides with the corresponding value in the temporaries. (iv) For every WRITE$_{sb}$ volatile $a (D, f) v A L R W$ the recorded value $v$ coincides with $f \theta$, and domain $D$ is subset of $\text{dom } \theta$ and is distinct from the following read temporaries. Note that the consistency of the ownership annotations is already covered by the aforementioned invariants. (v) For every suffix in the store buffer of the form PROG$_{sb} p_1, p_2 \ is' \ # \ sb'$, either $p_1 = p$ in case there is no preceding program node in the buffer or it corresponds to the last program state recorded there. Moreover, the program transition $\theta (\text{read-temps } sb') \vdash p_1 \rightarrow p (p_2, is')$ is possible, i.e., it was possible to execute the program transition at that point. (vi) The program configuration $p$ coincides with the last program configuration recorded in the store buffer. (vii) As the instructions from a program step are at the one hand appended to the instruction list and on the other hand recorded in the store buffer, we have for every suffix $sb'$ of the store buffer: $\exists is'. \text{instrs } sb' @ is = is' @ \text{prog-instrs } sb'$, i.e., the remaining instructions is correspond to a suffix of the recorded instructions $\text{prog-instrs } sb'$.

Flushes. If the dirty flag is unset there are no outstanding volatile writes in the store buffer.
Program step. The program-transitions are still a parameter of our model. In order to make the proof work, we have to assume some of the invariants also for the program steps. We allow the program-transitions to employ further invariants on the configurations, these are modeled by the parameter valid. For example, in the instantiation later on the program keeps a counter for the temporaries, for each thread. We maintain distinctness of temporaries by restricting all temporaries occurring in the memory system to be below that counter, which is expressed by instantiating valid. Program steps, memory steps and store buffer steps have to maintain valid. Furthermore we assume the following properties of a program step: (i) The program step generates fresh, distinct read temporaries, that are neither in $\emptyset$ nor in the store buffer temporaries of the memory system. (ii) The generated memory instructions respect data dependencies, and are valid according to valid-sop.

Proof sketch. We do not go into details but rather first sketch the main arguments for simulation of a step in the store buffer machine by a potentially empty sequence of steps in the virtual machine, maintaining the coupling relation. Second we exemplarily focus on some cases to illustrate common arguments in the proof. The first case distinction in the proof is on the global transitions in Figure 2. (i) Program step: we make a case distinction whether there is an outstanding volatile write in the store buffer or not. If not the configuration of the virtual machine corresponds to the executed store buffer and we can make the same step. Otherwise the virtual machine makes no step as we have to wait until all volatile writes have exited the store buffer. (ii) Memory step: we do case distinction on the rules in Figure 11. For read, non volatile write and ghost instructions we do the same case distinction as for the program step. If there is no outstanding volatile write in the store buffer we can make the step, otherwise we have to wait. When a volatile write enters the store buffer it is suspended until it exists the store buffer. Hence we do no step in the virtual machine. The read-modify-write and the fence instruction can all be simulated immediately since the store buffer has to be empty. (iii) Store Buffer step: we do case distinction on the rules in Figure 10. When a read, a non volatile write, a ghost operation or a program history node exits the store buffer, the virtual machine does not have to do any step since these steps are already visible. When a volatile write exits the store buffer, we execute all the suspended operations (including reads, ghost operations and program steps) until the next suspended volatile write is hit. This is possible since all writes are non volatile and thus memory modifications are thread local.

In the following we exemplarily describe some cases in more detail to give an impression on the typical arguments in the proof. We start with a configuration $c_{sbh} = (ts_{sbh}, m_{sbh}, S_{sbh})$ of the store buffer machine, where the next instruction to be executed is a read of thread $i$: \texttt{READ\_volatile \ a \ t} \hspace{1cm} \texttt{The configuration of the virtual machine is } \text{cfg} = (ts, m, S). \hspace{1cm} \text{We have to simulate this step on the virtual machine and can make use of the coupling relations } (ts_{sbh}, m_{sbh}, S_{sbh}) \sim (ts, m, S), \hspace{1cm} \text{the invariants } \text{invariant ts}_{sbh} S_{sbh} m_{sbh} \hspace{1cm} \text{and the safety of all reachable states of the virtual machine: } \text{safe-reach-delayed} (ts, m, S). \hspace{1cm} \text{The state of the store buffer machine and the coupling with the volatile machine is depicted in Figure 14. Note that if there are some suspended instructions in thread $i$, we cannot directly exploit the 'safety of the read', as the virtual machine has not yet reached the state where thread $i$ is poised to do the read. But fortunately we have safety of the virtual machin of all reachable states. Hence we can just execute all suspended instructions of thread $i$ until we reach the read. We refer to this configuration of the virtual machine as } \text{cfg'} = (ts', m', S'), \hspace{1cm} \text{which is depicted in Figure 15.} \hspace{1cm} \text{For now we want to consider the case where the read goes to memory and is not forwarded from the store buffer. The value read is } v = m_{sbh} a. \hspace{1cm} \text{Moreover, we make a case distinction whether there is an outstanding volatile write in the store buffer of thread $i$ or}
Fig. 14: Thread $i$ poised to read

Fig. 15: Forwarded computation of virtual machine
not. This determines if there are suspended instructions in the virtual machine or not. We start with the case where there is no such write. This means that there are no suspended instructions in thread $i$ and therefore $cfg'' = cfg$. We have to show that the virtual machine reads the same value from memory: $v = m a$. So what can go wrong? When can the the memory of the virtual machine hold a different value? The memory of the virtual machine is obtained from the memory of the store buffer machine by executing all store buffers until we hit the first volatile write. So if there is a discrepancy in the value this has to come from a non-volatile write in the executed parts of another thread, let us say thread $j$. This write is marked as x in Figure 16.

![Fig. 16: Conflicting write in thread j (marked x)](image)

We refer to x both for the write operation itself and to characterize the point in time in the computation of the virtual machine where the write was executed. At the point x the write was safe according to rules in Figure 9 for non-volatile writes. So it was owned by thread $j$ and unshared. This knowledge about the safety of write x is preserved in the invariants, namely (Ownership.i) and (Sharing.i). Additionally from invariant (Sharing.v) we know that address $a$ was not read-only at point x. Now we combine this information with the safety of the read of thread $i$ in the current configuration $cfg$: address $a$ either has to be owned by thread $i$, or has to be read-only or the read is volatile and $a$ is shared. Additionally there are the constraints on the released addresses which we will exploit below. Let us address all cases step by step. First, we consider that address $a$ is currently owned by thread $i$. As it was owned by thread $j$ at time x there has to be an release of $a$ in the executed prefix of the store buffer of thread $j$. This release is recorded in the release set, so we know $a \in \text{dom } R_{s[j]}$. This contradicts the safety of the read. Second, we consider that address $a$ is currently read-only. At time x address $a$ was owned by thread $j$, unshared and not read-only. Hence there was a release of address $a$ in the executed prefix of the store buffer of thread $j$, where it made a transition unshared and owned to shared. With the monotonicity of the release sets this means $a \in \text{dom } R_{s[j]}$, even more precisely $R_{s[j]} a = [\text{False}]$. Hence there is no chance to get the read safe (neither a volatile nor a non-volatile). Third, consider a volatile read and that address $a$ is currently shared. This is ruled out by the same line of reasoning as in the previous case. So ultimately we have ruled out all races that could destroy the value at address $a$ and have shown that we can simulate the step on the virtual machine. This completes the simulation of the case where there is no store buffer forwarding and no volatile write in the store buffer of thread $i$. The other cases are handled similar. The main arguments are obtained by arguing about safety of configuration $cfg''$ and exploiting the invariants to rule out conflicting operations.
in other store buffers. When there is a volatile write in the store buffer of thread \(i\) there are still pending suspended instructions in the virtual machine. Hence the virtual machine makes no step and we have to argue that the simulation relation as well as all invariants still hold.

Up to now we have focused on how to simulate the read and in particular on how to argue that the value read in the store buffer machine is the same as the value read in the virtual machine. Besides these simulation properties another major part of the proof is to show that all invariants are maintained. For example if the non-volatile read enters the store buffer we have to argue that this new entry is either owned or refers to an read-only address (Ownership.i). As for the simulation above this follows from safety of the virtual machine in configuration \(cfg''\). However, consider an ghost operation that acquires an address \(a\). From safety of the configuration \(cfg''\) we can only infer that there is no conflicting acquire in the non-volatile prefixes of the other store buffers. In case an conflicting acquire is in the suspended part of a store buffer of thread \(j\) safety of configuration \(cfg''\) is not enough. But as we have safety of all reachable states we can forward the computation of thread \(j\) until the conflicting acquire is about to be executed and construct an unsafe state which rules out the conflict.

Last we want to comment on the case where the store buffer takes a step. The major case distinction is whether a volatile write leaves the store buffer or not. In the former case the virtual machine has to simulate a whole bunch of instructions at once to simulate the store buffer machine up to the next volatile write in the store buffer. In the latter case the virtual machine does no step at all, since the instruction leaving the store buffer is already simulated. In both cases one key argument is commutativity of non-volatile operations with respect to global effects on the memory or the sharing map. Consider a non-volatile store buffer step of thread \(i\). In the configuration of the virtual machine before the store buffer step of thread \(i\), the simulation relation applies the update to the memory and the sharing map of the store buffer machine, within the operations exec-all-until-volatile-write and share-all-until-volatile-write ‘somewhere in the middle’ to obtain the memory and the sharing map of the virtual machine. After the store buffer step however, when the non-volatile operations has left the store buffer, the effect is applied to the memory and the sharing map right in the beginning. The invariants and safety sideconditions for non-volatile operations guarantee ‘locality’ of the operation which manifests in commutativity properties. For example, a non-volatile write is thread local. There is no conflicting write in any other store buffer and hence the write can be safely moved to the beginning.

This concludes the discussion on the proof of Theorem 2.

The simulation theorem for a single step is inductive and can therefore be extended to arbitrary long computations. Moreover, the coupling relation as well as the invariants become trivial for an initial configuration where all store buffers are empty and the ghost state is setup appropriately. To arrive at our final Theorem 1 we need the following steps:

1. simulate the computation of the store buffer machine \((ts_{sb}, m) \xrightarrow{sb}^* (ts'_{sb}, m')\) by a computation of a store buffer machine with history \((ts_{sbh}, m, S) \xrightarrow{sbh}^* (ts'_{sbh}, m', S')\),
2. simulate the computation of the store buffer machine with history by a computation of the virtual machine with delayed releases \((ts, m, S) \xrightarrow{v}^* (ts', m', S')\) by Theorem 2 (extended to the reflexive transitive closure),
3. simulate the computation of the virtual machine with delayed releases by a computation of the virtual machine with free flowing releases \((ts, m, S) \xrightarrow{v}^* (ts', m', S')\)

5 Here we are sloppy with \(ts\); strictly we would have to distinguish the thread configurations without the \(R\) component form the ones with the \(R\) component used for delayed releases.
Step 1 is trivial since the bookkeeping within the additional ghost and history state does not affect the control flow of the transition systems and can be easily removed. Similar the additional $\mathcal{R}$ ghost component can be ignored in Step 3. However, to apply Theorem 2 in Step 2 we have to convert from safe-reach $(ts, m, \mathcal{S})$ provided by the preconditions of Theorem 1 to the required safe-reach-delayed $(ts, m, \mathcal{S})$. This argument is more involved and we only give a short sketch here. The other direction is trivial as every single case for delayed releases (cf. Figure 9) immediately implies the corresponding case for free flowing releases (cf. Figure 7).

First keep in mind that the predicates ensure that all reachable configurations starting from $(ts, m, \mathcal{S})$ are safe, according to the rules for free flowing releases or delayed releases respectively. We show the theorem by contraposition and start with a computation which reaches a configuration $c$ that is unsafe according to the rules for delayed releases and want to show that there has to be a (potentially other) computation (starting from the same initial state) that leads to an unsafe configuration $c'$ according to free flowing releases. If $c$ is already unsafe according to free flowing releases we have $c' = c$ and are finished. Otherwise we have to find another unsafe configuration. Via induction on the length of the global computation we can also assume that for all shorter computations both safety notions coincide. A configuration can only be unsafe with respect to delayed releases and safe with respect to free flowing releases if there is a race between two distinct Threads $i$ and $j$ on an address $a$ that is in the release set $\mathcal{R}$ of one of the threads, lets say Thread $i$. For example Thread $j$ attempts to write to an address $a$ which is in the release set of Thread $i$. If the release map would be empty there cannot be such an race (it would simulataneously be unsafe with respect to free flowing releases). Now we aim to find a configuration $c'$ that is also reachable from the initial configuration and is unsafe with respect to free flowing releases. Intuitively this is a configuration where Thread $i$ is rewinded to the state just before the release of address $a$ and Thread $j$ is in the same state as in configuration $c$. Before the release of $a$ the address has to be owned by Thread $i$, which is unsafe according to free flowing releases as well as delayed releases. So we can argue that either Thread $j$ can reach the same state although Thread $i$ is rewinded or we even hit an unsafe configuration before. What kind of steps can Thread $i$ perform between between the free flowing release point (point of the ghost instruction) and the delayed release point (point of next volatile write, interlocked operation or fence at which the release map is emptied)? How can these actions affect Thread $j$? Note that the delayed release point is not yet reached as this would empty the release map (which we know not to be empty). Thus Thread $i$ does only perform reads, ghost instructions, program steps or non-volatile writes. All of these instructions of Thread $i$ either have no influence on the computation of Thread $j$ at all (e.g. a read, program step, non-volatile write or irrelevant ghost operation) or may cause a safety violation already in a shorter computation (e.g. acquiring an address that another thread holds). This is fine for our inductive argument. So either we can replay every step of Thread $j$ and reach the final configuration $c'$ which is now also unsafe according to free flowing releases, or we hit a configuration $c''$ in a shorter computation which violates the rules of delayed as well as free flowing releases (using the induction hypothesis).

6 PIMP

PIMP is a parallel version of IMP [11], a canonical WHILE-language.

An expression $e$ is either (i) $\text{Const } v$, a constant value, (ii) $\text{Mem volatile } a$, a (volatile) memory lookup at address $a$, (iii) $\text{Tmp sop}$, reading from the temporaries with a operation $sop$ which is an intermediate expression occurring in the transition rules for statements,
(iv) **Unop** \( f \ e \), a unary operation where \( f \) is a unary function on values, and finally
(v) **Binop** \( f \ e_1 \ e_2 \), a binary operation where \( f \) is a binary function on values.

A statement \( s \) is either (i) **SKIP**, the empty statement, (ii) **Assign volatile** \( a \ e \ A \ L \ R \ W \), a (volatile) assignment of expression \( e \) to address expression \( a \), (iii) **CAS** \( a \ c \ e \ A \ L \ R \ W \), atomic compare and swap at address expression \( a \) with compare expression \( c \) and swap expression \( e \), (iv) **SEQ** \( s_1 \ s_2 \), sequential composition, (v) **Cond** \( e \ s_1 \ s_2 \), the if-then-else statement, (vi) **While** \( e \ s \), the loop statement with condition \( e \), (vii) **SGhost**, and **SFence** as stubs for the corresponding memory instructions.

The key idea of the semantics is the following: expressions are evaluated by issuing instructions to the memory system, then the program waits until the memory system has made all necessary results available in the temporaries, which allows the program to make another step. Figure 17 defines expression evaluation. The function \( \text{used-tmps} \ e \) calculates the number of temporaries that are necessary to evaluate expression \( e \), where every **MEM** expression accounts to one temporary. With \( \text{issue-expr} \ t \ e \) we obtain the instruction list for expression \( e \) starting at temporary \( t \), whereas \( \text{eval-expr} \ t \ e \) constructs the operation as a pair of the domain and a function on the temporaries.

The program transitions are defined in Figure 18. We instantiate the program state by a tuple \( (s, \ t) \) containing the statement \( s \) and the temporary counter \( \ t \). To assign an expression \( e \) to an address(-expression) \( a \) we first create the memory instructions for evaluation the address \( a \) and transforming the expression to an operation on temporaries. The temporary counter is incremented accordingly. When the value is available in the temporaries we continue by creating the memory instructions for evaluation of expression \( e \) followed by the corresponding store operation. Note that the ownership annotations can depend on the temporaries and thus can take the calculated address into account.

Execution of compare and swap CAS involves evaluation of three expressions, the address \( a \) the compare value \( c_e \) and the swap value \( s_e \). It is finally mapped to the read-modify-write instruction RMW of the memory system. Recall that execution of RMW first stores the memory content at address \( a \) to the specified temporary. The condition compares this value with the result of evaluating \( c_e \) and writes swap value \( s_e \) if successful. In either case the temporary finally returns the old value read.

Sequential composition is straightforward. An if-then-else is computed by first issuing the memory instructions for evaluation of condition \( e \) and transforming the condition to an operation on temporaries. When the result is available the transition to the first or second statement is made, depending on the result of \( \text{isTrue} \). Execution of the loop is defined
∀ sop. a ≠ Tmp sop  
\[ a' = \text{Tmp (eval-expr } t \ a) \]
\[ t' = t + \text{used-tmps } a \]
\[ is = \text{issue-expr } t \ a \]
\[
\vartheta \vdash (\text{Assign volatile } a \ e \ A \ L \ R \ W, t) \rightarrow_p ((\text{Assign volatile } a' e \ A \ L \ R \ W, t'), is)
\]
\[ D \subseteq \text{dom } \vartheta \]
\[ is = \text{issue-expr } t \ e \ \forall [\text{Write volatile } (a \ \vartheta) (\text{eval-expr } t \ e) (A \ \vartheta) (L \ \vartheta) (R \ \vartheta) (W \ \vartheta)]\]
\[
\vartheta \vdash (\text{Assign volatile } (\text{Tmp } (D, a)) e \ A \ L \ R \ W, t) \rightarrow_p ((\text{Skip, } t + \text{used-tmps } e), is)
\]
∀ sop. a ≠ Tmp sop  
\[ a' = \text{Tmp (eval-expr } t \ a) \]
\[ t' = t + \text{used-tmps } a \]
\[ is = \text{issue-expr } t \ a \]
\[
\vartheta \vdash (\text{CAS } a c_s s_k A \ L \ R \ W, t) \rightarrow_p ((\text{CAS } a' c_s s_k A \ L \ R \ W, t'), is)
\]
\[ D_c \subseteq \text{dom } \vartheta \]
\[ \text{eval-expr } s_k = (D, t) \]
\[ t' = t + \text{used-tmps } s_k \]
\[ \text{cond} = (\lambda \vartheta. \text{true}) (\theta \ t') = c \ \vartheta \]
\[ \text{ret} = (\lambda v_1 v_2. v_1) \]
\[ is = \text{issue-expr } t \ s_k \ \forall [\text{RMW } (a \ \vartheta) t' (D, t) \text{ cond ret } (A \ \vartheta) (L \ \vartheta) (R \ \vartheta) (W \ \vartheta)]\]
\[
\vartheta \vdash (\text{CAS } (\text{Tmp } (D_c, a)) (\text{Tmp } (D_c, c)) s_k A \ L \ R \ W, t) \rightarrow_p ((\text{Skip, } \text{Suc } t'), is)
\]
\[
\vartheta \vdash (\text{SEQ } s_1 s_2, t) \rightarrow_p ((\text{SEQ } s_1 s_2, t'), is)
\]
\[
\vartheta \vdash (\text{SEQ SKIP } s_2, t) \rightarrow_p ((s_2, t), []]
\]
∀ sop. e ≠ Tmp sop  
\[ e' = \text{Tmp (eval-expr } t \ e) \]
\[ t' = t + \text{used-tmps } e \]
\[ is = \text{issue-expr } t \ e \]
\[
\vartheta \vdash (\text{Cond } e s_1 s_2, t) \rightarrow_p ((\text{Cond } e' s_1 s_2, t'), is)
\]
\[
\vartheta \vdash (\text{Cond } (\text{Tmp } (D, e)) s_1 s_2, t) \rightarrow_p ((s_1, t), [])
\]
\[
\vartheta \vdash (\text{Cond } (\text{Tmp } (D, e)) s_1 s_2, t) \rightarrow_p ((s_2, t), [])
\]
\[
\vartheta \vdash (\text{While } e s, t) \rightarrow_p ((\text{Cond } e (\text{SEQ } s (\text{While } e s)) \text{ Skip, } t), []]
\]
\[
\vartheta \vdash (\text{SGhost } A \ L \ R \ W, t) \rightarrow_p ((\text{Skip, } t), [\text{Ghost } (A \ \vartheta) (L \ \vartheta) (R \ \vartheta) (W \ \vartheta)])
\]
\[
\vartheta \vdash (\text{SFence, } t) \rightarrow_p ((\text{Skip, } t), [\text{Fence}])
\]

Fig. 18: Program transitions
by stepwise unfolding. Ghost and fence statements are just propagated to the memory system.

To instantiate Theorem 2 with PIMP we define the invariant parameter valid, which has to be maintained by all transitions of PIMP, the memory system and the store buffer. Let $\vartheta$ be the valuation of temporaries in the current configuration, for every thread configuration $\text{ts}_b[i] = ((s, t), \vartheta, \text{sb}, D, O)$ where $i < |\text{ts}_b|$ we require: (i) The domain of all intermediate $\text{Tmp}(D, f)$ expressions in statement $s$ is below counter $t$. (ii) All temporaries in the memory system including the store buffer are below counter $t$. (iii) All temporaries less than counter $t$ are either already defined in the temporaries $\vartheta$ or are outstanding read temporaries in the memory system.

For the PIMP transitions we prove these invariants by rule induction on the semantics. For the memory system (including the store buffer steps) the invariants are straightforward. The memory system does not alter the program state and does not create new temporaries, only the PIMP transitions create new ones in strictly ascending order.

7 Conclusion

We have presented a practical and flexible programming discipline for concurrent programs that ensures sequential consistency on TSO machines, such as present x64 architectures. Our approach covers a wide variety of concurrency control, covering locking, data races, single writer multiple readers, read only and thread local portions of memory. We minimize the need for store buffer flushes to optimize the usage of the hardware. Our theorem is not coupled to a specific logical framework like separation logic but is based on more fundamental arguments, namely the adherence to the programming discipline which can be discharged within any program logic using the standard sequential consistent memory model, without any of the complications of TSO.

Related work. Disclaimer. This contribution presents the state of our work from 2010 [8]. Finally, 8 years later, we made the AFP submission for Isabelle2018. This related work paragraph does not thoroughly cover publications that came up in the meantime.

A categorization of various weak memory models is presented in [2]. It is compatible with the recent revisions of the Intel manuals [10] and the revised x86 model presented in [15]. The state of the art in formal verification of concurrent programs is still based on a sequentially consistent memory model. To justify this on a weak memory model often a quite drastic approach is chosen, allowing only coarse-grained concurrency usually implemented by locking. Thereby data races are ruled out completely and there are results that data race free programs can be considered as sequentially consistent for example for the Java memory model [3, 18] or the x86 memory model [15]. Ridge [17] considers weak memory and data-races and verifies Peterson’s mutual exclusion algorithm. He ensures sequential consistency by flushing after every write to shared memory. Burckhardt and Musuvathi [6] describe an execution monitor that efficiently checks whether a sequentially consistent TSO execution has a single-step extension that is not sequentially consistent. Like our approach, it avoids having to consider the store buffers as an explicit part of the state. However, their condition requires maintaining in ghost state enough history information to determine causality between events, which means maintaining a vector clock (which is itself unbounded) for each memory address. Moreover, causality (being essentially graph reachability) is already not first-order, and hence unsuitable for many types of program verification. Closely related to our work is the draft of Owens [14] which also investigates on the conditions for sequential consistent reasoning within TSO. The notion of a triangular-race free trace is established to exactly characterize the traces on
a TSO machine that are still sequentially consistent. A triangular race occurs between a read and a write of two different threads to the same address, when the reader still has some outstanding writes in the store buffer. To avoid the triangular race the reader has to flush the store buffer before reading. This is essentially the same condition that our framework enforces, if we limit every address to be unowned and every access to be volatile. We regard this limitation as too strong for practical programs, where non-volatile accesses (without any flushes) to temporarily local portions of memory (e.g. lock protected data) is common practice. This is our core motivation for introducing the ownership based programming discipline. We are aware of two extensions of our work that were published in the meantime. Chen et al. [7] also take effects of the MMU into account and generalize our reduction theorem to handle programs that edit page tables. Oberhauser [13] improves on the flushing policy to also take non-triangular races into account and facilitates an alternative proof approach.

**Limitations.** There is a class of important programs that are not sequentially consistent but nevertheless correct.

First consider a simple spinlock implementation with a volatile lock \( l \), where \( l == 0 \) indicates that the lock is not taken. The following code acquires the lock:

```c
while(!interlocked_test_and_set(l));
<critical section accessing protected objects>,
```

and with the assignment \( l = 0 \) we can release the lock again. Within our framework address \( l \) can be considered unowned (and hence shared) and every access to it is volatile. We do not have to transfer ownership of the lock \( l \) itself but of the objects it protects. As acquiring the lock is an expensive interlocked operation anyway there are no additional restrictions from our framework. The interesting point is the release of the lock via the volatile write \( l = 0 \). This leaves the dirty bit set, and hence our programming discipline requires a flushing instruction before the next volatile read. If \( l \) is the only volatile variable this is fine, since the next operation will be a lock acquire again which is interlocked and thus flushes the store buffer. So there is no need for an additional fence. But in general this is not the case and we would have to insert a fence after the lock release to make the dirty bit clean again and to stay sequentially consistent. However, can we live without the fence? For the correctness of the mutual-exclusion algorithm we can, but we leave the domain of sequential consistent reasoning. The intuitive reason for correctness is that the threads waiting for the lock do no harm while waiting. They only take some action if they see the lock being zero again, this is when the lock release has made its way out of the store buffer.

Another typical example is the following simplified form of barrier synchronization: each processor has a flag that it writes (with ordinary volatile writes without any flushing) and other processors read, and each processor waits for all processors to set their flags before continuing past the barrier. This is not sequentially consistent – each processor might see his own flag set and later see all other flags clear – but it is still correct.

Common for these examples is that there is only a single writer to an address, and the values written are monotonic in a sense that allows the readers to draw the correct conclusion when they observe a certain value. This pattern is named *Publication Idiom* in Owens work [14].

**Future work.** The first direction of future work is to try to deal with the limitations of sequential consistency described above and try to come up with a more general reduction
theorem that can also handle non-sequential consistent code portions that follow some monotonicity rules.

Another direction of future work is to take compiler optimization into account. Our volatile accesses correspond roughly to volatile memory accesses within a C program. An optimizing compiler is free to convert any sequence of non-volatile accesses into a (sequentially semantically equivalent) sequence of accesses. As long as execution is sequentially consistent, equivalence of these programs (e.g., with respect to final states of executions that end with volatile operations) follows immediately by reduction. However, some compilers are a little more lenient in their optimizations, and allow operations on certain local variables to move across volatile operations. In the context of C (where pointers to stack variables can be passed by pointer), the notion of “locality” is somewhat tricky, and makes essential use of C forbidding (semantically) address arithmetic across memory objects.

Acknowledgements

We thank Mark Hillebrand for discussions and feedback on this work and extensive comments on this report.

A Appendix

After the explanatory text in the main body of the document we now show the plain theory files.

theory ReduceStoreBuffer
imports Main
begin

A.1 Memory Instructions

type-synonym addr = nat
type-synonym val = nat
type-synonym tmp = nat

type-synonym tmps = tmp ⇒ val option
type-synonym sop = tmp set × (tmps ⇒ val) — domain and function

locale valid-sop =
fixes sop :: sop
assumes valid-sop: \( \forall D \ f \ \theta . \ [sop=(D,f); D \subseteq \text{dom } \theta] \implies f \ \theta = f (\theta|\ D) \)

type-synonym memory = addr ⇒ val
type-synonym owns = addr set
type-synonym rels = addr ⇒ bool option
type-synonym shared = addr ⇒ bool option
type-synonym acq = addr set
type-synonym rel = addr set
type-synonym lcl = addr set
type-synonym wrt = addr set
type-synonym cond = tmps ⇒ bool
type-synonym ret = val ⇒ val ⇒ val

datatype instr = Read bool addr tmp
| Write bool addr sop acq lcl rel wrt
| RMW addr tmp sop cond ret acq lcl rel wrt
| Fence
| Ghost acq lcl rel wrt

type-synonym instrs = instr list

type-synonym (′p,′sb,′dirty,′owns,′rels) thread-config =
′p × instrs × tmps × ′sb × ′dirty × ′owns × ′rels
type-synonym (′p,′sb,′dirty,′owns,′rels,′shared) global-config =
(′p,′sb,′dirty,′owns,′rels) thread-config list × memory × ′shared

definition owned t = (let (p,instrs,θ,sb,D,O,R) = t in O)

lemma owned-simp [simp]: owned (p,instrs,θ,sb,D,O,R) = (O)
(proof)

definition O-sb t = (let (p,instrs,θ,sb,D,O,R) = t in (O,sb))

lemma O-sb-simp [simp]: O-sb (p,instrs,θ,sb,D,O,R) = (O,sb)
(proof)

definition released t = (let (p,instrs,θ,sb,D,O,R) = t in R)

lemma released-simp [simp]: released (p,instrs,θ,sb,D,O,R) = (R)
(proof)

lemma list-update-id′: v = xs ! i =⇒ xs[i := v] = xs
(proof)

lemmas converse-rtranclp-induct5 =
converse-rtranclp-induct [where a=(m,sb,O,R,S) and b=(m′,sb′,O′,R′,S′),
split-rule,consumes 1, case-names refl step]

A.2 Abstract Program Semantics

locale memory-system =

fixes
memop-step :: (instrs × tmps × ′sb × memory × ′dirty × ′owns × ′rels × ′shared) ⇒
(instrs × tmps × ′sb × memory × ′dirty × ′owns × ′rels × ′shared) ⇒ bool
(- →m - [60,60] 100) and
storebuffer-step:: (memory × 'sb × 'owns × 'rels × 'shared) ⇒ (memory × 'sb × 'owns × 'rels × 'shared) ⇒ bool and

locale program =
  fixes
  program-step :: tmps ⇒ 'p ⇒ 'p × instrs ⇒ bool (- ⊢ p - [60,60,60] 100)
  — A program only accesses the shared memory indirectly, it can read the temporaries and can output a sequence of memory instructions

locale computation = memory-system + program +
  constrains
  — The constrains are only used to name the types 'sb and 'p
  storebuffer-step:: (memory × 'sb × 'owns × 'rels × 'shared) ⇒ (memory × 'sb × 'owns × 'rels × 'shared) ⇒ bool and
  memop-step ::
    (instrs × tmps × 'sb × memory × 'dirty × 'owns × 'rels × 'shared) ⇒
    (instrs × tmps × 'sb × memory × 'dirty × 'owns × 'rels × 'shared) ⇒ bool
  and
  program-step :: tmps ⇒ 'p ⇒ 'p × instrs ⇒ bool
  fixes
  record :: 'p ⇒ 'p ⇒ instrs ⇒ 'sb ⇒ 'sb

begin

  inductive concurrent-step ::
    ( 'p,'sb,'dirty,'owns,'rels,'shared) global-config ⇒ ( 'p,'sb,'dirty,'owns,'rels,'shared)
  global-config ⇒ bool
    (- ⇒ - [60,60] 100)

where
  Program:
  [i < length ts; ts!i = (p,is,δ,sb,D,O,R);
   δ+p →p (p’,is’)] ⇒
  (ts,m,S) ⇒ (ts[i] := (p’,is@is’,δ,record p p’ is’ sb,D,O,R)],m,S)

| Memop:
  [i < length ts; ts!i = (p,is,δ,sb,D,O,R);
   (is,δ,sb,m,D,O,R,S) →m (is’,δ’,sb’,m’,D’,O’,R’,S’)] ⇒
  (ts,m,S) ⇒ (ts[i] := (p,is’,δ’,sb’,D’,O’,R’)],m’,S’)

| StoreBuffer:
  [i < length ts; ts!i = (p,is,δ,sb,D,O,R);
   (m,sb,O,R,S) →sb (m’,sb’,O’,R’,S’)] ⇒
  (ts,m,S) ⇒ (ts[i] := (p,is,δ,sb,D,O’,R’)],m’,S’)

definition final:: ( 'p,'sb,'dirty,'owns,'rels,'shared) global-config ⇒ bool
where
  final c = (¬ (∃ c’. c ⇒ c’))
Lemma store-buffer-steps:
Assumes sb-step: storebuffer-step** (m,sb,O,R,S) (m',sb',O',R',S')
Shows \( \forall ts. \ i < \text{length ts} \Rightarrow ts[i] = (p,is,\theta,sb,D,O,R,S) \Rightarrow \) concurrent-step** (ts,m,S) (ts[i:=(p,is,\theta,sb',D,O',R',R')],m',S')

Proof

Lemma step-preserves-length-ts:
Assumes step: (ts,m,S) \Rightarrow (ts',m',S')
Shows length ts' = length ts

Proof

Lemmas concurrent-step-cases = computation.concurrent-step.cases
[cases set, consumes 1, case-names Program Memop StoreBuffer]

Definition augment-shared:: shared \Rightarrow addr set \Rightarrow addr set \Rightarrow shared (- \oplus - [61,1000,60] 61)
Where
\( S \oplus_W S = (\lambda a. \text{if } a \in S \text{ then } \text{Some } (a \in W) \text{ else } S a) \)

Definition restrict-shared:: shared \Rightarrow addr set \Rightarrow addr set \Rightarrow shared (- \ominus - [51,1000,50] 51)
Where
\( S \ominus_A L = (\lambda a. \text{if } a \in L \text{ then } \text{None} \text{ else } (\text{case } S a \text{ of } \text{None} \Rightarrow \text{None} \mid \text{Some writeable} \Rightarrow \text{Some } (a \in A \lor \text{writeable}))) \)

Definition read-only :: shared \Rightarrow addr set
Where
read-only S \equiv \{ a. (S a = \text{Some False}) \}

Definition shared-le:: shared \Rightarrow shared \Rightarrow bool (infix \( \subseteq_s 50 \))
Where
\( m_1 \subseteq_s m_2 \equiv m_1 \subseteq_m m_2 \land \text{read-only } m_1 \subseteq \text{read-only } m_2 \)

Lemma shared-leD: m_1 \subseteq_s m_2 \Rightarrow m_1 \subseteq_m m_2 \land \text{read-only } m_1 \subseteq \text{read-only } m_2
Proof

Lemma shared-le-map-le: m_1 \subseteq_s m_2 \Rightarrow m_1 \subseteq_m m_2
Proof

Lemma shared-le-read-only-le: m_1 \subseteq_s m_2 \Rightarrow \text{read-only } m_1 \subseteq \text{read-only } m_2
Proof

Lemma dom-augment [simp]: dom (m \oplus_W S) = dom m \cup S
Proof

Lemma augment-empty [simp]: S \oplus_x \{\} = S
Proof
lemma inter-neg [simp]: $X \cap -L = X - L$
(proof)

lemma dom-restrict-shared [simp]: dom $(m \ominus_A L) = \text{dom } m - L$
(proof)

lemma restrict-shared-UNIV [simp]: $(m \ominus_A \text{UNIV}) = \text{Map.empty}$
(proof)

lemma restrict-shared-empty [simp]: $(\text{Map.empty} \ominus_A L) = \text{Map.empty}$
(proof)

lemma restrict-shared-in [simp]: $a \in L \implies (m \ominus_A L) a = \text{None}$
(proof)

lemma restrict-shared-out: $a \notin L \implies (m \ominus_A L) a = \text{map-option } (\lambda \text{writeable}. (a \in A \lor \text{writeable})) (m a)$
(proof)

lemma restrict-shared-out' [simp]:
$a \notin L \implies m a = \text{Some writeable} \implies (m \ominus_A L) a = \text{Some } (a \in A \lor \text{writeable})$
(proof)

lemma augment-mono-map': $A \subseteq_m B \implies (A \oplus_x C) \subseteq_m (B \oplus_x C)$
(proof)

lemma augment-mono-map: $A \subseteq_s B \implies (A \oplus_x C) \subseteq_s (B \oplus_x C)$
(proof)

lemma restrict-mono-map: $A \subseteq_s B \implies (A \ominus_x C) \subseteq_s (B \ominus_x C)$
(proof)

lemma augment-mono-aux: dom $A \subseteq \text{dom } B \implies \text{dom } (A \ominus_x C) \subseteq \text{dom } (B \ominus_x C)$
(proof)

lemma restrict-mono-aux: dom $A \subseteq \text{dom } B \implies \text{dom } (A \ominus_x C) \subseteq \text{dom } (B \ominus_x C)$
(proof)

lemma read-only-mono: $S \subseteq_m S' \implies a \in \text{read-only } S \implies a \in \text{read-only } S'$
(proof)

lemma in-read-only-restrict-conv:
$a \in \text{read-only } (S \ominus_A L) = (a \in \text{read-only } S \land a \notin L \land a \notin A)$
(proof)
**lemma** in-read-only-augment-conv: $a \in \text{read-only} (\mathcal{S} \oplus_{\text{W}} \mathcal{R}) = (\text{if } a \in \mathcal{R} \text{ then } a \not\in \mathcal{W} \text{ else } a \in \text{read-only } \mathcal{S})$

(proof)

**lemmas** in-read-only-convs = in-read-only-restrict-conv in-read-only-augment-conv

**lemma** read-only-dom: read-only $\mathcal{S} \subseteq \text{dom } \mathcal{S}$

(proof)

**lemma** read-only-empty [simp]: read-only Map.empty = {}

(proof)

**lemma** restrict-shared-fuse: $\mathcal{S} \ominus_{\text{A}} \mathcal{L} \ominus_{\text{B}} \mathcal{M} = (\mathcal{S} \ominus_{(\text{A} \cup \text{B})} (\mathcal{L} \cup \mathcal{M}))$

(proof)

**lemma** restrict-shared-empty-set [simp]: $\mathcal{S} \ominus \{\} = \mathcal{S}$

(proof)

**definition** augment-rels:: addr set $\Rightarrow$ addr set $\Rightarrow$ rels $\Rightarrow$ rels

where

augment-rels $\mathcal{S} \mathcal{R} \mathcal{R} = (\lambda a. \text{if } a \in \mathcal{R} \text{ then (case } \mathcal{R} \ a \text{ of None } \Rightarrow \text{ Some } (a \in \mathcal{S}) \ | \ \text{ Some } s \Rightarrow \text{ Some } (s \land (a \in \mathcal{S}))) \text{ else } \mathcal{R} \ a)$

declare domIff [iff del]

A.3 Memory Transitions

locale gen-direct-memop-step =

fixes emp::'rels and aug::owns $\Rightarrow$ rel $\Rightarrow$ 'rels $\Rightarrow$ 'rels

begin

inductive gen-direct-memop-step :: (instrs $\times$ tmps $\times$ unit $\times$ memory $\times$ bool $\times$ owns $\times$ 'rels $\times$ shared ) $\Rightarrow$

(instrs $\times$ tmps $\times$ unit $\times$ memory $\times$ bool $\times$ owns $\times$ 'rels $\times$ shared ) $\Rightarrow$ bool

(- $\rightarrow$ - [60,60] 100)

where

Read: (Read volatile $a$ $t$ # is,$\theta$, $x$, $m$,$\mathcal{D}$, $\mathcal{O}$, $\mathcal{R}$, $\mathcal{S}$) $\rightarrow$

(is, $\theta$ ($t$=$m$ a), $x$, $m$, $\mathcal{D}$, $\mathcal{O}$, $\mathcal{R}$, $\mathcal{S}$)

| WriteNonVolatile:

(Write False $a$ ($D,f$) $A$ $L$ $R$ $W$#is, $\theta$, $x$, $m$, $\mathcal{D}$, $\mathcal{O}$, $\mathcal{R}$, $\mathcal{S}$) $\rightarrow$

(is, $\theta$, $x$, m($a:=f$ $\theta$), $\mathcal{D}$, $\mathcal{O}$, $\mathcal{R}$, $\mathcal{S}$)

| WriteVolatile:

(Write True $a$ ($D,f$) $A$ $L$ $R$ $W$# is, $\theta$, $x$, $m$, $\mathcal{D}$, $\mathcal{O}$, $\mathcal{R}$, $\mathcal{S}$) $\rightarrow$

(is, $\theta$, $x$, m($a:=f$ $\theta$), True, $\mathcal{O}$ $\cup$ $A$ $-$ $R$, emp, $\mathcal{S}$ $\oplus_{\text{W}}$ $\mathcal{R}$ $\ominus_{\text{A}}$ $L$)

| Fence:
(Fence # is, \(\vartheta\), x, m, \(\mathcal{D}, \mathcal{O}, \mathcal{R}, \mathcal{S}\)) \(\rightarrow\) (is, \(\vartheta\), x, m, False, \(\mathcal{O}, \text{emp}, \mathcal{S}\))

<table>
<thead>
<tr>
<th>RMWReadOnly:</th>
<th>(condition (\neg \vartheta(t \mapsto m a))) (\Rightarrow)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(RMW a t (D,f) condition ret A L R W # is, (\vartheta), x, m, (\mathcal{D}, \mathcal{O}, \mathcal{R}, \mathcal{S})) (\rightarrow) (is, (\vartheta(t \mapsto m a), x, m,) False, (\mathcal{O}, \text{emp}, \mathcal{S}))</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RMWWrite:</th>
<th>(condition (\vartheta(t \mapsto m a))) (\Rightarrow)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(RMW a t (D,f) condition ret A L R W # is, (\vartheta), x, m, (\mathcal{D}, \mathcal{O}, \mathcal{R}, \mathcal{S})) (\rightarrow) (is, (\vartheta(t \mapsto \text{ret} (m a)) (f(\vartheta(t \mapsto m a))), x, m(a:= f(\vartheta(t \mapsto m a))), \text{False}, \mathcal{O} \cup \mathcal{A} - \mathcal{R}, \text{emp}, \mathcal{S} \ominus \mathcal{W} \ominus \mathcal{A} \ominus \mathcal{L})</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ghost:</th>
<th>(condition (\text{Ghost A L R W # is, } \vartheta, x, m, \mathcal{D}, \mathcal{O}, \mathcal{R}, \mathcal{S})) (\rightarrow)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(is, (\vartheta), x, m, (\mathcal{D}, \mathcal{O} \cup \mathcal{A} - \mathcal{R}, \text{aug} (\text{dom} \mathcal{S}) \ominus \mathcal{R}, \mathcal{S} \ominus \mathcal{W}, \mathcal{R} \ominus \mathcal{A} \ominus \mathcal{L})</td>
<td></td>
</tr>
</tbody>
</table>

end interpretation direct-memop-step: gen-direct-memop-step Map.empty augment-rels

\[\langle \text{proof}\rangle\]

**term** direct-memop-step.gen-direct-memop-step

**abbreviation** direct-memop-step :: (instrs \(\times\) tmprs \(\times\) unit \(\times\) memory \(\times\) bool \(\times\) owns \(\times\) rels \(\times\) shared) \(\Rightarrow\) (instrs \(\times\) tmprs \(\times\) unit \(\times\) memory \(\times\) bool \(\times\) owns \(\times\) rels \(\times\) shared) \(\Rightarrow\) bool

\((- \rightarrow - [60,60] 100)

**where**

direct-memop-step \(\equiv\) direct-memop-step.gen-direct-memop-step

**term** \(x \rightarrow Y\)

**abbreviation** direct-memop-steps :: (instrs \(\times\) tmprs \(\times\) unit \(\times\) memory \(\times\) bool \(\times\) owns \(\times\) rels \(\times\) shared) \(\Rightarrow\) (instrs \(\times\) tmprs \(\times\) unit \(\times\) memory \(\times\) bool \(\times\) owns \(\times\) rels \(\times\) shared) \(\Rightarrow\) bool

\((- \rightarrow^* - [60,60] 100)

**where**

direct-memop-steps \(==\) (direct-memop-step)^**

**term** \(x \rightarrow^* Y\)

interpretation virtual-memop-step: gen-direct-memop-step () (\(\lambda S \mathcal{R}. ()\)) \(\langle \text{proof}\rangle\)

**abbreviation** virtual-memop-step :: (instrs \(\times\) tmprs \(\times\) unit \(\times\) memory \(\times\) bool \(\times\) owns \(\times\) unit \(\times\) shared) \(\Rightarrow\) (instrs \(\times\) tmprs \(\times\) unit \(\times\) memory \(\times\) bool \(\times\) owns \(\times\) unit \(\times\) shared) \(\Rightarrow\) bool

\((- \rightarrow^*_v - [60,60] 100)

**where**

virtual-memop-step \(\equiv\) virtual-memop-step.gen-direct-memop-step
term \( x \rightarrow_{v} Y \)

**abbreviation** virtual-memop-steps ::

\[
\text{instruction} \times \text{tmps} \times \text{unit} \times \text{memory} \times \text{bool} \times \text{owns} \times \text{unit} \times \text{shared} \rightarrow \text{bool}
\]

where

virtual-memop-steps \( == \) \((\text{virtual-memop-step})^\ast\)

**term** \( x \rightarrow^* Y \)

**lemma** virtual-memop-step-simulates-direct-memop-step:

**assumes** step:

\[
(is, \theta, x, m, D, O, R, S) \rightarrow (is', \theta', x', m', D', O', R', S')
\]

**shows** \((is, \theta, x, m, D, O, (), S) \rightarrow_v (is', \theta', x', m', D', O', (), S')\)

\[\langle \text{proof} \rangle\]

A.4 Safe Configurations of Virtual Machines

**inductive** safe-direct-memop-state :: owns list \( \Rightarrow \) nat \( \Rightarrow \) bool

\[
\text{(instructions} \times \text{tmps} \times \text{memory} \times \text{bool} \times \text{owns} \times \text{unit} \times \text{shared}) \Rightarrow \text{bool}
\]

where

Read: \[
[a \in O \lor a \in \text{read-only} \ S \lor (\text{volatile} \land a \in \text{dom} \ S); \ \text{volatile} \rightarrow \lnot \ D]
\]

\[
\Rightarrow \ O_s, i \vdash (\text{Read volatile a t # is}, \ \theta, m, D, O, S)\sqrt{}
\]

<table>
<thead>
<tr>
<th>WriteNonVolatile:</th>
</tr>
</thead>
<tbody>
<tr>
<td>[a \in O; a \notin \text{dom} \ S]</td>
</tr>
</tbody>
</table>

\[
\Rightarrow \ O_s, i \vdash (\text{Write False a (D,f) A L R W# is}, \ \theta, m, D, O, S)\sqrt{}
\]

<table>
<thead>
<tr>
<th>WriteVolatile:</th>
</tr>
</thead>
<tbody>
<tr>
<td>[\forall j &lt; \text{length} \ O_s. \ i \neq j \rightarrow a \notin \ O_s!j; \ A \subseteq \text{dom} \ S \cup O; L \subseteq A; R \subseteq O; A \cap R = {};]</td>
</tr>
</tbody>
</table>

\[
\Rightarrow \ O_s, i \vdash (\text{Write True a (D,f) A L R W# is}, \ \theta, m, D, O, S)\sqrt{}
\]

<table>
<thead>
<tr>
<th>Fence:</th>
</tr>
</thead>
</table>
| \[O_s, i \vdash (\text{Fence # is}, \ \theta, m, D, O, S)\sqrt{}
\]

<table>
<thead>
<tr>
<th>Ghost:</th>
</tr>
</thead>
<tbody>
<tr>
<td>[A \subseteq \text{dom} \ S \cup O; L \subseteq A; R \subseteq O; A \cap R = {};]</td>
</tr>
</tbody>
</table>

\[
\forall j < \text{length} \ O_s. \ i \neq j \rightarrow A \cap O_s!j = \{}\]
\[\text{⇒ } \text{Os}, i \vdash (\text{Ghost } A \text{ L } R \text{ W# is } \varnothing, m, D, O, S) \sqrt{\text{\textendash\textendash\textendash}}\]

[RMWReadOnly:]
\[- \text{ cond } \left( \varnothing(t \mapsto \text{m a}) \right); a \in O \lor a \in \text{dom } S \]\[\text{⇒}\]
\[\text{Os}, i \vdash (\text{RMW } a \text{ t } (D, f) \text{ cond ret } A \text{ L } R \text{ W# is } \varnothing, m, D, O, S) \sqrt{\text{\textendash\textendash\textendash}}\]

[RMWWrite:]
\[\text{cond } \left( \varnothing(t \mapsto \text{m a}) \right);\]
\[
\begin{align*}
\forall j < \text{length } \text{Os}. \ i \neq j & \rightarrow a \notin \text{Os}[j]; \\
A \subseteq \text{dom } S \cup O; L \subseteq A; R \subseteq O; A \cap R = \{\}; \\
\forall j < \text{length } \text{Os}. \ i \neq j & \rightarrow A \cap \text{Os}[j] = \{\}; \\
a \notin \text{read-only } S\end{align*}
\]

\[\text{⇒}\]
\[\text{Os}, i \vdash (\text{RMW } a \text{ t } (D, f) \text{ cond ret } A \text{ L } R \text{ W# is } \varnothing, m, D, O, S) \sqrt{\text{\textendash\textendash\textendash}}\]

[Nil:]
\[\text{Os}, i \vdash ([], \varnothing, m, D, O, S) \sqrt{\text{\textendash\textendash\textendash}}\]

\begin{itemize}
  \item \textbf{indeutive} \text{safe-delayed-direct-memop-state :: owns list ⇒ rels list ⇒ nat ⇒}
  \[\text{ instrs } \times \text{ tmps } \times \text{ memory } \times \text{ owns } \times \text{ shared } \Rightarrow \text{ bool }\]
  \[\begin{array}{c}
  (-, -, -, - \vdash -) \\
  \text{where}
  \end{array}\]
  \begin{itemize}
    \item \textbf{Read:}
      \[\begin{align*}
      a \in O & \lor a \in \text{read-only } S \lor (\text{volatile } \land a \in \text{dom } S); \\
      \forall j < \text{length } \text{Os}. \ i \neq j & \rightarrow (\text{Os}[j]) a \neq \text{Some False}; (* \text{ no release of unshared address})
      \end{align*}\]
    \item \textbf{*)}
      \[\begin{align*}
      \neg \text{volatile} & \rightarrow (\forall j < \text{length } \text{Os}. \ i \neq j \rightarrow a \notin \text{dom } (\text{Os}[j])); \\
      \text{volatile} & \rightarrow \neg D \end{align*}\]
  \end{itemize}
\end{itemize}

\[\text{⇒}\]
\[\text{Os}, R_s, i \vdash (\text{Read volatile } a \text{ t } \# \text{ is } \varnothing, m, D, O, S) \sqrt{\text{\textendash\textendash\textendash}}\]

[WriteNonVolatile:]
\[\begin{align*}
[a \in O; a \notin \text{dom } S; \forall j < \text{length } \text{Os}. \ i \neq j & \rightarrow a \notin \text{dom } (\text{Os}[j])]
\end{align*}\]

\[\text{⇒}\]
\[\text{Os}, R_s, i \vdash (\text{Write False } a \text{ } (D, f) \text{ } A \text{ L } R \text{ W# is } \varnothing, m, D, O, S) \sqrt{\text{\textendash\textendash\textendash}}\]

[WriteVolatile:]
\[\begin{align*}
[\forall j < \text{length } \text{Os}. \ i \neq j & \rightarrow a \notin (\text{Os}[j] \cup \text{dom } (\text{Os}[j])); \\
A \subseteq \text{dom } S \cup O; L \subseteq A; R \subseteq O; A \cap R = \{\}; \\
\forall j < \text{length } \text{Os}. \ i \neq j & \rightarrow A \cap (\text{Os}[j] \cup \text{dom } (\text{Os}[j])) = \{\}; \\
a \notin \text{read-only } S\end{align*}\]

\[\text{⇒}\]
\[\text{Os}, R_s, i \vdash (\text{Write True } a \text{ } (D, f) \text{ } A \text{ L } R \text{ W# is } \varnothing, m, D, O, S) \sqrt{\text{\textendash\textendash\textendash}}\]

[ Fence:]
\[\text{Os}, R_s, i \vdash (\text{Fence } \# \text{ is } \varnothing, m, D, O, S) \sqrt{\text{\textendash\textendash\textendash}}\]

[ Ghost:]
\[\begin{align*}
[A \subseteq \text{dom } S \cup O; L \subseteq A; R \subseteq O; A \cap R = \{\}; \\
\forall j < \text{length } \text{Os}. \ i \neq j & \rightarrow A \cap (\text{Os}[j] \cup \text{dom } (\text{Os}[j])) = \{\}]
\end{align*}\]

\[\text{⇒}\]
\( Os, Rs, i \vdash (\text{Ghost A L R W# is} \varnothing, m, D, O, S) \sqrt{\text{علاقات}} \)

<table>
<thead>
<tr>
<th>RMWReadOnly:</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ \neg \text{cond } (\theta (t \mapsto m \ a)); a \in O \lor a \in \text{dom } S; \forall j &lt; \text{length } Os. i \neq j \longrightarrow (Rs[l]) a \neq \text{Some False} (* \text{no release of unshared address *}) ]</td>
</tr>
</tbody>
</table>

\[ \implies Os, Rs, i \vdash (\text{RMW a t (D,f) cond ret A L R W# is} \varnothing, m, D, O, S) \sqrt{\text{علاقات}} \]

<table>
<thead>
<tr>
<th>RMWWrite:</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ \text{cond } (\theta (t \mapsto m \ a)); a \in O \lor a \in \text{dom } S; \forall j &lt; \text{length } Os. i \neq j \longrightarrow (A \subseteq \text{dom } S \cup O; L \subseteq A; R \subseteq O; A \cap R = {}; a \notin \text{read-only } S] ]</td>
</tr>
</tbody>
</table>

\[ \implies Os, Rs, i \vdash (\text{RMW a t (D,f) cond ret A L R W# is} \varnothing, m, D, O, S) \sqrt{\text{علاقات}} \]

<table>
<thead>
<tr>
<th>Nil:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Os, Rs, i \vdash ([], \varnothing, m, D, O, S) \sqrt{\text{علاقات}}</td>
</tr>
</tbody>
</table>

**lemma memop-safe-delayed-implies-safe-free-flowing:**

**assumes** safe-delayed: Os, Rs, i \vdash (is, \varnothing, m, D, O, S) \sqrt{\text{علامات}}

**shows** Os, i \vdash (is, \varnothing, m, D, O, S) \sqrt{\text{علامات}}

*proof*

**lemma memop-empty-rels-safe-free-flowing-implies-safe-delayed:**

**assumes** safe: Os, i \vdash (is, \varnothing, m, D, O, S) \sqrt{\text{علامات}}

**assumes** empty: \( \forall R \in \text{set } Rs. R = \text{Map.empty} \)

**assumes** leq: \( \text{length } Os = \text{length } Rs \)

**assumes** unowned-shared: \( \forall a. (\forall i < \text{length } Os. a \notin (Os[i]) \longrightarrow a \in \text{dom } S) \)

**assumes** Os-i: Os[i] = O

**shows** Os, Rs, i \vdash (is, \varnothing, m, D, O, S) \sqrt{\text{علامات}}

*proof*

**inductive id-storebuffer-step::**

\( (\text{memory} \times \text{unit} \times \text{owns} \times \text{rels} \times \text{shared}) \Rightarrow (\text{memory} \times \text{unit} \times \text{owns} \times \text{rels} \times \text{shared}) \Rightarrow \text{bool } (- \rightarrow_{I} - [60, 60) 100) \)

**where**

Id: (m, x, O, \text{R}, S) \rightarrow_{I} (m, x, O, \text{R}, S)

**definition empty-storebuffer-step::**\( (\text{memory} \times 'sb \times 'owns \times 'rels \times 'shared) \Rightarrow (\text{memory} \times 'sb \times 'owns \times 'rels \times 'shared) \Rightarrow \text{bool} \)

**where**

empty-storebuffer-step c c' = False

**context** program

**begin**

**abbreviation** direct-concurrent-step ::
(\langle p, \text{unit}, \text{bool}, \text{owns}, \text{rels}, \text{shared} \rangle \Rightarrow (\langle p, \text{unit}, \text{bool}, \text{owns}, \text{rels}, \text{shared} \rangle \Rightarrow \text{bool} \\
(- \Rightarrow_d - [100,60] 100) \\
\text{where} \\
\text{direct-concurrent-step} \equiv \\
\text{computation.concurrent-step} \quad \text{direct-memop-step}. \quad \text{gen-direct-memop-step} \\
\text{empty-storebuffer-step} \quad \text{program-step} \\
(\lambda p \ p' \text{is sb. sb}) \\
\text{abbreviation} \text{direct-concurrent-steps}:: \\
(\langle p, \text{unit}, \text{bool}, \text{owns}, \text{rels}, \text{shared} \rangle \Rightarrow (\langle p, \text{unit}, \text{bool}, \text{owns}, \text{rels}, \text{shared} \rangle \Rightarrow \text{bool} \\
(- \Rightarrow_d^* - [60,60] 100) \\
\text{where} \\
\text{direct-concurrent-steps} \equiv \text{direct-concurrent-step}^{**} \\
\text{abbreviation} \text{virtual-concurrent-step} :: \\
(\langle p, \text{unit}, \text{bool}, \text{owns}, \text{unit}, \text{shared} \rangle \Rightarrow (\langle p, \text{unit}, \text{bool}, \text{owns}, \text{unit}, \text{shared} \rangle \Rightarrow \text{bool} \\
(- \Rightarrow_v - [100,60] 100) \\
\text{where} \\
\text{virtual-concurrent-step} \equiv \\
\text{computation.concurrent-step} \quad \text{virtual-memop-step}. \quad \text{gen-direct-memop-step} \\
\text{empty-storebuffer-step} \quad \text{program-step} \\
(\lambda p \ p' \text{is sb. sb}) \\
\text{abbreviation} \text{virtual-concurrent-steps}:: \\
(\langle p, \text{unit}, \text{bool}, \text{owns}, \text{unit}, \text{shared} \rangle \Rightarrow (\langle p, \text{unit}, \text{bool}, \text{owns}, \text{unit}, \text{shared} \rangle \Rightarrow \text{bool} \\
(- \Rightarrow_v^* - [60,60] 100) \\
\text{where} \\
\text{virtual-concurrent-steps} \equiv \text{virtual-concurrent-step}^{**} \\
\text{term} x \Rightarrow_v Y \\
\text{term} x \Rightarrow_d Y \\
\text{term} x \Rightarrow_d^* Y \\
\text{term} x \Rightarrow_v^* Y \\
\text{end} \\
\text{definition} \\
\text{safe-reach step safe cfg} \equiv \\
\forall \text{cfg'}, \text{step}^{**} \text{cfg cfg'} \longrightarrow \text{safe cfg'} \\
\text{lemma} \text{safe-reach-safe-refl:} \text{safe-reach step safe cfg} \implies \text{safe cfg} \\
(\text{proof})
lemma safe-reach-safe-rtrancl: safe-reach step safe \( \text{cfg} \rightarrow \text{step}^{**} \text{cfg} \rightarrow \text{cfg}' \rightarrow \text{safe} \text{cfg}'

(proof)

lemma safe-reach-steps: safe-reach step safe \( \text{cfg} \rightarrow \text{step}^{**} \text{cfg} \rightarrow \text{cfg}' \rightarrow \text{safe} \text{cfg}'

(proof)

lemma safe-reach-step: safe-reach step safe \( \text{cfg} \rightarrow \text{step} \text{cfg} \rightarrow \text{cfg}' \rightarrow \text{safe} \text{cfg}'

(proof)

context program
begin

abbreviation safe-reach-direct \( \equiv \text{safe-reach direct-concurrent-step} \)

lemma safe-reac-direct-def':
safe-reach-direct safe \( \text{cfg} \equiv \forall \text{cfg}', \text{cfg} \Rightarrow \text{d}^{*} \text{cfg}' \rightarrow \text{safe} \text{cfg}'

(proof)

abbreviation safe-reach-virtual \( \equiv \text{safe-reach virtual-concurrent-step} \)

lemma safe-reac-virtual-def':
safe-reach-virtual safe \( \text{cfg} \equiv \forall \text{cfg}', \text{cfg} \Rightarrow \text{v}^{*} \text{cfg}' \rightarrow \text{safe} \text{cfg}'

(proof)

definition safe-free-flowing \( \text{cfg} \equiv \text{let } (\text{ts}, \text{m}, \text{S}) = \text{cfg} \)
in \( \forall i < \text{length ts}; \text{let } (p, is, \theta, x, D, O, R) = \text{ts!i in map owned ts}, \text{i} \vdash (is, \theta, m, D, O, S) \sqrt{\}) \)

lemma safeE: [safe-free-flowing \( (\text{ts}, m, \text{S}) \); i < length \( \text{ts}; ts!i = (p, is, \theta, x, D, O, R) \)]
\( \Rightarrow \) map owned ts, i \( \vdash (is, \theta, m, D, O, S) \sqrt{\})

(proof)

definition safe-delayed \( \text{cfg} \equiv \text{let } (\text{ts}, m, \text{S}) = \text{cfg} \)
in \( \forall i < \text{length ts}; \text{let } (p, is, \theta, x, D, O, R) = \text{ts!i in map owned ts}, \text{map released ts}, \text{i} \vdash (is, \theta, m, D, O, S) \sqrt{\}) \)

lemma safe-delayedE: [safe-delayed \( (\text{ts}, m, \text{S}) \); i < length \( \text{ts}; ts!i = (p, is, \theta, x, D, O, R) \)]
\( \Rightarrow \) map owned ts, map released ts, i \( \vdash (is, \theta, m, D, O, S) \sqrt{\})

(proof)
**Definition** \( \text{remove-rels} \equiv \text{map} \ (\lambda (p, is, sb, D, O, R). (p, is, \emptyset, sb, D, O, R)) \)

**Theorem (in program) virtual-simulates-direct-step:**
- **Assumes** step: \((ts, m, S) \Rightarrow_d (ts', m', S')\)
- **Shows** \((\text{remove-rels} ts, m, S) \Rightarrow_v (\text{remove-rels} ts', m', S')\)

\[\text{proof}\]

**Lemmas** \(\text{converse-rtranclp-induct-sbh-steps} = \text{converse-rtranclp-induct}\)
- of - \((ts, m, S) (ts', m', S')\), split-rule,
- consumes 1, case-names refl step

**Theorem (in program) virtual-simulates-direct-steps:**
- **Assumes** steps: \((ts, m, S) \Rightarrow_\ast (ts', m', S')\)
- **Shows** \((\text{remove-rels} ts, m, S) \Rightarrow_v \ast (\text{remove-rels} ts', m', S')\)

\[\text{proof}\]

**Locale** simple-ownership-distinct =
- **Fixes** \(ts::(p, sb, \text{dirty}, \text{owns}, \text{rels}) \text{ thread-config list}\)
- **Assumes** simple-ownership-distinct:
  \[\forall i p \text{ is } D O R \text{ sb } \Theta.\]
  \[\forall j < \text{length } ts, j < \text{length } ts, i \neq j.\]
  \[(p, is, \emptyset, sb, D, O, \emptyset) = ts!i;\]
  \[(p, is, \emptyset, sb, D, O, \emptyset) = ts!j;\]
  \[\Rightarrow O_i \cap O_j = \{\}\]

\[\text{proof}\]

**Lemma (in simple-ownership-distinct)**
- **Simple-ownership-distinct-nth-update**:
  \[\forall i p \text{ is } D O R \text{ sb } \Theta.\]
  \[\forall j < \text{length } ts, i \neq j .\]
  \[\Rightarrow (\text{let } (p, is, \emptyset, sb, D, O, \emptyset) = ts!i;\]
  \[\Rightarrow (\text{let } (p, is, \emptyset, sb, D, O, \emptyset) = ts!j;\]
  \[\Rightarrow (O_i' \cap O_j') = \{\}\]

\[\text{proof}\]

**Locale** read-only-unowned =
- **Fixes** \(S::\text{shared} \text{ and } ts::(p, sb, \text{dirty}, \text{owns}, \text{rels}) \text{ thread-config list}\)
- **Assumes** read-only-unowned:
  \[\forall i p \text{ is } D O R \text{ sb } \Theta.\]
  \[\forall j < \text{length } ts, i \neq j, j < \text{length } ts.\]
  \[\Rightarrow (p, is, \emptyset, sb, D, O, \emptyset) = ts!i;\]
  \[\Rightarrow (p, is, \emptyset, sb, D, O, \emptyset) = ts!j;\]
  \[\Rightarrow (O_i' \cap O_j') = \{\}\]

\[\text{proof}\]

**Lemma (in read-only-unowned)**
- **Read-only-unowned-nth-update**:
  \[\forall i p \text{ is } D O R \text{ sb } \Theta.\]
  \[\forall j < \text{length } ts, i \neq j .\]
  \[\Rightarrow (\text{let } (p, is, \emptyset, sb, D, O, \emptyset) = ts!i;\]
  \[\Rightarrow (\text{let } (p, is, \emptyset, sb, D, O, \emptyset) = ts!j;\]
  \[\Rightarrow (S[i := (p, is', \emptyset, sb', D, O, \emptyset)]))\]

\[\text{proof}\]

**Locale** unowned-shared =
fixes \( S::\text{shared} \) and \( \text{ts}::\{p, sb, \text{dirty.owns}, \text{rels}\} \) thread-config list

assumes unowned-shared: \( \bigcup ((\lambda (\cdot, \cdot, \cdot, \cdot, \cdot, O, \cdot). O') \setminus \text{set ts}) \subseteq \text{dom } S \)

lemma (in \( \text{unowned-shared} \))

unowned-shared-nth-update:

assumes i-bound: \( i < \text{length ts} \)

assumes ith: \( \text{ts}!i = (p, is, xs, sb, D, O, R) \)

assumes subset: \( O \subseteq O' \)

shows unowned-shared \( S (\text{ts}[i := (p', is', xs', sb', D', O', R')]) \)

lemma (in \( \text{unowned-shared} \)) a-unowned-by-others-owned-or-shared:

assumes i-bound: \( i < \text{length ts} \)

assumes ts-i: \( \text{ts}!i = (p, is, 0, sb, D, O, R) \)

assumes a-unowned-others:

\[ \forall j < \text{length (map owned ts)}. i \neq j \rightarrow (\text{let } O_j = (\text{map owned ts})!j \text{ in } a \notin O_j) \]

shows \( a \in O \lor a \in \text{dom } S \)

lemma (in \( \text{unowned-shared} \)) unowned-shared':

assumes notin: \( \forall i < \text{length ts}. a \notin \text{owned } (\text{ts}!i) \)

shows \( a \in \text{dom } S \)

lemma unowned-shared-def': unowned-shared \( S \text{ ts} = (\forall a. (\forall i < \text{length ts}. a \notin \text{owned } (\text{ts}!i)) \rightarrow a \in \text{dom } S) \)

definition

initial \( \text{cfg} \equiv \text{let } (\text{ts}, m, S) = \text{cfg} \)

in unowned-shared \( S \text{ ts} \land \)

\( (\forall i < \text{length ts}. \text{let } (p, is, 0, x, D, O, R) = \text{ts}!i \text{ in } \mathcal{R} = \text{Map.empty} ) \)

lemma initial-empty-rels: initial \( (\text{ts}, m, S) \implies \forall \mathcal{R} \in \text{set (map released ts)}. \mathcal{R} = \text{Map.empty} \)

lemma initial-unowned-shared: initial \( (\text{ts}, m, S) \implies \text{unowned-shared } S \text{ ts} \)

lemma initial-safe-free-flowing-implies-safe-delayed:

assumes init: initial \( c \)

assumes safe: safe-safe-free-flowing \( c \)

shows safe-delayed \( c \)

\( \langle \text{proof} \rangle \)
locale program-progress = program +
assumes progress: \(\forall p \rightarrow_p (p',is') \implies p' \neq p \lor is' \neq []\)

The assumption 'progress' could be avoided if we introduce stuttering steps in lemma undo-local-step or make the scheduling of threads explicit, such that we can directly express that 'thread i does not make a step'.

**lemma (in program-progress) undo-local-step:**
assumes step: \((ts,m,S) \Rightarrow_d (ts',m',S')\)
assumes i-bound: \(i < \text{length ts}\)
assumes unchanged: \(ts!i = ts'!i\)
assumes safe-delayed-undo: safe-delayed \((u-ts,u-m,u-shared)\) — proof should also work with weaker safe-free-flowing
assumes leq: \(\text{length } u-ts = \text{length } ts\)
assumes others-same: \(\forall j < \text{length ts}. j \neq i \rightarrow u-ts!j = ts!j\)
assumes u-ts-i: \(u-ts!i=(u-p,u-is,u-tmps,u-x,u-dirty,u-owns,u-rels)\)
assumes u-m-other: \(\forall a \in u-owns \rightarrow u-m a = m a\)
assumes u-m-shared: \(\forall a \in u-owns \rightarrow a \in \text{dom } u-shared \rightarrow u-m a = m a\)
assumes u-shared: \(\forall a \notin u-owns \rightarrow a \notin \text{owned } (ts!i) \rightarrow u-shared a = S a\)
assumes dist: simple-ownership-distinct ts
assumes dist-ts: simple-ownership-distinct ts
shows \(\exists u-ts' \ 'u-shared' u-m'. (u-ts,u-m,u-shared) \Rightarrow_d (u-ts',u-m',u-shared')\)
  — thread i is unchanged
    \(u-ts'!i = u-ts!i\)
    \(\forall a \in u-owns. u-shared' a = u-shared a\)
    \(\forall a \in u-owns. S' a = S a\)
    \(\forall a \in u-owns. u-m' a = u-m a\)
  — other threads are simulated
    \(\forall j < \text{length ts}. j \neq i \rightarrow u-ts'!j = ts'!j\)
    \(\forall a \notin u-owns \rightarrow a \notin \text{owned } (ts!i) \rightarrow u-shared' a = S' a\)
⟨proof⟩

**theorem (in program) safe-step-preserves-simple-ownership-distinct:**
assumes step: \((ts,m,S) \Rightarrow_d (ts',m',S')\)
assumes safe: safe-delayed \((ts,m,S)\)
assumes dist: simple-ownership-distinct ts
shows simple-ownership-distinct ts'
⟨proof⟩

**theorem (in program) safe-step-preserves-read-only-unowned:**
assumes step: \((ts,m,S) \Rightarrow_d (ts',m',S')\)
assumes safe: safe-delayed \((ts,m,S)\)
assumes dist: simple-ownership-distinct ts
assumes ro-unowned: read-only-unowned \(S\) ts
shows read-only-unowned \(S'\) ts'
⟨proof⟩

**theorem (in program) safe-step-preserves-unowned-shared:**

45
assumes step: \((ts, m, S) \Rightarrow_d (ts', m', S')\)
assumes safe: safe-delayed \((ts, m, S)\)
assumes dist: simple-ownership-distinct \(ts\)
assumes unowned-shared: unowned-shared \(S\) \(ts\)
says unowned-shared \(S'\) \(ts'\)

\(\langle proof\rangle\)

locale program-trace = program +
fixes \(c\) — enumeration of configurations:
\(c\) \(n\) \(\Rightarrow_d c\) \((n + 1)\) \(\ldots \Rightarrow_d c\) \((n + k)\)
fixes \(n::nat\) — starting index
fixes \(k::nat\) — steps

assumes step: \(\forall l. 1 < k \implies c\) \((n+l)\) \(\Rightarrow_d c\) \((n + (Suc\ l))\)

abbreviation \((in\ program)\)
\(trace \equiv program-trace\) program-step

lemma \((in\ program)\) trace-0 [simp]: \(trace\ c\ n\ 0\)
\(\langle proof\rangle\)

lemma split-less-Suc: \((\forall x < Suc\ k. P\ x) = (P\ k \land (\forall x < k. P\ x))\)
\(\langle proof\rangle\)

lemma split-le-Suc: \((\forall x \leq Suc\ k. P\ x) = (P\ (Suc\ k) \land (\forall x \leq k. P\ x))\)
\(\langle proof\rangle\)

lemma \((in\ program)\) steps-to-trace:
assumes steps: \(x \Rightarrow_d y\)
shows \(\exists c\ k. \, trace\ c\ 0\ k \land c\ 0 = x \land c\ k = y\)
\(\langle proof\rangle\)

lemma \((in\ program)\) trace-preserves-length-ts:
\(\forall l. x. \, trace\ c\ n\ k \implies l \leq k \implies x \leq k \implies length\ (fst\ (c\ (n + l))) = length\ (fst\ (c\ (n + x)))\)
\(\langle proof\rangle\)

lemma \((in\ program)\) trace-preserves-simple-ownership-distinct:
assumes dist: simple-ownership-distinct \((fst\ (c\ n))\)
shows \(\forall l. \, trace\ c\ n\ k \implies (\forall x < k. \, safe-delayed\ (c\ (n + x))) \implies l \leq k \implies simple-ownership-distinct\ (fst\ (c\ (n + l)))\)
\(\langle proof\rangle\)

lemma \((in\ program)\) trace-preserves-read-only-unowned:
assumes dist: simple-ownership-distinct \((fst\ (c\ n))\)
assumes ro: read-only-unowned \((snd\ (snd\ (c\ n)))\) \((fst\ (c\ n))\)
shows \(\forall l. \, trace\ c\ n\ k \implies (\forall x < k. \, safe-delayed\ (c\ (n + x))) \implies l \leq k \implies read-only-unowned\ (snd\ (snd\ (c\ (n + l))))\) \((fst\ (c\ (n + l)))\)
\(\langle proof\rangle\)
lemma (in program) trace-preserves-unowned-shared:
assumes dist: simple-ownership-distinct (fst (c n))
assumes ro: unowned-shared (snd (snd (c n))) (fst (c n))
shows \( \forall l. \) trace c n k \( \implies \) (\( \forall x < k. \) safe-delayed (c (n + x))) \( \implies \)
\( l \leq k \implies \) unowned-shared (snd (snd (c (n + l)))) (fst (c (n + l)))))
⟨proof⟩

theorem (in program-progress) undo-local-steps:
assumes steps: trace c n k
assumes c-n: c n = (ts, m, S)
assumes unchanged: \( \forall l \leq k. \) (\( \forall x < k. \) (\( \forall x \leq l. \) length (fst (c (n + x)))) = length (fst (c (n + x))))
assumes leq: length u-ts = length ts
assumes i-bound: i < length ts
assumes others-same: \( \forall j < l. \) u-ts!j = ts!j
assumes u-ts-i: u-ts!i = (u-p, u-is, u-tmps, u-sb, u-dirty, u-rels)
assumes u-m-other: \( \forall a. a \not\in u-owns \implies u-m a = m a \)
assumes u-m-shared: \( \forall a. a \in u-owns \implies a \in \text{dom} u-shared \implies u-m a = m a \)
assumes u-shared: \( \forall a. a \not\in u-owns \implies a \not\in \text{owned} (ts!i) \implies u-shared a = S a \)
assumes dist: simple-ownership-distinct u-ts
assumes dist-ts: simple-ownership-distinct ts
assumes safe-orig: \( \forall x. \) x < k \( \implies \) safe-delayed (c (n + x))
shows \( \exists c' l. \) l \( \leq k \land \) trace c' n l \land
\( \forall x \leq l. \) length (fst (c' (n + x))) = length (fst (c (n + x)))
\( \forall x < l. \) Safe-Delayed (c' (n + x))
\( \forall x \leq l. \) Safe-Delayed (c' (n + x))
\( \forall x \leq l. \) Safe-Delayed (c' (n + x))
\( \forall x \leq l. \) Safe-Delayed (c' (n + x))
⟨proof⟩

locale program-safe-reach-upto = program +
fixes n fixes safe fixes c0

47
assumes safe-config: $[k \leq n; \text{trace } c \ 0 \ k; \ c \ 0 = c_0; \ 1 \leq k \ ] \implies \text{safe } (c \ 1)$

abbreviation (in program)
safe-reach-upto \equiv \text{program-safe-reach-upto program-step}

lemma (in program) safe-reach-upto-le:
assumes safe: safe-reach-upto n safe c_0
assumes m-n: $m \leq n$
shows safe-reach-upto m safe c_0
⟨proof⟩

lemma (in program) last-action-of-thread:
assumes trace: trace c 0 k
shows — thread i never executes
$(\forall l \leq k. \ \text{fst } (c \ l)!i = \text{fst } (c \ k)!i) \ \lor$
— thread i has a last step in the trace
$(\exists \text{last } < k.
\ \text{fst } (c \ \text{last})!i \neq \text{fst } (c \ (\text{Suc last}))!i \ \land
\ (\forall l. \ \text{last } < l \implies l \leq k \implies \text{fst } (c \ l)!i = \text{fst } (c \ k)!i))$
⟨proof⟩

lemma (in program) sequence-traces:
assumes trace1: trace c_1 0 k
assumes trace2: trace c_2 m l
assumes seq: $c_2 \ m = c_1 \ k$
assumes c-def: $c = (\lambda x. \ \text{if } x \leq k \ \text{then } c_1 \ x \ \text{else } (c_2 \ (m + x - k)))$
shows trace c 0 (k + l)
⟨proof⟩

theorem (in program-progress) safe-free-flowing-implies-safe-delayed:
assumes init: initial c_0
assumes dist: simple-ownership-distinct (fst c_0)
assumes read-only-unowned: read-only-unowned (snd (snd c_0)) (fst c_0)
assumes unowned-shared: unowned-shared (snd (snd c_0)) (fst c_0)
assumes safe-reach-ff: safe-reach-upto n safe-free-flowing c_0
shows safe-reach-upto n safe-delayed c_0
⟨proof⟩

datatype ′p memref =
  Write_{sb} bool addr sop val acq lcl rel wrt
| Read_{sb} bool addr tmp val
| Prog_{sb} ′p ′p instrs
| Ghost_{sb} acq lcl rel wrt

type-synonym ′p store-buffer = ′p memref list
inductive flush-step:: memory \times ′p store-buffer \times owns \times rels \times shared \Rightarrow memory \times ′p store-buffer \times owns \times rels \times shared \Rightarrow bool
(- → t - [60,60] 100)
where
Write\textsb\[O′ = (if \text{volatile} then O ∪ A − R else O);\]
  \[S′ = (if \text{volatile} then S ⊕ W R ⊖ A L else S);\]
  \[R′ = if \text{volatile then Map.empty else R}]\]
⇒

(m, Write\textsb\(a\) volatile a sop v A L R W# rs, O, R, S) \→ \(m(a := v), rs, O′, R′, S′\)
| Read\textsb\[a\] (m, Read\textsb\(a\) volatile a t v#rs, O, R, S) \→ \(m, rs, O, R, S\)
| Prog\textsb\(a\) (m, Prog\textsb\(a\) p p’ is#rs, O, R, S) \→ \(m, rs, O, R, S\)
| Ghost (m, Ghost\textsb\(a\) A L R W# rs, O, R, S) \→ \(m, rs, O ∪ A − R, \text{augment-rels (dom } S)\)
R, R, S ⊕ W R ⊖ A L)

abbreviation flush-steps::memory × ’p store-buffer × owns × rels × shared ⇒ memory × ’p store-buffer × owns × rels × shared ⇒ bool
(- \→ \* - [60,60] 100)
where
flush-steps == flush-step˘**

term x \→ \* Y

lemmas flush-step-induct =
flush-step.induct [split-format (complete), consumes 1, case-names Write\textsb\ Read\textsb\ Read\textsb\ Prog\textsb\ Ghost]

inductive store-buffer-step:: memory × ’p store-buffer × owns × rels × ’shared ⇒ memory × ’p memref list × ’owns × ’rels × ’shared ⇒ bool
(- \→ \w\* - [60,60] 100)
where
SBWrite\textsb\:
(m, Write\textsb\ volatile a sop v A L R W# rs, O, R, S) \→ \w\(m(a := v), rs, O, R, S\)

abbreviation store-buffer-steps::memory × ’p store-buffer × ’owns × ’rels × ’shared ⇒ memory × ’p store-buffer × ’owns × ’rels × ’shared ⇒ bool
(- \→ \w\* - [60,60] 100)
where
store-buffer-steps == store-buffer-step˘**

term x \→ \w\* Y

fun buffered-val :: ’p memref list ⇒ addr ⇒ val option
where
| buffered-val [] a = None
| buffered-val (r # rs) a’ =
  (case r of
   Write\textsb\ volatile a - v - - - ⇒ (case buffered-val rs a’ of
      None ⇒ (if a’=a then Some v else None)
      | Some v’ ⇒ Some v’)
  - ⇒ buffered-val rs a’)

definition address-of :: ’p memref ⇒ addr set
where
address-of \( r = (\text{case } r \text{ of } \text{Write}_{sb} \text{ volatile } a \cdot v \cdot - - - \Rightarrow \{a\} \mid \text{Read}_{sb} \text{ volatile } a \cdot t \cdot v \Rightarrow \{a\} \mid - \Rightarrow \{\}) \)

**lemma** address-of-simps [simp]:
address-of (\text{Write}_{sb} \text{ volatile } a \cdot s \cdot v \cdot A \cdot L \cdot R \cdot W) = \{a\}
address-of (\text{Read}_{sb} \text{ volatile } a \cdot t \cdot v) = \{a\}
address-of (\text{Prog}_{sb} \text{ p } p' \text{ is}) = \{}
address-of (\text{Ghost}_{sb} \text{ A } L \cdot R \cdot W) = \{}

(proof)

**definition** is-volatile :: 'p memref \(\Rightarrow\) bool

**where**
is-volatile \( r = (\text{case } r \text{ of } \text{Write}_{sb} \text{ volatile } a \cdot v \cdot - - - \Rightarrow \text{volatile} \mid \text{Read}_{sb} \text{ volatile } a \cdot t \cdot v \Rightarrow \text{volatile} \mid - \Rightarrow \text{False}) \)

**lemma** is-volatile-simps [simp]:
is-volatile (\text{Write}_{sb} \text{ volatile } a \cdot s \cdot v \cdot A \cdot L \cdot R \cdot W) = \text{volatile}
is-volatile (\text{Read}_{sb} \text{ volatile } a \cdot t \cdot v) = \text{volatile}
is-volatile (\text{Prog}_{sb} \text{ p } p' \text{ is}) = \text{False}
is-volatile (\text{Ghost}_{sb} \text{ A } L \cdot R \cdot W) = \text{False}

(proof)

**definition** is-Writesb :: 'p memref \(\Rightarrow\) bool

**where**
is-Write_{sb} \( r = (\text{case } r \text{ of } \text{Write}_{sb} \text{ volatile } a \cdot v \cdot - - - \Rightarrow \text{True} \mid - \Rightarrow \text{False}) \)

**definition** is-Readsb :: 'p memref \(\Rightarrow\) bool

**where**
is-Read_{sb} \( r = (\text{case } r \text{ of } \text{Read}_{sb} \text{ volatile } a \cdot t \cdot v \Rightarrow \text{True} \mid - \Rightarrow \text{False}) \)

**definition** is-Progsb :: 'p memref \(\Rightarrow\) bool

**where**
is-Prog_{sb} \( r = (\text{case } r \text{ of } \text{Prog}_{sb} \cdot - - - \Rightarrow \text{True} \mid - \Rightarrow \text{False}) \)

**definition** is-Ghostsb :: 'p memref \(\Rightarrow\) bool

**where**
is-Ghost_{sb} \( r = (\text{case } r \text{ of } \text{Ghost}_{sb} \cdot - - - \Rightarrow \text{True} \mid - \Rightarrow \text{False}) \)

**lemma** is-Write_{sb}-simps [simp]:
is-Write_{sb} (\text{Write}_{sb} \text{ volatile } a \cdot s \cdot v \cdot A \cdot L \cdot R \cdot W) = \text{True}
is-Write_{sb} (\text{Read}_{sb} \text{ volatile } a \cdot t \cdot v) = \text{False}
is-Write_{sb} (\text{Prog}_{sb} \text{ p } p' \text{ is}) = \text{False}
is-Write_{sb} (\text{Ghost}_{sb} \text{ A } L \cdot R \cdot W) = \text{False}

(proof)

**lemma** is-Read_{sb}-simps [simp]:
is-Read_{sb} (\text{Read}_{sb} \text{ volatile } a \cdot t \cdot v) = \text{True}
is-Read_{sb} (\text{Write}_{sb} \text{ volatile } a \cdot s \cdot v \cdot A \cdot L \cdot R \cdot W) = \text{False}
is-Read_{sb} (\text{Prog}_{sb} \text{ p } p' \text{ is}) = \text{False}
\(\text{is-Read}_{sb} (\text{Ghost}_{sb} A L R W) = \text{False} \)

(proof)

\textbf{lemma} is-Prog\(_{sb}\)-simps [simp]:
\begin{align*}
\text{is-Prog}_{sb} (\text{Read}_{sb} \text{ volatile a t v}) &= \text{False} \\
\text{is-Prog}_{sb} (\text{Write}_{sb} \text{ volatile a sop v A L R W}) &= \text{False} \\
\text{is-Prog}_{sb} (\text{Prog}_{sb} p p' \text{ is}) &= \text{True} \\
\text{is-Prog}_{sb} (\text{Ghost}_{sb} A L R W) &= \text{False}
\end{align*}

(proof)

\textbf{definition} is-volatile-Write\(_{sb}\):: \(p \ \text{memref} \Rightarrow \text{bool} \)
where
\begin{align*}
\text{is-volatile-Write}_{sb} r &= (\text{case } r \text{ of } \text{Write}_{sb} \text{ volatile a - v - - - - - - - } \Rightarrow \text{volatile } | \ - \Rightarrow \text{False})
\end{align*}

\textbf{lemma} is-volatile-Write\(_{sb}\)-simps [simp]:
\begin{align*}
\text{is-volatile-Write}_{sb} (\text{Write}_{sb} \text{ volatile a sop v A L R W}) &= \text{volatile} \\
\text{is-volatile-Write}_{sb} (\text{Read}_{sb} \text{ volatile a t v}) &= \text{False} \\
\text{is-volatile-Write}_{sb} (\text{Prog}_{sb} p p' \text{ is}) &= \text{False} \\
\text{is-volatile-Write}_{sb} (\text{Ghost}_{sb} A L R W) &= \text{False}
\end{align*}

(proof)

\textbf{definition} is-volatile-Read\(_{sb}\):: \(p \ \text{memref} \Rightarrow \text{bool} \)
where
\begin{align*}
\text{is-volatile-Read}_{sb} r &= (\text{case } r \text{ of } \text{Read}_{sb} \text{ volatile a t v } \Rightarrow \text{volatile } | \ - \Rightarrow \text{False})
\end{align*}

\textbf{lemma} is-volatile-Read\(_{sb}\)-address-of [simp]: is-volatile-Read\(_{sb}\) \(x \Rightarrow \) address-of \(x \neq \emptyset\)

(proof)

\textbf{definition} is-non-volatile-Write\(_{sb}\):: \(p \ \text{memref} \Rightarrow \text{bool} \)
where
\begin{align*}
\text{is-non-volatile-Write}_{sb} r &= (\text{case } r \text{ of } \text{Write}_{sb} \text{ volatile a t v } \Rightarrow \text{volatile } | \ - \Rightarrow \text{False})
\end{align*}

\textbf{lemma} is-non-volatile-Write\(_{sb}\)-simps [simp]:
\begin{align*}
\text{is-non-volatile-Write}_{sb} (\text{Write}_{sb} \text{ volatile a sop v A L R W}) &= (\neg \text{volatile}) \\
\text{is-non-volatile-Write}_{sb} (\text{Prog}_{sb} p p' \text{ is}) &= \text{False} \\
\text{is-non-volatile-Write}_{sb} (\text{Ghost}_{sb} A L R W) &= \text{False}
\end{align*}

(proof)
is-non-volatile-Write_{sb} (\text{Ghost}_{sb} A L R W) = \text{False}

\langle \text{proof} \rangle

\textbf{definition} \ is-non-volatile-Read_{sb} :: \ 'p \ \text{memref} \Rightarrow \text{bool}
\textbf{where}
is-non-volatile-Read_{sb} r = (\text{case } r \text{ of } \text{Read}_{sb} \text{ volatile } a t v \Rightarrow \neg \text{volatile} | - \Rightarrow \text{False})

\textbf{lemma} \ is-non-volatile-Read_{sb}-\text{sims} \ [\text{simp}]:
is-non-volatile-Read_{sb} (\text{Read}_{sb} \text{ volatile } a t v) = (\neg \text{volatile})
is-non-volatile-Read_{sb} (\text{Write}_{sb} \text{ volatile } a \text{ sop } v A L R W) = \text{False}
is-non-volatile-Read_{sb} (\text{Prog}_{sb} p p' is) = \text{False}
is-non-volatile-Read_{sb} (\text{Ghost}_{sb} A L R W) = \text{False}
\langle \text{proof} \rangle

\textbf{lemma} \ is-volatile-split: \ is-volatile r =
is-volatile-Read_{sb} r \lor \text{is-volatile-Write}_{sb} r
\langle \text{proof} \rangle

\textbf{lemma} \ is-non-volatile-split:
\neg \ is-volatile r = (\text{is-non-volatile-Read}_{sb} r \lor \text{is-non-volatile-Write}_{sb} r \lor \text{is-Prog}_{sb} r \lor \text{is-Ghost}_{sb} r)
\langle \text{proof} \rangle

\textbf{fun} \ \text{outstanding-refs}:: (\ 'p \ \text{memref} \Rightarrow \text{bool}) \Rightarrow \ 'p \ \text{memref} \ \text{list} \Rightarrow \text{addr set}
\textbf{where}
\text{outstanding-refs } P [\ ] = \{\}
| \text{outstanding-refs } P (r#rs) = (\text{if } P r \text{ then } (\text{address-of } r) \cup (\text{outstanding-refs } P rs) \\
| \text{else } \text{outstanding-refs } P rs)

\textbf{lemma} \ \text{outstanding-refs-conv}: \text{outstanding-refs } P \ \text{sb} = \bigcup (\text{address-of } ' \{r. \ r \in \text{set sb} \land P r\})
\langle \text{proof} \rangle

\textbf{lemma} \ \text{outstanding-refs-append}:
\forall ys. \text{outstanding-refs } \text{vol } (xs@ys) = \text{outstanding-refs } \text{vol } xs \cup \text{outstanding-refs } \text{vol } ys
\langle \text{proof} \rangle

\textbf{lemma} \ \text{outstanding-refs-empty-negate}: \ (\text{outstanding-refs } P \ \text{sb} = \{\}) \implies
(\text{outstanding-refs } (\text{Not } \circ P) \ \text{sb} = \bigcup (\text{address-of } ' \ \text{set sb}))
\langle \text{proof} \rangle

\textbf{lemma} \ \text{outstanding-refs-mono-pred}:
\forall sb sb'.
\forall r. P r \rightarrow P' r \implies \text{outstanding-refs } P \ \text{sb} \subseteq \text{outstanding-refs } P' \ \text{sb}
\langle \text{proof} \rangle

\textbf{lemma} \ \text{outstanding-refs-mono-set}:
\forall sb sb'.
set sb \subseteq set sb' \implies \text{outstanding-refs P sb} \subseteq \text{outstanding-refs P sb}'

\textit{proof}

\textbf{lemma} outstanding-refs-takeWhile:
\text{outstanding-refs P (takeWhile P' sb)} \subseteq \text{outstanding-refs P sb}

\textit{proof}

\textbf{lemma} outstanding-refs-subsets:
\text{outstanding-refs is-volatile-Write \_sb sb} \subseteq \text{outstanding-refs is-Write \_sb sb}
\text{outstanding-refs is-non-volatile-Write \_sb sb} \subseteq \text{outstanding-refs is-Write \_sb sb}

\text{outstanding-refs is-volatile-Read \_sb sb} \subseteq \text{outstanding-refs is-Read \_sb sb}
\text{outstanding-refs is-non-volatile-Read \_sb sb} \subseteq \text{outstanding-refs is-Read \_sb sb}

\text{outstanding-refs is-volatile-Write \_sb sb} \subseteq \text{outstanding-refs (Not o is-volatile) sb}
\text{outstanding-refs is-non-volatile-Write \_sb sb} \subseteq \text{outstanding-refs (Not o is-volatile) sb}

\text{outstanding-refs is-volatile-Read \_sb sb} \subseteq \text{outstanding-refs (is-volatile) sb}
\text{outstanding-refs is-non-volatile-Read \_sb sb} \subseteq \text{outstanding-refs (is-volatile) sb}

\text{outstanding-refs is-non-volatile-Write \_sb sb} \subseteq \text{outstanding-refs (Not o is-volatile-Write \_sb sb)}
\text{outstanding-refs is-non-volatile-Read \_sb sb} \subseteq \text{outstanding-refs (Not o is-volatile-Write \_sb sb)}

\text{outstanding-refs is-volatile-Read \_sb sb} \subseteq \text{outstanding-refs (Not o is-volatile-Write \_sb sb)}
\text{outstanding-refs is-non-volatile-Read \_sb sb} \subseteq \text{outstanding-refs (Not o is-volatile-Write \_sb sb)}

\textbf{proof}

\textbf{lemma} outstanding-non-volatile-refs-conv:
\text{outstanding-refs (Not o is-volatile) sb} =
\text{outstanding-refs is-non-volatile-Write \_sb sb} \cup \text{outstanding-refs is-non-volatile-Read \_sb sb}

\textit{proof}

\textbf{lemma} outstanding-volatile-refs-conv:
\text{outstanding-refs is-volatile sb} =
\text{outstanding-refs is-volatile-Write \_sb sb} \cup \text{outstanding-refs is-volatile-Read \_sb sb}

\textit{proof}

\textbf{lemma} outstanding-is-Write \_sb-ref-refs-conv:
\text{outstanding-refs is-Write \_sb sb} =
\text{outstanding-refs is-non-volatile-Write \_sb sb} \cup \text{outstanding-refs is-volatile-Write \_sb sb}

\textit{proof}

\textbf{lemma} outstanding-is-Read \_sb-ref-refs-conv:
\text{outstanding-refs is-Read \_sb sb} =
\text{outstanding-refs is-non-volatile-Read \_sb sb} \cup \text{outstanding-refs is-volatile-Read \_sb sb}

\textit{proof}
lemma outstanding-not-volatile-Read_{sb}-refs-conv: outstanding-refs \{(\text{Not } \circ \text{is-volatile-Read}_{sb})\sb\} = 
outstanding-refs \text{is-Write}_{sb} \sb \cup \text{outstanding-refs is-non-volatile-Read}_{sb} \sb
⟨proof⟩

lemmas misc-outstanding-refs-convs = outstanding-non-volatile-refs-conv
outstanding-volatile-refs-conv
outstanding-is-Write_{sb}-refs-conv
outstanding-not-volatile-Read_{sb}-refs-conv

lemma no-outstanding-vol-write-takeWhile-append: outstanding-refs \text{is-volatile-Write}_{sb} \sb = \{\} \implies 
takeWhile (\text{Not } \circ \text{is-volatile-Write}_{sb}) (\sb@xs) = \sb@(\text{takeWhile } (\text{Not } \circ \text{is-volatile-Write}_{sb}) \xs)
⟨proof⟩

lemma outstanding-vol-write-takeWhile-append: outstanding-refs \text{is-volatile-Write}_{sb} \sb \neq \{\} \implies 
takeWhile (\text{Not } \circ \text{is-volatile-Write}_{sb}) (\sb@xs) = (\text{takeWhile } (\text{Not } \circ \text{is-volatile-Write}_{sb}) \sb)@xs 
⟨proof⟩

lemma no-outstanding-vol-write-dropWhile-append: outstanding-refs \text{is-volatile-Write}_{sb} \sb = \{\} \implies 
dropWhile (\text{Not } \circ \text{is-volatile-Write}_{sb}) (\sb@xs) = (\text{dropWhile } (\text{Not } \circ \text{is-volatile-Write}_{sb}) \xs)
⟨proof⟩

lemma outstanding-vol-write-dropWhile-append: outstanding-refs \text{is-volatile-Write}_{sb} \sb \neq \{\} \implies 
dropWhile (\text{Not } \circ \text{is-volatile-Write}_{sb}) (\sb@xs) = (\text{dropWhile } (\text{Not } \circ \text{is-volatile-Write}_{sb}) \sb)@xs 
⟨proof⟩

lemmas outstanding-vol-write-take-drop-appends = 
no-outstanding-vol-write-takeWhile-append
outstanding-vol-write-takeWhile-append
no-outstanding-vol-write-dropWhile-append
outstanding-vol-write-dropWhile-append

lemma outstanding-refs-is-non-volatile-Write_{sb}-takeWhile-conv: 
outstanding-refs \text{is-non-volatile-Write}_{sb} (\text{takeWhile } (\text{Not } \circ \text{is-volatile-Write}_{sb}) \sb) = 
outstanding-refs \text{is-Write}_{sb} (\text{takeWhile } (\text{Not } \circ \text{is-volatile-Write}_{sb}) \sb)
⟨proof⟩

lemma dropWhile-not-vol-write-empty:
outstanding-refs is-volatile-Write_{sb} \{\} \Rightarrow (\text{dropWhile} (\text{Not} \circ \text{is-volatile-Write}_{sb}) \sb) = []

\langle \text{proof} \rangle

\textbf{lemma} \ \text{takeWhile-not-vol-write-outstanding-refs}:
outstanding-refs is-volatile-Write_{sb} (\text{takeWhile} (\text{Not} \circ \text{is-volatile-Write}_{sb}) \sb) = \{\}

\langle \text{proof} \rangle

\textbf{lemma} \ \text{no-volatile-Write}_{sb}s-conv: (\text{outstanding-refs is-volatile-Write}_{sb} \sb = \{\}) = 
(\forall r \in \text{set} \sb. (\forall v' \text{ sop}' a' A L R W. r \neq \text{Write}_{sb} \text{ True} a' \text{ sop}' v' A L R W))

\langle \text{proof} \rangle

\textbf{lemma} \ \text{no-volatile-Read}_{sb}s-conv: (\text{outstanding-refs is-volatile-Read}_{sb} \sb = \{\}) = 
(\forall r \in \text{set} \sb. (\forall v' \text{ t}' a'. r \neq \text{Read}_{sb} \text{ True} a' \text{ t}' v'))

\langle \text{proof} \rangle

\textbf{inductive} \ \text{sb-memop-step} :: (\text{instrs} \times \text{tmps} \times 'p \text{ store-buffer} \times \text{memory} \times 'd \text{irty} \times 'o \text{wns} \times 'rels \times 's \text{hared } ) \Rightarrow 
(\text{instrs} \times \text{tmps} \times 'p \text{ store-buffer} \times \text{memory} \times 'd \text{irty} \times 'o \text{wns} \times 'rels \times 's \text{hared } ) \Rightarrow \text{bool}
(- \rightarrow_{sb} - [60,60] 100)

\textbf{where}

\text{SBReadBuffered}:
[\text{buffered-val} \ sb \ a = \text{Some} \ v] 
\Rightarrow 
(\text{Read} \text{ volatile} \ a \ t \ # \ is, \bar{d}, \sb, \m, \text{O}, \text{R}, \text{S}) \rightarrow_{sb} 
(is, \bar{d} (t \mapsto v), \sb, \m, \text{D}, \text{O}, \text{R}, \text{S})

| \text{SBReadUnbuffered}:
[\text{buffered-val} \ sb \ a = \text{None}]
\Rightarrow 
(\text{Read} \text{ volatile} \ a \ t \ # \ is, \bar{d}, \sb, \m, \text{D}, \text{O}, \text{R}, \text{S}) \rightarrow_{sb}
(is, \bar{d} (t \mapsto m a), \sb, \m, \text{D}, \text{O}, \text{R}, \text{S})

| \text{SBWriteNonVolatile}:
(\text{Write} \text{ False} \ a (\text{D},f) A L R W \# \text{is}, \bar{d}, \sb, \m, \text{D}, \text{O}, \text{R}, \text{S}) \rightarrow_{sb}
(is, \bar{d}, \sb @ [\text{Write}_{sb} \text{ False} \ a (\text{D},f) (f \bar{d}) A L R W], \m, \text{D}, \text{O}, \text{R}, \text{S})

| \text{SBWriteVolatile}:
(\text{Write} \text{ True} \ a (\text{D},f) A L R W \# \text{is}, \bar{d}, \sb, \m, \text{D}, \text{O}, \text{R}, \text{S}) \rightarrow_{sb}
(is, \bar{d}, \sb @ [\text{Write}_{sb} \text{ True} \ a (\text{D},f) (f \bar{d}) A L R W], \m, \text{D}, \text{O}, \text{R}, \text{S})

| \text{SBFence}:
(\text{Fence} \ # \ is, \bar{d}, [], \m, \text{D}, \text{O}, \text{R}, \text{S}) \rightarrow_{sb} (is, \bar{d}, [], \m, \text{D}, \text{O}, \text{R}, \text{S})

| \text{SBRMWReadOnly}:
[\neg \text{ cond} (\bar{d}(t \mapsto m a))] \Rightarrow
(RMW a t (D,f) cond ret A L R W# is, $\emptyset$, $\emptyset$, m,D, O, R, S) $\xrightarrow{s_b}$ (is, $\emptyset(t\rightarrow m a)$, m,D, O, R, S)

| SBRMWWrite:  
| $\left[\text{cond } (\emptyset(t\rightarrow m a))\right] \implies$  
| (RMW a t (D,f) cond ret A L R W# is, $\emptyset$, m,D, O, R, S) $\xrightarrow{s_b}$  
| (is, $\emptyset(t\rightarrow \text{ret } (m a))$ (f(\$\emptyset(t\rightarrow m a))))$, m(a:= f(\$\emptyset(t\rightarrow m a)))$, D, O, R, S)  

| SBGhost:  
| (Ghost A L R W# is, $\emptyset$, $\emptyset$ m,D, O, R, S) $\xrightarrow{s_b}$  
| (is, $\emptyset$, sb, m,D, O, R, S)

**inductive** sbh-memop-step ::  

| (intrs $\times$ tmps $\times$ $\{\text{store-buffer} \times \text{memory} \times \text{bool} \times \text{owns} \times \text{rels} \times \text{shared}\}) \Rightarrow$  
| (bool $\neg \xrightarrow{s_{\text{bh}}} [60, 60] 100$)

**where**  

| SBHReadBuffered:  
| [buffered-val sb a = Some v]  
| $\implies$  
| (Read volatile a t # is, $\emptyset$, sb, m, D, O, R, S) $\xrightarrow{s_{\text{bh}}}$  
| (is, $\emptyset$ (t$\rightarrow$m a), sb@[Read_{sb} \text{volatile } a$ t v], m, D, O, R, S)

| SBHReadUnbuffered:  
| [buffered-val sb a = None]  
| $\implies$  
| (Read volatile a t # is, $\emptyset$, sb, m, D, O, R, S) $\xrightarrow{s_{\text{bh}}}$  
| (is, $\emptyset$ (t$\rightarrow$m a), sb@[Read_{sb} \text{volatile } a$ t (m a)], m, D, O, R, S)

| SBHWriteNonVolatile:  
| (Write False a (D,f) A L R W#is, $\emptyset$, sb, m, D, O, R, S) $\xrightarrow{s_{\text{bh}}}$  
| (is, $\emptyset$, sb@[Write_{sb} False a (D,f) (f $\emptyset$) A L R W], m, D, O, R, S)

| SBHWriteVolatile:  
| (Write True a (D,f) A L R W# is, $\emptyset$, sb, m, D, O, R, S) $\xrightarrow{s_{\text{bh}}}$  
| (is, $\emptyset$, sb@[Write_{sb} True a (D,f) (f $\emptyset$) A L R W], m, True, O, R, S)

| SBHFence:  
| (Fence # is, $\emptyset$, $\emptyset$, m, D, O, R, S) $\xrightarrow{s_{\text{bh}}}$ (is, $\emptyset$, $\emptyset$, m, False, O, Map.empty, S)

| SBHRMWRReadOnly:  
| $\neg \text{ cond } (\emptyset(t\rightarrow m a)) \implies$  
| (RMW a t (D,f) cond ret A L R W# is, $\emptyset$, $\emptyset$, m, D, O, R, S) $\xrightarrow{s_{\text{bh}}}$ (is, $\emptyset(t\rightarrow m a)$, $\emptyset$, m, False, O, Map.empty, S)

| SBHRMWWrite:  
| [cond (\$\emptyset(t\rightarrow m a))] \implies$  

56
\[(\text{RMW} a t (D,f) \text{ cond ret } A L R W\# \text{ is, } \emptyset, [], m, D, O, R, S) \rightarrow_{sbh}
\]
\[(\text{is, } \emptyset(t\rightarrow\text{ret} (m a)) f((\emptyset(t\rightarrow m a))), [], m(a:= f((\emptyset(t\rightarrow m a))))) \text{, False, } O \cup A \rightarrow R, \text{Map.empty, } S \oplus_{W} R \ominus_{A} L)\]

\text{SBHGhost:}
\[(\text{Ghost } A L R W\# \text{ is, } \emptyset, \text{sb, } m, D, O, R, S) \rightarrow_{sbh}
\]
\[\text{is, } \emptyset, \text{sb}(\text{Ghost}_{sb} A L R W] m, D, O, R, S)]\]

\text{interpretation} direct: memory-system direct-memop-step id-storebuffer-step \text{ (proof)}
\text{interpretation} sb: memory-system sb-memop-step store-buffer-step \text{ (proof)}
\text{interpretation} sbh: memory-system sbh-memop-step flush-step \text{ (proof)}

primrec non-volatile-owned-or-read-only:: bool \Rightarrow shared \Rightarrow owns \Rightarrow 'a memref list \Rightarrow bool
\text{where}
non-volatile-owned-or-read-only pending-write S O [] = True
| non-volatile-owned-or-read-only pending-write S O (x#xs) =
\[(\text{case } x \text{ of}
\]
Read_{sb} volatile a t v \Rightarrow
\[
(\neg \text{volatile } \rightarrow \text{pending-write } \rightarrow (a \in O \lor a \in \text{read-only } S)) \land
\]
non-volatile-owned-or-read-only pending-write S O xs
| Write_{sb} volatile a sop v A L R W \Rightarrow
\[(\text{if volatile then non-volatile-owned-or-read-only True } (S \oplus_{W} R \ominus_{A} L) (O \cup A \rightarrow R) \text{ xs}
\]
\[
\text{else } a \in O \land \text{non-volatile-owned-or-read-only pending-write } S O \text{ xs}
| Ghost_{sb} A L R W \Rightarrow \text{non-volatile-owned-or-read-only pending-write } (S \oplus_{W} R \ominus_{A} L)
\[
(O \cup A \rightarrow R) \text{ xs}
| - \Rightarrow \text{non-volatile-owned-or-read-only pending-write } S O \text{ xs}
| \]

primrec acquired:: bool \Rightarrow 'a memref list \Rightarrow addr set \Rightarrow addr set
\text{where}
acquired pending-write [] A = (if pending-write then A else {})
| acquired pending-write (x#xs) A =
\[(\text{case } x \text{ of}
\]
Write_{sb} volatile - - - A' L R W \Rightarrow
\[
(\text{if volatile then acquired True xs (if pending-write then } (A \cup A' \rightarrow R) \text{ else } (A' \rightarrow R))
\]
\[
\text{else acquired pending-write xs A}
| \text{Ghost}_{sb} A' L R W \Rightarrow \text{acquired pending-write xs (if pending-write then } (A \cup A' \rightarrow R) \text{ else A)
| - \Rightarrow \text{acquired pending-write xs A)
| \]

primrec share:: 'a memref list \Rightarrow shared \Rightarrow shared
\text{where}
share [] S = S
| share (x#xs) S =
\[(\text{case } x \text{ of}
\]
Write_{sb} volatile - - - A L R W \Rightarrow \text{(if volatile then } (\text{share xs } (S \oplus_{W} R \ominus_{A} L)) \text{ else share xs S)
|
\]

57
primrec acquired-reads :: bool ⇒ 'a memref list ⇒ addr set ⇒ addr set
where
acquired-reads pending-write [] A = {}
| acquired-reads pending-write (x#xs) A =
  (case x of
      Read sb volatile a t v ⇒
          (if pending-write ∧ ¬ volatile ∧ a ∈ A
            then insert a (acquired-reads pending-write xs A)
            else acquired-reads pending-write xs A)
    | Write sb volatile _ _ _ ⇒
        (if volatile then acquired-reads True xs (if pending-write then (A ∪ A' − R) else A)
            else acquired-reads pending-write xs A)
    | Ghost sb A' L R W ⇒
        acquired-reads pending-write xs (A ∪ A' − R)
    | - ⇒ acquired-reads pending-write xs A)

lemma union-mono-aux: A ⊆ B ⇒ A ∪ C ⊆ B ∪ C
⟨proof⟩

lemma set-minus-mono-aux: A ⊆ B ⇒ A − C ⊆ B − C
⟨proof⟩

lemma acquired-mono: A ⊆ B ⇒ acquired pending-write xs A ⊆ acquired pending-write xs B
⟨proof⟩

lemma acquired-mono-in:
assumes x-in: x ∈ acquired pending-write xs A
assumes sub: A ⊆ B
shows x ∈ acquired pending-write xs B
⟨proof⟩

lemma acquired-no-pending-write:
A ⊆ B ⇒ acquired False xs A = acquired False xs B
⟨proof⟩

lemma acquired-no-pending-write-in:
x ∈ acquired False xs A ⇒ x ∈ acquired False xs B
⟨proof⟩

lemma acquired-pending-write-mono-in:
x ∈ acquired False xs A ⇒ x ∈ acquired True xs B
⟨proof⟩

lemma acquired-pending-write-mono:
aquired False xs A ⊆ acquired True xs B
⟨proof⟩

lemma acquired-append:
A pending-write. acquired pending-write (xs@ys) A =
acquired (pending-write ∨ outstanding-refs is-volatile-Write_{sb} xs ≠ {}) ys (acquired pending-write xs A)
⟨proof⟩

**lemma** acquired-take-drop:
acquired (pending-write ∨ outstanding-refs is-volatile-Write_{sb} (takeWhile P xs) ≠ {})
(dropWhile P xs) (acquired pending-write (takeWhile P xs) A) =
acquired pending-write xs A
⟨proof⟩

**lemma** share-mono: ∩ A B. dom A ⊆ dom B ⇒ dom (share xs A) ⊆ dom (share xs B)
⟨proof⟩

**lemma** share-mono-in:
assumes x-in: x ∈ dom (share xs A)
assumes sub: dom A ⊆ dom B
shows x ∈ dom (share xs B)
⟨proof⟩

**lemma** acquired-reads-mono:
∩ A B pending-write. A ⊆ B ⇒ acquired-reads pending-write xs A ⊆ acquired-reads pending-write xs B
⟨proof⟩

**lemma** acquired-reads-mono-in:
assumes x-in: x ∈ acquired-reads pending-write xs A
assumes sub: A ⊆ B
shows x ∈ acquired-reads pending-write xs B
⟨proof⟩

**lemma** acquired-reads-no-pending-write:
∩ A B. acquired-reads False xs A = acquired-reads False xs B
⟨proof⟩

**lemma** acquired-reads-no-pending-write-in:
x ∈ acquired-reads False xs A ⇒ x ∈ acquired-reads False xs B
⟨proof⟩

**lemma** acquired-reads-pending-write-mono:
∩ A. acquired-reads False xs A ⊆ acquired-reads True xs A
⟨proof⟩

**lemma** acquired-reads-pending-write-mono-in:
assumes x-in: x ∈ acquired-reads False xs A
shows x ∈ acquired-reads True xs A
⟨proof⟩

**lemma** acquired-reads-append: ∩ pending-write A. acquired-reads pending-write (xs@ys) A =
acquired-reads pending-write xs A ∪
acquired-reads (pending-write ∨ (outstanding-refs is-volatile-Write_{sb} xs ≠ {})) ys
(acquired pending-write xs A)
⟨proof⟩

lemma in-acquired-reads-no-pending-write-outstanding-write:
∀ A. a ∈ acquired-reads False xs A ⇒ outstanding-refs (is-volatile-Write_{sb}) xs ≠ {}
⟨proof⟩

lemma augment-read-only-mono: read-only S ⊆ read-only S' ⇒
read-only (S ⊕ W) ⊆ read-only (S' ⊕ W)
⟨proof⟩

lemma restrict-read-only-mono: read-only S ⊆ read-only S' ⇒
read-only (S ⊖ A) ⊆ read-only (S' ⊖ A)
⟨proof⟩

lemma share-read-only-mono: \(\forall SS'.\) read-only S ⊆ read-only S' ⇒
read-only (share sb S) (acquired True xs O) ys
⟨proof⟩

lemma non-volatile-owned-or-read-only-append:
∀ O S pending-write. non-volatile-owned-or-read-only pending-write S O (xs@ys)
= (non-volatile-owned-or-read-only pending-write S O xs ∧
    non-volatile-owned-or-read-only (pending-write ∨ outstanding-refs
is-volatile-Write_{sb} xs ≠ {}))
    (share xs S) (acquired True xs O) ys
⟨proof⟩

lemma non-volatile-owned-or-read-only-mono:
∀ O O' S pending-write. O ⊆ O' ⇒ non-volatile-owned-or-read-only pending-write S O xs
⇒ non-volatile-owned-or-read-only pending-write S O' xs
⟨proof⟩

lemma non-volatile-owned-or-read-only-shared-mono:
\(\forall SS' O pending-write. S ⊆ S' \Rightarrow non-volatile-owned-or-read-only pending-write S O xs\)
⇒ non-volatile-owned-or-read-only pending-write S' O xs
⟨proof⟩

lemma non-volatile-owned-or-read-only-pending-write-antimono:
∀ O S. non-volatile-owned-or-read-only True S O xs
⇒ non-volatile-owned-or-read-only False S O xs
⟨proof⟩

primrec all-acquired :: 'a memref list ⇒ addr set
where
all-acquired [] = {}
| all-acquired (i#is) =
  (case i of
    Write sb volatile - - - A L R W ⇒ (if volatile then A ∪ all-acquired is else all-acquired is)
    | Ghost sb A L R W ⇒ A ∪ all-acquired is
    | - ⇒ all-acquired is)

lemma all-acquired-append: all-acquired (xs@ys) = all-acquired xs ∪ all-acquired ys
⟨proof⟩

lemma acquired-reads-all-acquired: \(∀O\) pending-write.
  acquired-reads pending-write sb \(O \subseteq O \cup all-acquired sb\)
⟨proof⟩

lemma acquired-takeWhile-non-volatile-Write sb:
\(∀A\). (acquired True (takeWhile (Not ◦ is-volatile-Write sb) sb) A) \(⊆\)
  A ∪ all-acquired (takeWhile (Not ◦ is-volatile-Write sb) sb)
⟨proof⟩

lemma acquired-False-takeWhile-non-volatile-Write sb:
acquired False (takeWhile (Not ◦ is-volatile-Write sb) sb) A = {}
⟨proof⟩

lemma outstanding-refs-takeWhile-opposite: outstanding-refs P (takeWhile (Not ◦ P) xs) = {}
⟨proof⟩

lemma no-outstanding-volatile-Write sb-acquired:
outstanding-refs is-volatile-Write sb = {}
⇒ acquired False sb A = {}
⟨proof⟩

lemma acquired-all-acquired:\(∀pending-write A\). acquired pending-write xs A \(⊆\) A ∪ all-acquired xs
⟨proof⟩

lemma acquired-all-acquired-in: x ∈ acquired pending-write xs A ⇒ x ∈ A ∪ all-acquired xs
⟨proof⟩

primrec sharing-consistent:: shared ⇒ owns ⇒ 'a memref list ⇒ bool
where
  sharing-consistent \(S\ O\ []\) = True
| sharing-consistent \(S\ O\ (r#rs)\) =
  (case r of
    Write sb volatile - - - A L R W ⇒
(if volatile then \(A \subseteq \text{dom} \ \mathcal{S} \cup \mathcal{O} \land L \subseteq A \land A \cap R = \{\} \land R \subseteq \mathcal{O} \land \text{sharing-consistent} \ (\mathcal{S} \oplus_W R \ominus_A L) \ (\mathcal{O} \cup A - R) \ rs\) \\
else \text{sharing-consistent} \ (\mathcal{S} \ O \ rs)\)

\(\text{Ghost}_{sb} A L R W \Rightarrow A \subseteq \text{dom} \ \mathcal{S} \cup \mathcal{O} \land L \subseteq A \land A \cap R = \{\} \land R \subseteq \mathcal{O} \land \text{sharing-consistent} \ (\mathcal{S} \oplus_W R \ominus_A L) \ (\mathcal{O} \cup A - R) \ rs\)

\(| - \Rightarrow \text{sharing-consistent} \ \mathcal{S} \ O \ rs)\)

\textbf{lemma} \text{sharing-consistent-all-acquired:}
\[\forall \mathcal{S} \ O. \ \text{sharing-consistent} \ \mathcal{S} \ O \ sb \implies \text{all-acquired} \ sb \subseteq \text{dom} \ \mathcal{S} \cup \mathcal{O}\]

\(\langle \text{proof} \rangle\)

\textbf{lemma} \text{sharing-consistent-append:}
\[\forall \mathcal{S} \ O. \ \text{sharing-consistent} \ \mathcal{S} \ O \ (xs@ys) = \]
\[\text{(sharing-consistent} \ \mathcal{S} \ O \ xs \land \text{sharing-consistent} \ (\text{share} \ xs \ S) \ (\text{acquired} \ True \ xs \ O) \ ys)\]

\(\langle \text{proof} \rangle\)

\textbf{primrec} \text{read-only-reads :: owns} \Rightarrow \ 'a memref list \Rightarrow \text{addr set}

\textbf{where}
\text{read-only-reads} \ O \ [] = \{\}
| \text{read-only-reads} \ O \ (x#xs) = 
\text{(case} \ x \text{of}
\text{Read}_{sb} \ \text{volatile} \ a \ t \ v \Rightarrow (if} \neg \text{volatile} \land a \notin \mathcal{O} \text{then insert} \ a \text{\ (read-only-reads} \ O \ xs) \text{else read-only-reads} \ O \ xs)\)
| \text{Write}_{sb} \ \text{volatile} \ -\ -\ - A L R W \Rightarrow \text{(if} \neg \text{volatile then read-only-reads} \ (\mathcal{O} \cup A - R) \ xs \text{else read-only-reads} \ O \ xs)\)
| \text{Ghost}_{sb} A L R W \Rightarrow \text{read-only-reads} \ (\mathcal{O} \cup A - R) \ xs\)
| - \Rightarrow \text{read-only-reads} \ O \ xs)\)

\textbf{lemma} \text{read-only-reads-append:}
\[\forall \mathcal{O}. \ \text{read-only-reads} \ O \ (xs@ys) = \]
\[\text{read-only-reads} \ O \ xs \cup \text{read-only-reads} \ (\text{acquired} \ True \ xs \ O) \ ys\]

\(\langle \text{proof} \rangle\)

\textbf{lemma} \text{read-only-reads-antimono:}
\[\forall \mathcal{O} \mathcal{O}'.
\mathcal{O} \subseteq \mathcal{O}' \implies \text{read-only-reads} \ \mathcal{O}' \ sb \subseteq \text{read-only-reads} \ \mathcal{O} \ sb\]

\(\langle \text{proof} \rangle\)

\textbf{primrec} \text{non-volatile-writes-unshared:: shared} \Rightarrow \ 'a memref list \Rightarrow \text{bool}

\textbf{where}
\text{non-volatile-writes-unshared} \ S \ [] = \text{True}
| \text{non-volatile-writes-unshared} \ S \ (x#xs) = 
\text{(case} \ x \text{of}
\text{Write}_{sb} \ \text{volatile} \ a \ \text{sop} \ v \ A \ L \ R \ W \Rightarrow \text{(if} \neg \text{volatile then non-volatile-writes-unshared} \ (S \oplus_W R \ominus_A L) \ xs \text{else} \ a \notin \text{dom} \ S \land \text{non-volatile-writes-unshared} \ S \ xs)\)
| \text{Ghost}_{sb} A L R W \Rightarrow \text{non-volatile-writes-unshared} \ (S \oplus_W R \ominus_A L) \ xs
lemma non-volatile-writes-unshared-append:
\( \forall S. \) non-volatile-writes-unshared \( S \) \((xs@ys)\)
= (non-volatile-writes-unshared \( S \) \(xs\) \(\land\) non-volatile-writes-unshared (share \(xs\) \(S\) \(ys\))
⟨proof⟩

lemma non-volatile-writes-unshared-antimono:
\( \forall S S'. \) dom \( S \subseteq \) dom \( S' \) \(\implies\) non-volatile-writes-unshared \( S' \) \(xs\)
\(\implies\) non-volatile-writes-unshared \( S \) \(xs\)
⟨proof⟩

primrec no-write-to-read-only-memory:: shared ⇒ 'a memref list ⇒ bool
where
no-write-to-read-only-memory \( S \) \([]\) = True
| no-write-to-read-only-memory \( S \) \((x##xs)\) =
  (case \(x\) of
    Write\_sb volatile a sop v A L R W ⇒ \(a\not\in\) read-only \(S\) \(\land\)
    (if \(volatile\) then no-write-to-read-only-memory \((S \oplus W R \ominus A\) L) \(xs\)
else no-write-to-read-only-memory \(S\) \(xs\))
| \( - \) ⇒ no-write-to-read-only-memory \( S \) \(xs\))

lemma no-write-to-read-only-memory-append:
\( \forall S. \) no-write-to-read-only-memory \( S \) \((xs@ys)\)
= (no-write-to-read-only-memory \( S \) \(xs\) \(\land\) no-write-to-read-only-memory (share \(xs\) \(S\) \(ys\))
⟨proof⟩

lemma no-write-to-read-only-memory-antimono:
\( \forall S S'. \) S ⊆_x S' \(\implies\) no-write-to-read-only-memory \( S' \) \(xs\)
\(\implies\) no-write-to-read-only-memory \( S \) \(xs\)
⟨proof⟩

locale outstanding-non-volatile-refs-owned-or-read-only =
fixes S::shared
fixes ts::('p, p store-buffer, bool, owns, rels) thread-config list
assumes outstanding-non-volatile-refs-owned-or-read-only:
\( \forall i. \) \(is\) \(\ominus\) \(D\) \(\ominus\) sb \(p\).
[\(i < \) length ts; ts!i = (p, is, \theta, sb, D, \Theta, \mathcal{R}) ]
\(\implies\)
non-volatile-owned-or-read-only False \( S \) \(O\) sb

locale outstanding-volatile-writes-unowned-by-others =
fixes ts::('p, p store-buffer, bool, owns, rels) thread-config list
assumes outstanding-volatile-writes-unowned-by-others:
\( \forall i, j. \) is_i \(\ominus\) \(\mathcal{R}\) \(i\) \(D\) \(\ominus\) sb_i \(j\) p_j \(is\) j \(\ominus\) \(\mathcal{R}\) j \(D\) j \(\ominus\) sb_j,

63
locale read-only-reads-unowned =
fixes ts::(p,p store-buffer,bool,owns,rels) thread-config list
assumes read-only-reads-unowned:
\[ \forall i p i s O j R j D j \; \forall j sb j \; \forall j \; i \neq j; \]
\[ ts i = (p i ,is i ,\theta i ,sb i ,D i ,O i ,R i ); \; ts j = (p j,is j,\theta j,\; sb j,D j ,O j ,R j ) \]
\[ \Rightarrow \]
\[ (O j \cup \text{all-acquired sb}_j) \cap \text{outstanding-refs is-volatile-Write}_{sb} \; sb i = {} \]

locale ownership-distinct =
fixes ts::(p,p store-buffer,bool,owns,rels) thread-config list
assumes ownership-distinct:
\[ \forall i p i s O j R j D j \; \forall j sb j \; \forall j \; i \neq j; \]
\[ ts i = (p i ,is i ,\theta i ,sb i ,D i ,O i ,R i ); \; ts j = (p j,is j,\theta j,\; sb j,D j ,O j ,R j ) \]
\[ \Rightarrow \]
\[ (O j \cup \text{all-acquired sb}_j) \cap \text{read-only-reads (acquired True}
\]
\[ \text{takeWhile (Not is-volatile-Write}_{sb} \; sb i ) \; O i ) \]
\[ \text{dropWhile (Not is-volatile-Write}_{sb} \; sb i ) = {} \]

locale valid-ownership =
outstanding-non-volatile-refs-owned-or-read-only +
outstanding-volatile-writes-unowned-by-others +
read-only-reads-unowned +
ownership-distinct

locale outstanding-non-volatile-writes-unshared =
fixes S::shared and ts::(p,p store-buffer,bool,owns,rels) thread-config list
assumes outstanding-non-volatile-writes-unshared:
\[ \forall i p is \; O j R j D j \; \forall sb j \; \forall j \; i \neq j; \]
\[ ts i = (p i ,is i ,\theta i ,sb i ,D i ,O i ,R i ); \; ts j = (p j,is j,\theta j,\; sb j,D j ,O j ,R j ) \]
\[ \Rightarrow \]
\[ (O j \cup \text{all-acquired sb}_j) \cap (O j \cup \text{all-acquired sb}_j) = {} \]

locale sharing-consis =
fixes S::shared and ts::(p,p store-buffer,bool,owns,rels) thread-config list
assumes sharing-consis:
\[ \forall i p is \; O j R j D j \; \forall sb \]
\[ \forall i \; \forall j \; i \neq j; \]
\[ ts i = (p i ,is i ,\theta i ,sb,D i ,O i ,R i ) \]
\[ \Rightarrow \]

64
sharing-consistent $S \ O \ sb$

**locale** no-outstanding-write-to-read-only-memory =
**fixes** $S::\text{shared}$ and $ts::\langle p,^p\text{store-buffer,bool,owns,rels}\rangle$ thread-config list

**assumes** no-outstanding-write-to-read-only-memory:

$\bigwedge i \ p \text{ is } O \ R \ D \ \emptyset \ sb.$

$\left[ i < \text{length ts}; ts[i] = (p,\text{is},\emptyset,\text{sb},D,O,R) \right]$

$\Rightarrow$

no-write-to-read-only-memory $S \ sb$

**locale** valid-sharing =

outstanding-non-volatile-writes-unshared +
sharing-consis +
read-only-unowned +
unowned-shared +
no-outstanding-write-to-read-only-memory

**locale** valid-ownership-and-sharing = valid-ownership +
outstanding-non-volatile-writes-unshared +
sharing-consis +
no-outstanding-write-to-read-only-memory

**lemma** (in read-only-reads-unowned)

read-only-reads-unowned-nth-update:

$\bigwedge i \ p \text{ is } O \ R \ D \ \emptyset \ sb.$

$\left[ i < \text{length ts}; ts[i] = (p,\text{is},\emptyset,\text{sb},D,O,R) \right];$

read-only-reads (acquired True \(\text{takeWhile} \ (\not\circ\ \text{is-volatile-Write}_{\text{sb}}) \ \text{sb}') \ O')$

\(\text{dropWhile} \ (\not\circ\ \text{is-volatile-Write}_{\text{sb}}) \ \text{sb}) \subseteq \text{read-only-reads} \ (\text{acquired True}
\ (\text{takeWhile} \ (\not\circ\ \text{is-volatile-Write}_{\text{sb}}) \ \text{sb}) \ O)$

\(\text{dropWhile} \ (\not\circ\ \text{is-volatile-Write}_{\text{sb}}) \ \text{sb}) \ O' \cup \text{all-acquired sb}' \subseteq O \cup \text{all-acquired sb}] \Rightarrow$

read-only-reads-unowned (ts[i := (p',\text{is}',\emptyset',\text{sb}',D',O',R')])

(proof)

**lemma** outstanding-non-volatile-refs-owned-or-read-only-tl:

outstanding-non-volatile-refs-owned-or-read-only $S$ \((t\#ts) \Rightarrow$

outstanding-non-volatile-refs-owned-or-read-only $S \ ts$

(proof)

**lemma** outstanding-volatile-writes-unowned-by-others-tl:

outstanding-volatile-writes-unowned-by-others \((t\#ts) \Rightarrow$

outstanding-volatile-writes-unowned-by-others $\langle\rangle$

(proof)
lemma read-only-reads-unowned-tl:
read-only-reads-unowned \((t \# ts)\) \(\implies\)
read-only-reads-unowned \((ts)\)
\(\langle proof\rangle\)

lemma ownership-distinct-tl:
assumes dist: ownership-distinct \((t\#ts)\)
shows ownership-distinct ts
\(\langle proof\rangle\)

lemma valid-ownership-tl: valid-ownership \(S\) \((t\#ts)\) \(\implies\) valid-ownership \(S\) ts
\(\langle proof\rangle\)

lemma sharing-consistent-takeWhile:
assumes consis: sharing-consistent \(S \ O \ sb\)
shows sharing-consistent \(S \ O\) \((\text{takeWhile } P \ sb)\)
\(\langle proof\rangle\)

lemma sharing-consis-tl: sharing-consis \(S\) \((t\#ts)\) \(\implies\) sharing-consis \(S\) ts
\(\langle proof\rangle\)

lemma sharing-consis-Cons:
\([\text{sharing-consis } S \ ts; \text{sharing-consistent } S \ O \ sb]\]
\(\implies\) sharing-consis \(S\) \(((p,\is,\theta,\sb,D,O,R)\#ts)\)
\(\langle proof\rangle\)

lemma outstanding-non-volatile-writes-unshared-tl:
opt-outstanding-non-volatile-writes-unshared \(S\) \((t\#ts)\) \(\implies\)
opt-outstanding-non-volatile-writes-unshared \(S\) ts
\(\langle proof\rangle\)

lemma no-outstanding-write-to-read-only-memory-tl:
no-outstanding-write-to-read-only-memory \(S\) \((t\#ts)\) \(\implies\)
opt-no-outstanding-write-to-read-only-memory \(S\) ts
\(\langle proof\rangle\)

lemma valid-ownership-and-sharing-tl:
valid-ownership-and-sharing \(S\) \((t\#ts)\) \(\implies\) valid-ownership-and-sharing \(S\) ts
\(\langle proof\rangle\)

lemma non-volatile-owned-or-read-only-outstanding-non-volatile-writes:
\(\forall S \ \text{pending-write. } [\text{non-volatile-owned-or-read-only pending-write } S \ O \ sb]\)
\(\implies\) outstanding-refs is-non-volatile-Write\(sb\) \(sb \subseteq O \cup\ \text{all-acquired sb}\)
\(\langle proof\rangle\)
lemma (in outstanding-non-volatile-refs-owned-or-read-only)

outstanding-non-volatile-writes-owned:
assumes i-bound: i < length ts
assumes ts-i: ts!i = (p, is, 0, sb, D, O, R)
shows outstanding-refs is-non-volatile-Write sb ⊆ O ∪ all-acquired sb

⟨proof⟩

lemma non-volatile-reads-acquired-or-read-only:
[non-volatile-owned-or-read-only True S O sb; sharing-consistent S O sb] [non-volatile-owned-or-read-only pending-write S O sb]
⇒ outstanding-refs is-non-volatile-Read sb ⊆ O ∪ all-acquired sb ∪ read-only S

⟨proof⟩

lemma non-volatile-reads-acquired-or-read-only-reads:
[non-volatile-owned-or-read-only pending-write. S O sb]
⇒ outstanding-refs is-non-volatile-Read sb ⊆ O ∪ all-acquired sb ∪ read-only-reads O

⟨proof⟩

lemma non-volatile-owned-or-read-only-outstanding-refs:
[non-volatile-owned-or-read-only pending-write S O sb] (Not ⊪ is-volatile) sb ⊆ O ∪ all-acquired sb ∪ read-only-reads O

⟨proof⟩

lemma no-unacquired-write-to-read-only:
[no-write-to-read-only-memory S sb; sharing-consistent S O sb; a ∈ read-only S; a /∈ (O ∪ all-acquired sb)]
⇒ a /∈ outstanding-refs is-Write sb

⟨proof⟩

lemma read-only-reads-read-only:
[non-volatile-owned-or-read-only True S O sb; sharing-consistent S O sb]
⇒ read-only-reads O sb ⊆ O ∪ all-acquired sb ∪ read-only S

⟨proof⟩

67
lemma no-unacquired-write-to-read-only-reads:
\( \forall S \ O . \left[ \text{no-write-to-read-only-memory} \ S \ sb \right] \)

non-volatile-owned-or-read-only True \( S \ O \ sb \); sharing-consistent \( S \ O \ sb \);
\( a \in \text{read-only-reads} \ O \ \text{sb} ; \ a \notin (O \ \cup \ \text{all-acquired sb}) \] \[ \implies a \notin \text{outstanding-refs is-Write}_{sb} \ sb \]

\( \langle \text{proof} \rangle \)

lemma no-unacquired-write-to-read-only\(^{''} \):
\begin{align*}
\text{assumes} & \text{ no-wrt: no-write-to-read-only-memory} \ S \ sb \\
\text{assumes} & \text{ consis: sharing-consistent} \ S \ O \ sb \\
\text{shows} & \text{ read-only} \ S \ \cap \ \text{outstanding-refs is-Write}_{sb} \ sb \ \subseteq O \ \cup \ \text{all-acquired sb}
\end{align*}

\( \langle \text{proof} \rangle \)

lemma no-unacquired-volatile-write-to-read-only:
\begin{align*}
\text{assumes} & \text{ no-wrt: no-write-to-read-only-memory} \ S \ sb \\
\text{assumes} & \text{ consis: sharing-consistent} \ S \ O \ sb \\
\text{shows} & \text{ read-only} \ S \ \cap \ \text{outstanding-refs is-volatile-Write}_{sb} \ sb \ \subseteq O \ \cup \ \text{all-acquired sb}
\end{align*}

\( \langle \text{proof} \rangle \)

lemma no-unacquired-non-volatile-write-to-read-only-reads:
\begin{align*}
\text{assumes} & \text{ no-wrt: no-write-to-read-only-memory} \ S \ sb \\
\text{assumes} & \text{ consis: sharing-consistent} \ S \ O \ sb \\
\text{shows} & \text{ read-only-reads} \ O \ \text{sb} \ \cap \ \text{outstanding-refs is-non-volatile-Write}_{sb} \ sb \ \subseteq O \ \cup \ \text{all-acquired sb}
\end{align*}

\( \langle \text{proof} \rangle \)

lemma no-unacquired-write-to-read-only-reads\(^{'} \):
\begin{align*}
\text{assumes} & \text{ no-wrt: no-write-to-read-only-memory} \ S \ sb \\
\text{assumes} & \text{ non-vol: non-volatile-owned-or-read-only} \ \text{True} \ S \ O \ sb \\
\text{assumes} & \text{ consis: sharing-consistent} \ S \ O \ sb \\
\text{shows} & \text{ read-only-reads} \ O \ \text{sb} \ \cap \ \text{outstanding-refs is-Write}_{sb} \ sb \ \subseteq O \ \cup \ \text{all-acquired sb}
\end{align*}

\( \langle \text{proof} \rangle \)

lemma no-unacquired-volatile-write-to-read-only-reads:
\begin{align*}
\text{assumes} & \text{ no-wrt: no-write-to-read-only-memory} \ S \ sb \\
\text{assumes} & \text{ non-vol: non-volatile-owned-or-read-only} \ \text{True} \ S \ O \ sb \\
\text{assumes} & \text{ consis: sharing-consistent} \ S \ O \ sb \\
\text{shows} & \text{ read-only-reads} \ O \ \text{sb} \ \cap \ \text{outstanding-refs is-volatile-Write}_{sb} \ sb \ \subseteq O \ \cup \ \text{all-acquired sb}
\end{align*}

\( \langle \text{proof} \rangle \)

lemma no-unacquired-non-volatile-write-to-read-only:
\begin{align*}
\text{assumes} & \text{ no-wrt: no-write-to-read-only-memory} \ S \ sb \\
\text{assumes} & \text{ non-vol: non-volatile-owned-or-read-only} \ \text{True} \ S \ O \ sb \\
\text{assumes} & \text{ consis: sharing-consistent} \ S \ O \ sb \\
\text{shows} & \text{ read-only-reads} \ O \ \text{sb} \ \cap \ \text{outstanding-refs is-non-volatile-Write}_{sb} \ sb \ \subseteq O \ \cup \ \text{all-acquired sb}
\end{align*}

\( \langle \text{proof} \rangle \)

68
lemma set-dropWhileD: \( x \in \text{set} \ (\text{dropWhile} \ P \ xs) \implies x \in \text{set} \ xs \)  
\( \langle \text{proof} \rangle \)

lemma outstanding-refs-takeWhileD:  
\( x \in \text{outstanding-refs} \ P \ (\text{takeWhile} \ P' \ sb) \implies x \in \text{outstanding-refs} \ P \ sb \)  
\( \langle \text{proof} \rangle \)

lemma outstanding-refs-dropWhileD:  
\( x \in \text{outstanding-refs} \ P \ (\text{dropWhile} \ P' \ sb) \implies x \in \text{outstanding-refs} \ P \ sb \)  
\( \langle \text{proof} \rangle \)

lemma dropWhile-ConsD: \( \text{dropWhile} \ P \ xs = y \# ys \implies \neg P \ y \)  
\( \langle \text{proof} \rangle \)

lemma non-volatile-owned-or-read-only-drop:  
non-volatile-owned-or-read-only \( False \ S \ O \ sb \implies \neg \text{non-volatile-owned-or-read-only} \ True \)  
\( (\text{share} \ (\text{takeWhile} \ (\text{Not} \circ \text{is-volatile-Write}_{sb}) \ sb) \ S) \)  
\( (\text{acquired} \ True \ (\text{takeWhile} \ (\text{Not} \circ \text{is-volatile-Write}_{sb}) \ sb) \ O) \)  
\( (\text{dropWhile} \ (\text{Not} \circ \text{is-volatile-Write}_{sb}) \ sb) \)  
\( \langle \text{proof} \rangle \)

lemma read-only-share: \( \bigwedge S \ O. \)  
\( \text{sharing-consistent} \ S \ O \ sb \implies \text{read-only} \ (\text{share} \ sb \ S) \subseteq \text{read-only} \ S \cup O \cup \text{all-acquired} \ sb \)  
\( \langle \text{proof} \rangle \)

lemma (in valid-ownership-and-sharing) outstanding-non-write-non-vol-reads-drop-disj:  
assumes i-bound: \( i < \text{length} \ ts \)  
assumes j-bound: \( j < \text{length} \ ts \)  
assumes neq-i-j: \( i \neq j \)  
assumes ith: \( \text{ts!i} = (p_i,i\_is_i,\theta_i,sb_i,D_i,O_i,R_i) \)  
assumes jth: \( \text{ts!j} = (p_j,i\_is_j,\theta_j,sb_j,D_j,O_j,R_j) \)  
shows outstanding-refs \( \text{is-Write}_{sb} \ (\text{dropWhile} \ (\text{Not} \circ \text{is-volatile-Write}_{sb}) \ sb_i) \cap \)  
outstanding-refs \( \text{is-non-volatile-Read}_{sb} \ (\text{dropWhile} \ (\text{Not} \circ \text{is-volatile-Write}_{sb}) \ sb_j) \)  
\( = \{\} \)  
\( \langle \text{proof} \rangle \)

lemma (in valid-ownership-and-sharing) outstanding-non-volatile-write-disj:  
assumes i-bound: \( i < \text{length} \ ts \)  
assumes j-bound: \( j < \text{length} \ ts \)
assumes neq-i-j: i ≠ j
assumes ith: ts!i = (p_i, is_i, θ_i, sb_i, D_i, O_i, R_i)
assumes jth: ts!j = (p_j, is_j, θ_j, sb_j, D_j, O_j, R_j)
shows outstanding-refs (is-non-volatile-Write_{sb_i}) (takeWhile (Not o is-volatile-Write_{sb_i}) sb_i) ∩
  (outstanding-refs is-volatile-Write_{sb_i} sb_j ∪
   outstanding-refs is-non-volatile-Write_{sb_i} sb_j ∪
   outstanding-refs is-non-volatile-Read_{sb_i} (dropWhile (Not o is-volatile-Write_{sb_i}) sb_j)
   ∪
   (outstanding-refs is-non-volatile-Read_{sb_j} (takeWhile (Not o is-volatile-Write_{sb_j}) sb_j)
   −
   read-only-reads O_j (takeWhile (Not o is-volatile-Write_{sb_j}) sb_j)) ∪
   (O_j ∪ all-acquired (takeWhile (Not o is-volatile-Write_{sb_j}) sb_j))
) = { } (is ?non-vol-writes-i ∩ ?not-volatile-j = { })
⟨proof⟩

lemma (in valid-ownership-and-sharing) outstanding-non-volatile-write-not-volatile-read-disj:
assumes i-bound: i < length ts
assumes j-bound: j < length ts
assumes neq-i-j: i ≠ j
assumes ith: ts!i = (p_i, is_i, θ_i, sb_i, D_i, O_i, R_i)
assumes jth: ts!j = (p_j, is_j, θ_j, sb_j, D_j, O_j, R_j)
shows outstanding-refs (is-non-volatile-Write_{sb_i}) (takeWhile (Not o is-volatile-Write_{sb_i}) sb_i) ∩
  (outstanding-refs (Not ◦ is-volatile-Read_{sb_j}) (dropWhile (Not ◦ is-volatile-Write_{sb_j}) sb_j) = { })
  (is ?non-vol-writes-i ∩ ?not-volatile-j = { })
⟨proof⟩

lemma (in valid-ownership-and-sharing) outstanding-refs-is-Write_{sb_i}-takeWhile-disj:
∀ i < length ts. (∀ j < length ts. i ≠ j →
  (let (sr, sr, sb_i, r, r, r) = ts!i;
       (sr, sr, sb_j, r, r, r) = ts!j
       in outstanding-refs is-Write_{sb_i} sb_i ∩
       outstanding-refs is-Write_{sb_j} (takeWhile (Not o is-volatile-Write_{sb_j}) sb_j) = { }))
⟨proof⟩

fun read-tmps:: 'p store-buffer ⇒ tmp set
where
  read-tmps [] = {}
| read-tmps (r # rs) =
    (case r of
      Read_{sb_i} volatile a t v ⇒ insert t (read-tmps rs)
    | - ⇒ read-tmps rs)
**Lemma** in-read-tmps-conv: 
\[(t \in \text{read-tmps } xs) = (\exists \text{volatile a v. } \text{Read}_{ab} \text{ volatile a t v } \in \text{set xs})\]

\[\text{(proof)}\]

**Lemma** read-tmps-mono: \(\forall ys. \text{set xs } \subseteq \text{set ys } \implies \text{read-tmps } xs \subseteq \text{read-tmps } ys\)

\[\text{(proof)}\]

**Fun** distinct-read-tmps:: 'p store-buffer \Rightarrow \text{bool}

**Where**
- \(\text{distinct-read-tmps } [] = \text{True}\)
- \(\text{distinct-read-tmps } (r#rs) =\)
  - (case \(r\) of 
    - \(\text{Read}_{ab} \) \text{volatile a t v } \Rightarrow \text{t v } \notin \text{set rs } \land \text{distinct-read-tmps } rs\)
    - \(- \Rightarrow \text{distinct-read-tmps } rs\)

**Lemma** distinct-read-tmps-conv:
\(\text{distinct-read-tmps } xs = (\forall i < \text{length xs. } \forall j < \text{length xs. } i \neq j \rightarrow\)
- (case \(xs[i]\) of 
  - \(\text{Read}_{ab} \) \text{volatile a t } \Rightarrow \text{t } \neq \text{t } \land \text{distinct-read-tmps } rs\)
  - \(- \Rightarrow \text{True}\)

— Nice lemma, ugly proof.

\[\text{(proof)}\]

**Fun** load-tmps:: instrs \Rightarrow \text{tmp set}

**Where**
- \(\text{load-tmps } [] = \{\}\)
- \(\text{load-tmps } (i#is) =\)
  - (case \(i\) of 
    - \(\text{Read }\) \text{volatile a t } \Rightarrow \text{insert t } (\text{load-tmps } is)\)
    - \(\text{RMW } t \) \text{- - - - - - - - } \Rightarrow \text{insert t } (\text{load-tmps } is)\)
    - \(- \Rightarrow \text{load-tmps } is\)

**Lemma** in-load-tmps-conv:
\(t \in \text{load-tmps } xs = ((\exists \text{volatile a. } \text{Read } \text{volatile a t } \in \text{set xs}) \lor\)
- (\(\exists \text{a sop cond ret A L R W. } \text{RMW a t sop cond ret A L R W } \in \text{set xs})\)

\[\text{(proof)}\]

**Lemma** load-tmps-mono: \(\forall ys. \text{set xs } \subseteq \text{set ys } \implies \text{load-tmps } xs \subseteq \text{load-tmps } ys\)

\[\text{(proof)}\]

**Fun** distinct-load-tmps:: instrs \Rightarrow \text{bool}

**Where**
- \(\text{distinct-load-tmps } [] = \text{True}\)
- \(\text{distinct-load-tmps } (r#rs) =\)
  - (case \(r\) of 
    - \(\text{Read }\) \text{volatile a t } \Rightarrow \text{t } \neq \text{t } \land \text{distinct-load-tmps } rs\)

71
| RMW a t sop cond ret A L R W ⇒ t ∉ (load-tmps rs) ∧ distinct-load-tmps rs
| - ⇒ distinct-load-tmps rs)

locale load-tmps-distinct =
fixes ts::('p, 'p store-buffer, bool, owns, rels) thread-config list
assumes load-tmps-distinct:
\[ \forall i. p \text{ is O R D } \theta \text{ sb.} \]
\[ [i < \text{length ts}; ts!i = (p.is, \theta, \text{sb}, D, O, R) ] \]
⇒
distinct-load-tmps is

locale read-tmps-distinct =
fixes ts::('p, 'p store-buffer, bool, owns, rels) thread-config list
assumes read-tmps-distinct:
\[ \forall i. p \text{ is O R D } \theta \text{ sb.} \]
\[ [i < \text{length ts}; ts!i = (p.is, \theta, \text{sb}, D, O, R) ] \]
⇒
distinct-read-tmps sb

locale load-tmps-read-tmps-distinct =
fixes ts::('p, 'p store-buffer, bool, owns, rels) thread-config list
assumes load-tmps-read-tmps-distinct:
\[ \forall i. p \text{ is O R D } \theta \text{ sb.} \]
\[ [i < \text{length ts}; ts!i = (p.is, \theta, \text{sb}, D, O, R) ] \]
⇒
load-tmps is ∩ read-tmps sb = {}

locale tmps-distinct =
load-tmps-distinct +
read-tmps-distinct +
load-tmps-read-tmps-distinct

lemma rev-read-tmps: read-tmps (rev xs) = read-tmps xs
⟨proof⟩

lemma rev-load-tmps: load-tmps (rev xs) = load-tmps xs
⟨proof⟩

lemma distinct-read-tmps-append: \( \forall ys. \text{distinct-read-tmps } (xs \odot ys) = \)
\( \text{(distinct-read-tmps xs} \land \text{distinct-read-tmps ys} \land \)
\( \text{read-tmps xs} \cap \text{read-tmps ys} = \{\} \)
⟨proof⟩

lemma distinct-load-tmps-append: \( \forall ys. \text{distinct-load-tmps } (xs \odot ys) = \)
\( \text{(distinct-load-tmps xs} \land \text{distinct-load-tmps ys} \land \)
\( \text{load-tmps xs} \cap \text{load-tmps ys} = \{\} \)
⟨proof⟩

lemma read-tmps-append: read-tmps (xs@ys) = (read-tmps xs ∪ read-tmps ys)
lemma load-tmps-append: load-tmps (xs@ys) = (load-tmps xs ∪ load-tmps ys)

fun write-sops:: 'p store-buffer ⇒ sop set
where
write-sops [] = {}
| write-sops (r#rs) =
  (case r of
    Write sb volatile a sop v - - - - ⇒ insert sop (write-sops rs)
| - ⇒ write-sops rs)

lemma in-write-sops-conv:
(sop ∈ write-sops xs) = (∃ volatile a v A L R W. Write sb volatile a sop v A L R W ∈ set xs)

lemma write-sops-mono: \( \forall ys. \text{set } xs \subseteq \text{set } ys \implies \text{write-sops } xs \subseteq \text{write-sops } ys \)

lemma write-sops-append: write-sops (xs@ys) = write-sops xs ∪ write-sops ys

fun store-sops:: instrs ⇒ sop set
where
store-sops [] = {}
| store-sops (i#is) =
  (case i of
    Write volatile a sop - - - - ⇒ insert sop (store-sops is)
| RMW a t sop cond ret A L R W ⇒ insert sop (store-sops is)
| - ⇒ store-sops is)

lemma in-store-sops-conv:
(sop ∈ store-sops xs) = (\( \exists \) volatile a v A L R W. Write volatile a sop A L R W ∈ set xs) ∨
\( \exists \) a t cond ret A L R W. RMW a t sop cond ret A L R W ∈ set xs)

lemma store-sops-mono: \( \forall ys. \text{set } xs \subseteq \text{set } ys \implies \text{store-sops } xs \subseteq \text{store-sops } ys \)

lemma store-sops-append: store-sops (xs@ys) = store-sops xs ∪ store-sops ys

locale valid-write-sops =
fixes ts::('p,'p store-buffer,bool,owns,rels) thread-config list
assumes valid-write-sops:
\( \forall i p {\text{is } O R D \& \& sb.} \)
\[\forall \text{sop} \in \text{write-sops sb. valid-sop sop}\]

locale valid-store-sops =
fixes ts::('p,\ p \text{ store-buffer, bool, owns, rels}) thread-config list
assumes valid-store-sops:
\[\begin{array}{l}
[i < \text{length ts}; \text{ts!i} = (\text{p, is, \theta, sb, D, O, R})] \\
\Rightarrow \\
\forall \text{sop} \in \text{store-sops is. valid-sop sop}
\end{array}\]

locale valid-sops = valid-write-sops + valid-store-sops
The value stored in a non-volatile Read\sb in the store-buffer has to match the last value written to the same address in the store buffer or the memory content if there is no corresponding write in the store buffer. No volatile read may follow a volatile write. Volatile reads in the store buffer may refer to a stale value: e.g. imagine one writer and multiple readers

fun reads-consistent:: bool \Rightarrow own \Rightarrow memory \Rightarrow 'p store-buffer \Rightarrow bool
where
reads-consistent pending-write \text{O m} [] = True
| reads-consistent pending-write \text{O m} (r#rs) =
\begin{array}{l}
\text{(case r of}
\text{Read\sb volatile a t v \Rightarrow (\neg \text{volatile } \rightarrow (\text{pending-write} \vee a \in \text{O}) \rightarrow v = m a) } \\
\text{reads-consistent pending-write \text{O m rs}}
\end{array}
| Write\sb volatile a sop v A L R W \Rightarrow
\begin{array}{l}
\text{(if volatile then}
\text{outstanding-refs is-volatile-Read\sb rs = \{} \wedge
\text{reads-consistent True (O \cup A - R) (m(a := v)) rs}
\text{else reads-consistent pending-write \text{O (m(a := v)) rs}}
\text{reads-consistent pending-write (O \cup A - R) m rs}
\text{| - } \Rightarrow \text{reads-consistent pending-write \text{O m rs}}
\end{array}

fun volatile-reads-consistent:: memory \Rightarrow 'p store-buffer \Rightarrow bool
where
volatile-reads-consistent m [] = True
| volatile-reads-consistent m (r#rs) =
\begin{array}{l}
\text{(case r of}
\text{Read\sb volatile a t v \Rightarrow (volatile } \rightarrow v = m a) \wedge \text{volatile-reads-consistent m rs}
\text{| Write\sb volatile a sop v A L R W } \Rightarrow \text{volatile-reads-consistent (m(a := v)) rs}
\text{| - } \Rightarrow \text{volatile-reads-consistent m rs}
\end{array}

fun flush:: 'p store-buffer \Rightarrow memory \Rightarrow memory
where
flush [] m = m
| flush (r#rs) m =
\begin{array}{l}
\text{(case r of}
\text{Write\sb volatile a - v - - - } \Rightarrow \text{flush rs (m(a:=v))}
\text{| - } \Rightarrow \text{flush rs m})
\end{array}
**lemma** reads-consistent-pending-write-antimono:

\[ \forall O \ m. \ \text{reads-consistent} \ True \ O \ m \ sb \implies \text{reads-consistent} \ False \ O \ m \ sb \]

(*proof*)

**lemma** reads-consistent-owns-antimono:

\[ \forall O'O' \pending-write \ m. \ O \subseteq O' \implies \text{reads-consistent} \ pending-write \ O' \ m \ sb \implies \text{reads-consistent} \ pending-write \ O \ m \ sb \]

(*proof*)

**lemma** acquired-reads-mono':

\[ x \in \text{acquired-reads} \ b \ xs \ A \implies \text{acquired-reads} \ b \ xs \ B = \{\} \implies A \subseteq B \implies False \]

(*proof*)

**lemma** reads-consistent-append:

\[ \forall m \ pending-write \ O. \ \text{reads-consistent} \ pending-write \ O \ m \ (xs@ys) = \]

\[ (\text{reads-consistent} \ pending-write \ O \ m \ xs \land \]

\[ \text{reads-consistent} \ (\text{pending-write} \lor \text{outstanding-refs} \ \text{is-volatile-Write}_{sb} \ xs \neq \{\}) \]

\[ (\text{acquired} \ True \ xs \ O) \ (\text{flush} \ xs \ m) \ ys \land \]

\[ (\text{outstanding-refs} \ \text{is-volatile-Write}_{sb} \ xs \neq \{\}) \rightarrow (\text{outstanding-refs} \ \text{is-volatile-Read}_{sb} \ ys = \{\}) ) \]

(*proof*)

**lemma** reads-consistent-mem-eq-on-non-volatile-reads:

assumes mem-eq: \( \forall a \in A. \ m' a = m a \)

assumes subset: outstanding-refs (is-non-volatile-Read_{sb}) sb \subseteq A

— We could be even more restrictive here, only the non volatile reads that are not buffered in sb have to be the same.

assumes consis-m: reads-consistent pending-write O m sb

shows reads-consistent pending-write O m' sb

(*proof*)

**lemma** volatile-reads-consistent-mem-eq-on-volatile-reads:

assumes mem-eq: \( \forall a \in A. \ m' a = m a \)

assumes subset: outstanding-refs (is-volatile-Read_{sb}) sb \subseteq A

— We could be even more restrictive here, only the non volatile reads that are not buffered in sb have to be the same.

assumes consis-m: volatile-reads-consistent m sb

shows volatile-reads-consistent m' sb

(*proof*)

locale valid-reads =

fixes m::memory and ts::{i p, i store-buffer,bool,owns,rels} thread-config list

assumes valid-reads: \( \forall i \ p \ is \ O \ R \ D \ \emptyset \ sb. \)

\[ [i < \text{length} \ ts; \ ts!i = (p,is,\emptyset,sb,D,O,R) ] \implies \]
reads-consistent False m sb

**Lemma** valid-reads-Con: valid-reads m (t#ts) =
(let (\(r,\cdots, sb, \cdots, \mathcal{O}, \cdots\)) \(= t\) in reads-consistent False m sb \(\land\) valid-reads m ts)

**Proof**
Reads and writes have in the store-buffer have to conform to the valuation of temporaries.

**context** program

begin

**fun** history-consistent:: tmps \(\Rightarrow\) \('p \Rightarrow 'p\) store-buffer \(\Rightarrow\) bool

where
history-consistent \(\emptyset\) p [] = True
| history-consistent \(\emptyset\) p (r#rs) =
  (case r of
    Read sb vol a t v =
      (case \(\emptyset\) t of Some v' \(\Rightarrow\) v'=v' \(\land\) history-consistent \(\emptyset\) p rs | - \(\Rightarrow\) False)
| Write sb vol a (D,f) v - - - - \(\Rightarrow\) D \subseteq\ dom \(\emptyset\) \(\land\) f \(\emptyset\) = v \(\land\) D \(\cap\) read-tmps rs = {} \(\land\) history-consistent \(\emptyset\) p rs
| Prog sb p1 p2 is \(\Rightarrow\) p1=p \(\land\)
  \(\emptyset\) |'(dom \(\emptyset\) \(\land\) read-tmps rs)\(\vdash\) p1 \(\rightarrow\) p (p2,is) \(\land\)
  history-consistent \(\emptyset\) p2 rs
| - \(\Rightarrow\) history-consistent \(\emptyset\) p rs)

end

**fun** hd-prog:: \('p \Rightarrow 'p\) store-buffer \(\Rightarrow\) \('p\)

where
hd-prog p [] = p
| hd-prog p (i#is) = (case i of
  Prog sb p' - - - - \(\Rightarrow\) p'
| - \(\Rightarrow\) hd-prog p is)

**fun** last-prog:: \('p \Rightarrow 'p\) store-buffer \(\Rightarrow\) \('p\)

where
last-prog p [] = p
| last-prog p (i#is) = (case i of
  Prog sb - p' - - - - \(\Rightarrow\) last-prog p' is
| - \(\Rightarrow\) last-prog p is)

**locale** valid-history = program +

**constrains**

program-step :: tmps \(\Rightarrow\) \('p \Rightarrow 'p\) \(\times\) instrs \(\Rightarrow\) bool

**fixes** ts::\(\{'p, \\cdots, 'p\) store-buffer, bool, owns, rels\) thread-config list

**assumes** valid-history:
\(\forall i\ p \in \mathcal{O} \ \mathcal{R} \ \mathcal{D} \ \emptyset\ \text{sb.}
\[i < \text{length ts; } t!i = (p, is, \emptyset, sb; D, O, R) \]\(\Rightarrow\)
program.history-consistent program-step \(\emptyset\) (hd-prog p sb) sb

**fun** data-dependency-consistent-instrs:: addr set \(\Rightarrow\) instrs \(\Rightarrow\) bool

where
data-dependency-consistent-instrs T [] = True
| data-dependency-consistent-instrs T (i#is) =
  (case i of

76
Write volatile a (D,f) - - - - \Rightarrow D \subseteq T \land D \cap load-tmps is = \{\} \land 
data-dependency-consistent-instrs T is 
| RMW a t (D,f) cond ret - - - - \Rightarrow D \subseteq T \land D \cap load-tmps is = \{\} \land 
data-dependency-consistent-instrs (insert t T) is 
| Read - - t \Rightarrow data-dependency-consistent-instrs (insert t T) is 
| - \Rightarrow data-dependency-consistent-instrs T is) 

lemma data-dependency-consistent-mono: 
\land T T'. [data-dependency-consistent-instrs T is; T \subseteq T'] \Rightarrow data-dependency-consistent-instrs T' is 
(proof) 

lemma data-dependency-consistent-instrs-append: 
\land ys T . data-dependency-consistent-instrs T (xs@ys) = 
(data-dependency-consistent-instrs T xs \land 
data-dependency-consistent-instrs (T \cup load-tmps xs) ys \land 
load-tmps ys \cap \bigcup (fst ' store-sops xs) = \{\}) 
(proof) 

locale valid-data-dependency = 
fixes ts::('p,'p store-buffer,bool,owns,rels) thread-config list 
assumes data-dependency-consistent-instrs: 
\land i p is O D \emptyset sb. 
[i < length ts; ts!i = (p,is,\emptyset,\emptyset,D,O,R) ] \Rightarrow 
data-dependency-consistent-instrs (dom \emptyset) is 
assumes load-tmps-write-tmps-distinct: 
\land i p is O D \emptyset sb. 
[i < length ts; ts!i = (p,is,\emptyset,\emptyset,D,O,R) ] \Rightarrow 
load-tmps is \cap \bigcup (fst ' write-sops sb) = \{\} 

locale load-tmps-fresh = 
fixes ts::('p,'p store-buffer,bool,owns,rels) thread-config list 
assumes load-tmps-fresh: 
\land i p is O D \emptyset sb. 
[i < length ts; ts!i = (p,is,\emptyset,\emptyset,D,O,R) ] \Rightarrow 
load-tmps is \cap dom \emptyset = \{\} 

fun acquired-by-instrs :: instrs \Rightarrow addr set \Rightarrow addr set 
where 
acquired-by-instrs [] A = A 
| acquired-by-instrs (i#is) A = 
(case i of 
 Read - - - - \Rightarrow acquired-by-instrs is A 
| Write volatile - - A' L R W \Rightarrow acquired-by-instrs is (if volatile then (A \cup A' - R) else A) 
| RMW a t sop cond ret A' L R W \Rightarrow acquired-by-instrs is \{\} 
| Fence \Rightarrow acquired-by-instrs is \{\} 
| Ghost A' L R W \Rightarrow acquired-by-instrs is (A \cup A' - R)) 

77
fun acquired-loads :: bool ⇒ instrs ⇒ addr set ⇒ addr set

where
acquired-loads pending-write [] A = {}
| acquired-loads pending-write (i#is) A =
  (case i of
   Read volatile a - ⇒ (if pending-write ∧ ¬ volatile ∧ a ∈ A
     then insert a (acquired-loads pending-write is A)
     else acquired-loads pending-write is A)
   | Write volatile - - A′ L R W ⇒ (if volatile then acquired-loads True is (if pending-write
     then (A ∪ A′ − R) else {}))
     else acquired-loads pending-write is A)
   | RMW a t sop cond ret A′ L R W ⇒ acquired-loads pending-write is {}
   | Fence ⇒ acquired-loads pending-write is {}
   | Ghost A′ L R W ⇒ acquired-loads pending-write is (A ∪ A′ − R))

lemma acquired-by-instrs-mono:
∧ A B. A ⊆ B ⇒ acquired-by-instrs is A ⊆ acquired-by-instrs is B
⟨proof⟩

lemma acquired-by-instrs-mono-in:
assumes x-in: x ∈ acquired-by-instrs is A
assumes sub: A ⊆ B
shows x ∈ acquired-by-instrs is B
⟨proof⟩

locale enough-flushs =
fixes ts::(′p store-buffer,bool,owns,rels) thread-config list
assumes clean-no-outstanding-volatile-Write sb:
∧ i p is O R D t sb.
[i < length ts; tsl = (p,is,t,sb,D,O,R);¬ D] ⇒
(outstanding-refs is-volatile-Write sb = {})

fun prog-instrs:: ′p store-buffer ⇒ instrs
where
prog-instrs [] = []
|prog-instrs (i#is) = (case i of
  Progsb - - is′ ⇒ is′ @ prog-instrs is
  | - ⇒ prog-instrs is)

fun instrs:: ′p store-buffer ⇒ instrs
where
instrs [] = []
| instrs (i#is) = (case i of
  Write sb volatile a sop v A L R W ⇒ Write volatile a sop A L R W# instrs is
  | Read sb volatile a t v ⇒ Read volatile a t # instrs is
  | Ghost sb A L R W ⇒ Ghost A L R W# instrs is
  | - ⇒ instrs is)

locale causal-program-history =
fixes is\_sb and sb

assumes causal-program-history:
\[ \forall \text{sb}_1 \; \text{sb}_2. \; \text{sb}_1 = \text{sb}_1 @ \text{sb}_2 \implies \exists \text{is}. \; \text{instrs} \; \text{sb}_2 @ \text{is} = \text{is} @ \text{prog-instrs} \; \text{sb}_2 \]

lemma causal-program-history-empty [simp]: causal-program-history is []
(proof)

lemma causal-program-history-suffix:
causal-program-history is \( \text{sb} @ \text{sb}' \) \( \implies \) causal-program-history is \( \text{sb} \) \( \text{sb}' \)
(proof)

locale valid-program-history =
fixes ts::(p, p store-buffer, bool, owns, rels) thread-config list
assumes valid-program-history:
\[ \forall \text{i p is ORD} \theta \text{sb}. \; \begin{cases} \text{i < length ts}; & \text{ts[i] = (p, is, } \theta, \text{sb, D, O, R)} \; \implies \text{causal-program-history is sb} \end{cases} \]

assumes valid-last-prog:
\[ \forall \text{i p is ORD} \theta \text{sb}. \; \begin{cases} \text{i < length ts}; & \text{ts[i] = (p, is, } \theta, \text{sb, D, O, R)} \; \implies \text{last-prog p sb} = p \end{cases} \]

lemma (in valid-program-history) valid-program-history-nth-update:
\[ [\text{i < length ts}; \; \text{causal-program-history is sb}; \; \text{last-prog p sb} = p] \implies \text{valid-program-history (ts [i := (p, is, } \theta, \text{sb, D, O, R)])} \]
(proof)

lemma (in outstanding-non-volatile-refs-owned-or-read-only)
outstanding-non-volatile-refs-owned-instructions-read-value-independent:
\[ \forall \text{i p is ORD} \theta \text{sb}. \; \begin{cases} \text{i < length ts}; & \text{ts[i] = (p, is, } \theta, \text{sb, D, O, R)} \; \implies \text{outstanding-non-volatile-refs-owned-or-read-only S (ts[i := (p', is', } \theta', \text{sb, D', O, R')])} \end{cases} \]
(proof)

lemma (in outstanding-non-volatile-refs-owned-or-read-only)
outstanding-non-volatile-refs-owned-or-read-only-nth-update:
\[ \forall \text{i is ORD} \theta \text{sb}. \; \begin{cases} \text{i < length ts}; & \text{non-volatile-owned-or-read-only False S O sb} \implies \text{outstanding-non-volatile-refs-owned-or-read-only S (ts[i := (p, is, } \theta, \text{sb, D, O, R)])} \end{cases} \]
(proof)

lemma (in outstanding-volatile-writes-unowned-by-others)
outstanding-volatile-writes-unowned-by-others-instructions-read-value-independent:
\[ \forall \text{i p is ORD} \theta \text{sb}. \; \begin{cases} \text{i < length ts}; & \text{ts[i] = (p, is, } \theta, \text{sb, D, O, R)} \; \implies \text{outstanding-volatile-writes-unowned-by-others (ts[i := (p', is', } \theta', \text{sb, D', O, R')])} \end{cases} \]
(proof)

79
Lemma (in read-only-reads-unowned)
read-only-unowned-instructions-read-value-independent:
\[ \forall i \ p \ is \ O \ R \ D \ \not\exists \ sb. \]
\[ [i < length \ ts; \ ts!i = (p, is, \emptyset, sb, D, O, R) ] \implies \]
read-only-reads-unowned (ts[i := (p', is', \emptyset', sb, D', O, R')])
\[
\]
lemma Write\text{sb}-in-outstanding-refs:
Write\text{sb} True \ a \ sop v A L R W \in \ set \ xs \implies a \in \ outstanding-refs
\[
\]
lemma (in outstanding-volatile-writes-unowned-by-others)
outstanding-volatile-writes-unowned-by-others-store-buffer:
\[ \forall i \ p \ is \ ORD \ \not\exists \ sb. \]
\[ [i < length \ ts; \ ts!i = (p, is, \emptyset, sb, D, O, R), \]
outstanding-refs is-volatile-Write\text{sb} sb' \subseteq outstanding-refs is-volatile-Write\text{sb} sb;
all-acquired sb' \subseteq all-acquired sb] \implies \]
outstanding-volatile-writes-unowned-by-others (ts[i := (p', is', \emptyset', sb', D', O, R')])
\[
\]
lemma (in ownership-distinct)
ownership-distinct-instructions-read-value-store-buffer-independent:
\[ \forall i \ p \ is \ O \ R \ D \ \not\exists \ sb. \]
\[ [i < length \ ts; \ ts!i = (p, is, \emptyset, sb, D, O, R), \]
all-acquired sb' \subseteq all-acquired sb] \implies \]
ownership-distinct (ts[i := (p', is', \emptyset', sb', D', O, R')])
\[
\]
lemma (in ownership-distinct)
ownership-distinct-nth-update:
\[ \forall i \ p \ is \ O \ R \ D \ xs \ sb. \]
\[ [i < length \ ts; \ ts!i = (p, is, \emptyset, sb, D, O, R), \]
\[ \forall j < length \ ts. i \neq j \implies (let (p_j, is_j, sb_j, D_j, O_j, R_j) = ts!j \]
in (O' \cup all-acquired sb') \cap (O_j \cup all-acquired sb_j) = {}) ] \implies \]
ownership-distinct (ts[i := (p', is', \emptyset', sb', D', O', R')])
\[
\]
lemma (in valid-write-sops) valid-write-sops-nth-update:
\[ [i < length \ ts; \forall sop \in write-sops sb. valid-sop sop] \implies \]
valid-write-sops (ts[i := (p, is, xs, sb, D, O, R)])
\[
\]
lemma (in valid-store-sops) valid-store-sops-nth-update:
\[ [i < length \ ts; \forall sop \in store-sops is. valid-sop sop] \implies \]
valid-store-sops (ts[i := (p, is, xs, sb, D, O, R)])

(proof)

**lemma (in valid-sops) valid-sops-nth-update:**

\[ [i < \text{length } ts; \forall \text{sop } \in \text{write-sops } sb. \text{valid-sop sop}; \forall \text{sop } \in \text{store-sops } is. \text{valid-sop sop}] \implies \text{valid-sops (ts[i := (p, is, xs, sb, D, O, R)])} \]

(proof)

**lemma (in valid-data-dependency) valid-data-dependency-nth-update:**

\[ [i < \text{length } ts; \text{data-dependency-consistent-instrs (dom } \varnothing \text{) is}; \text{load-tmps } \cap \bigcup \{\text{fst } \text{write-sops } sb\} = \{\} \implies \text{valid-data-dependency (ts[i := (p, is, \varnothing, sb, D, O, R)])} \]

(proof)

**lemma (in enough-flushs) enough-flushs-nth-update:**

\[ [i < \text{length } ts; \neg D \implies (\text{outstanding-ref } \text{is-volatile-Write}_{sb} = \{\})] \implies \text{enough-flushs (ts[i := (p, is, \varnothing, sb, D, O, R)])} \]

(proof)

**lemma (in outstanding-non-volatile-writes-unshared) outstanding-non-volatile-writes-unshared-nth-update:**

\[ [i < \text{length } ts; \text{non-volatile-writes-unshared } S_{sb}] \implies \text{outstanding-non-volatile-writes-unshared } S \text{ (ts[i := (p, is, xs, sb, D, O, R)])} \]

(proof)

**lemma (in sharing-consis) sharing-consis-nth-update:**

\[ [i < \text{length } ts; \text{sharing-consistent } S \text{ O } sb] \implies \text{sharing-consis } S \text{ (ts[i := (p, is, xs, sb, D, O, R)])} \]

(proof)

**lemma (in no-outstanding-write-to-read-only-memory) no-outstanding-write-to-read-only-memory-nth-update:**

\[ [i < \text{length } ts; \text{no-write-to-read-only-memory } S_{sb}] \implies \text{no-outstanding-write-to-read-only-memory } S \text{ (ts[i := (p, is, xs, sb, D, O, R)])} \]

(proof)

**lemma in-Union-image-nth-conv:**

\[ a \in \bigcup \{f \mapsto \text{set } xs\} \implies \exists i. i < \text{length } xs \land a \in f (xs!i) \]

(proof)

**lemma in-Inter-image-nth-conv:**

\[ a \in \bigcap \{f \mapsto \text{set } xs\} = (\forall i < \text{length } xs. a \in f (xs!i)) \]

(proof)
lemma release-ownership-nth-update:
assumes R-subset: R ⊆ O
shows \[ i < \text{length ts}; \text{ts}[i] = (p, is, xs, sb, D, O, R) \]
ownership-distinct ts
\[ \implies \bigcup ((\lambda(\cdot,\cdot,\cdot,\cdot,O,.). O) ^ i \text{ set ts}[:=(p',is',xs',sb',D',O - R,R')] ) \]
\[ = ((\bigcup ((\lambda(\cdot,\cdot,\cdot,\cdot,O,.). O) ^ i \text{ set ts})) - R) \]
\[ \langle \text{proof} \rangle \]

lemma acquire-ownership-nth-update:
specializes R-subset: R ⊆ O
shows \[ i < \text{length ts}; \text{ts}[i] = (p, is, xs, sb, D, O, R) \]
\[ \implies \bigcup ((\lambda(\cdot,\cdot,\cdot,\cdot,O,.). O) ^ i \text{ set ts}[:=(p',is',xs',sb',D',O \cup A,R')] ) \]
\[ = ((\bigcup ((\lambda(\cdot,\cdot,\cdot,\cdot,O,.). O) ^ i \text{ set ts})) \cup A) \]
\[ \langle \text{proof} \rangle \]

lemma acquire-release-ownership-nth-update:
assumes R-subset: R ⊆ O
shows \[ i < \text{length ts}; \text{ts}[i] = (p, is, xs, sb, D, O, R) \]
ownership-distinct ts
\[ \implies \bigcup ((\lambda(\cdot,\cdot,\cdot,\cdot,O,.). O) ^ i \text{ set ts}[:=(p',is',xs',sb',D',O \cup A,R')] ) \]
\[ = ((\bigcup ((\lambda(\cdot,\cdot,\cdot,\cdot,O,.). O) ^ i \text{ set ts})) \cup A - R) \]
\[ \langle \text{proof} \rangle \]

lemma (in valid-history) valid-history-nth-update:
\[ i < \text{length ts}; \text{history-consistent } \emptyset \text{ (hd-prog p sb) sb } \implies \text{ valid-history program-step (ts[i] := (p, is, } \emptyset \text{, sb, D, O, R))} \]
\[ \langle \text{proof} \rangle \]

lemma (in valid-reads) valid-reads-nth-update:
\[ i < \text{length ts}; \text{reads-consistent False O m sb } \implies \text{ valid-reads m (ts[i] := (p, is, xs, sb, D, O, R))} \]
\[ \langle \text{proof} \rangle \]

lemma (in load-tmps-distinct) load-tmps-distinct-nth-update:
\[ i < \text{length ts}; \text{distinct-load-tmps is} \implies \text{ load-tmps-distinct (ts[i] := (p, is, xs, sb, D, O, R))} \]
\[ \langle \text{proof} \rangle \]

lemma (in read-tmps-distinct) read-tmps-distinct-nth-update:
\[ i < \text{length ts}; \text{distinct-read-tmps sb} \implies \text{ read-tmps-distinct (ts[i] := (p, is, xs, sb, D, O, R))} \]
\[ \langle \text{proof} \rangle \]

lemma (in load-tmps-read-tmps-distinct) load-tmps-read-tmps-distinct-nth-update:
\[ i < \text{length ts}; \text{load-tmps is } \cap \text{ read-tmps sb } = \{\} \implies \text{ load-tmps-read-tmps-distinct (ts[i] := (p, is, xs, sb, D, O, R))} \]
\[ \langle \text{proof} \rangle \]
lemma (in load-tmps-fresh) load-tmps-fresh-nth-update:

\[ i < \text{length } ts; \]
\[ \text{load-tmps is } \cap \text{dom } \emptyset = \{ \} \implies \]
\[ \text{load-tmps-fresh } (ts[i := (p, is, sb, D, O, R)]) \]

(proof)

fun flush-all-until-volatile-write::

\('p, p\text{ store-buffer, dirty, owns, rels) thread-config list } \Rightarrow \text{ memory } \Rightarrow \text{ memory}\

where

flush-all-until-volatile-write [] m = m

| flush-all-until-volatile-write ((\(_, \_, \_, sb, \_, \_\)#ts) m =
flush-all-until-volatile-write ts (flush (takeWhile (Not \(o\ is-volatile-Write_{sb}) sb) m)

fun share-all-until-volatile-write::

\('p, p\text{ store-buffer, dirty, owns, rels) thread-config list } \Rightarrow \text{ shared } \Rightarrow \text{ shared}\

where

share-all-until-volatile-write [] S = S

| share-all-until-volatile-write ((\(_, \_, \_, sb, \_, \_\)#ts) S =
share-all-until-volatile-write ts (share (takeWhile (Not \(o\ is-volatile-Write_{sb}) sb) S)

lemma buffered-val-witness: buffered-val sb a = Some v =
\exist v\ \text{volatile sop A L R W. Write}_{sb} \text{volatile a sop v A L R W } \in \text{ set sb}\

(proof)

lemma flush-append-Read_{sb}:

\forall m. (\text{flush } (\text{takeWhile } (\text{o } \text{is-volatile-Write}_{sb}) \text{ (sb @ [Read}_{sb} \text{ volatile a t v]})) m) = \text{flush } (\text{takeWhile } (\text{o } \text{is-volatile-Write}_{sb}) \text{ sb}) m\

(proof)

lemma flush-append-write:

\forall m. (\text{flush } (\text{sb @ [Write}_{sb} \text{ volatile a sop v A L R W]}) m) = (\text{flush sb m}) (a:=v)\

(proof)

lemma flush-append-Prog_{sb}:

\forall m. (\text{flush } (\text{takeWhile } (\text{o } \text{is-volatile-Write}_{sb}) \text{ (sb @ [Prog}_{sb} p_1 p_2 mis])) m) =
(\text{flush } (\text{takeWhile } (\text{o } \text{is-volatile-Write}_{sb}) \text{ sb}) m)
\(\text{lemma flush-append-Ghost}\):
\[ \forall m. \ (\text{flush} \ (\text{takeWhile} \ (\text{Not} \circ \text{is-volatile-Write}_{sb}) \ (\text{sb} \ @[\text{Ghost}_{sb} A L R W])) \ m) = \ (\text{flush} \ (\text{takeWhile} \ (\text{Not} \circ \text{is-volatile-Write}_{sb}) \ \text{sb}) \ m) \]
\(\text{(proof)}\)

\(\text{lemma share-append}\):
\[ \forall S. \ (\text{share} \ (\text{takeWhile} \ (\text{Not} \circ \text{is-volatile-Write}_{sb}) \ (\text{sb}@[\text{Read}_{sb} \ volatile a \ t v])) \ S) = \ (\text{share} \ (\text{takeWhile} \ (\text{Not} \circ \text{is-volatile-Write}_{sb}) \ \text{sb}) \ S) \]
\(\text{(proof)}\)

\(\text{lemma share-append-Read}_{sb}\):
\[ \forall S. \ (\text{share} \ (\text{takeWhile} \ (\text{Not} \circ \text{is-volatile-Write}_{sb}) \ (\text{sb}@[\text{Write}_{sb} volatile a sop v A L R W])) \ S) = \ (\text{share} \ (\text{takeWhile} \ (\text{Not} \circ \text{is-volatile-Write}_{sb}) \ \text{sb}) \ S) \]
\(\text{(proof)}\)

\(\text{lemma share-append-Prog}_{sb}\):
\[ \forall S. \ (\text{share} \ (\text{takeWhile} \ (\text{Not} \circ \text{is-volatile-Write}_{sb}) \ (\text{sb}@[\text{Prog}_{sb} p1 p2 mis])) \ S) = \ (\text{share} \ (\text{takeWhile} \ (\text{Not} \circ \text{is-volatile-Write}_{sb}) \ \text{sb}) \ S) \]
\(\text{(proof)}\)

\(\text{lemma in-acquired-no-pending-write-outstanding-write}\):
\[ a \in \text{acquired False sb A} \implies \text{outstanding-refs is-volatile-Write}_{sb} \neq \{\} \]
\(\text{(proof)}\)

\(\text{lemma flush-buffered-val-conv}\):
\[ \forall m. \ (\text{flush} \ \text{sb} \ m \ a = \ (\text{case} \ \text{buffered-val} \ \text{sb} \ a \ \text{of} \ \text{None} \Rightarrow m \ a \ | \ \text{Some} \ v \Rightarrow v) \]
\(\text{(proof)}\)

\(\text{lemma reads-consistent-unbuffered-snoc}\):
\[ \forall m. \ (\text{buffered-val} \ \text{sb} \ a = \ \text{None} \Rightarrow m \ a = v \Rightarrow \text{reads-consistent pending-write} \ \mathcal{O} \ m \ \text{sb} \]
\[ \Rightarrow \]
\[ \text{volatile} \Rightarrow \]
\[ \text{outstanding-refs is-volatile-Write}_{sb} \ \text{sb} = \{\} \]
\[ \Rightarrow \text{reads-consistent pending-write} \ \mathcal{O} \ m \ (\text{sb}@[\text{Read}_{sb} volatile a \ t v]) \]
\(\text{(proof)}\)

\(\text{lemma reads-consistent-buffered-snoc}\):
\[ \forall m. \ (\text{buffered-val} \ \text{sb} \ a = \ \text{Some} \ v \Rightarrow \text{reads-consistent pending-write} \ \mathcal{O} \ m \ \text{sb} \]
\[ \Rightarrow \]
\[ \text{volatile} \Rightarrow \text{outstanding-refs is-volatile-Write}_{sb} \ \text{sb} = \{\} \]
\[ \Rightarrow \text{reads-consistent pending-write} \ \mathcal{O} \ m \ (\text{sb}@[\text{Read}_{sb} volatile a \ t v]) \]
\(\text{(proof)}\)

84
lemma reads-consistent-snoc-Write\sb:
\(\forall m. \text{reads-consistent pending-write } O \ m \ \text{sb} \implies \text{reads-consistent pending-write } O \ m \ (\text{sb} \oplus [\text{Write}\sb \text{volatile a sop v A L R W}])\)
\(\langle \text{proof} \rangle\)

lemma reads-consistent-snoc-Prog\sb:
\(\forall m. \text{reads-consistent pending-write } O \ m \ \text{sb} \implies \text{reads-consistent pending-write } O \ m \ (\text{sb} \oplus [\text{Prog}\sb p_1 p_2 mis])\)
\(\langle \text{proof} \rangle\)

lemma reads-consistent-snoc-Ghost\sb:
\(\forall m. \text{reads-consistent pending-write } O \ m \ \text{sb} \implies \text{reads-consistent pending-write } O \ m \ (\text{sb} \oplus [\text{Ghost}\sb A L R W])\)
\(\langle \text{proof} \rangle\)

lemma restrict-map-id \[\text{simp}\] : \(\vdash \text{dom } m = m\)
\(\langle \text{proof} \rangle\)

lemma flush-all-until-volatile-write-Read-commute:
shows \(\forall m \ i. \ [i < \text{length ls}; \text{ls}!i=(p,\text{Read volatile a t#is,}\theta,\text{sb},D,O,R)] \implies \text{flush-all-until-volatile-write}\)
\[
\begin{array}{c}
\text{flush-all-until-volatile-write} \\
\text{(ls[i := (p, is', \theta(t\mapsto v), \text{sb} \oplus [\text{Read}\sb \text{volatile a t v}, D',O',R']]) m = flush-all-until-volatile-write ls m)}
\end{array}
\]
\(\langle \text{proof} \rangle\)

lemma flush-all-until-volatile-write-append-Ghost-commute:
\(\forall i \ m. \ [i < \text{length ts}; \text{ts}!i=(p,\text{is},\theta,\text{sb},D,O,R)] \implies \text{flush-all-until-volatile-write}\)
\[
\begin{array}{c}
\text{flush-all-until-volatile-write} \\
\text{(ts[i := (p',is',\theta', \text{sb} \oplus [\text{Ghost}\sb A L R W}, D',O',R'])]} m = \text{flush-all-until-volatile-write ts m}
\end{array}
\]
\(\langle \text{proof} \rangle\)

lemma update-commute:
assumes g-unchanged: \(\forall a \ m. \ a \notin G \implies g \ m \ a = m \ a\)
assumes g-independent: \(\forall a \ m. \ a \in G \implies g \ (f \ m) \ a = g \ m \ a\)
assumes f-unchanged: \(\forall a \ m. \ a \notin F \implies f \ m \ a = m \ a\)
assumes f-independent: \(\forall a \ m. \ a \in F \implies f \ (g \ m) \ a = f \ m \ a\)
assumes disj: \(G \cap F = \{\}\)
shows \(f \ (g \ m) = g \ (f \ m)\)
\(\langle \text{proof} \rangle\)

lemma update-commute':
assumes g-unchanged: \(\forall a \ m. \ a \notin G \implies g \ m \ a = m \ a\)
assumes g-independent: \(\forall a \ m_{1} m_2. \ a \in G \implies g \ m_1 \ a = g \ m_2 \ a\)
assumes f-unchanged: \(\forall a \ m. \ a \notin F \implies f \ m \ a = m \ a\)

85
**assumes** f-independent: \( \forall a m_1 m_2. a \in F \rightarrow f m_1 a = f m_2 a \)

**assumes** disj: \( G \cap F = \{ \} \)

**shows** \( f (g m) = g (f m) \)

\[(proof)\]

**lemma** flush-unchanged-addresses: \( \forall m. a \notin \text{outstanding-ref}s \text{ is-Write}_{sb} \rightarrow \text{flush sb m a} = m a \)

\[(proof)\]

**lemma** flushed-values-mem-independent:
\( \forall m m'. a \in \text{outstanding-ref}s \text{ is-Write}_{sb} \rightarrow \text{flush sb m a} = \text{flush sb m' a} \)

\[(proof)\]

**lemma** flush-all-until-volatile-write-unchanged-addresses:
\( \forall m. a \notin \bigcup (\lambda e.\text{outstanding-ref}s \text{ is-Write}_{sb} (\text{takeWhile (Not is-volatile-Write}_{sb}) \text{ sb})) \rightarrow \text{flush-all-until-volatile-write ls m a} = m a \)

\[(proof)\]

**lemma** notin-outstanding-non-volatile-takeWhile-lem:
\[ a \notin \text{outstanding-ref}s (\text{Not is-volatile}) \text{ sb} \rightarrow a \notin \text{outstanding-ref}s \text{ is-Write}_{sb} (\text{takeWhile (Not is-volatile-Write}_{sb}) \text{ sb}) \]

\[(proof)\]

**lemma** notin-outstanding-non-volatile-takeWhile-lem':
\[ a \notin \text{outstanding-ref}s \text{ is-non-volatile-Write}_{sb} \text{ sb} \rightarrow a \notin \text{outstanding-ref}s \text{ is-Write}_{sb} (\text{takeWhile (Not is-volatile-Write}_{sb}) \text{ sb}) \]

\[(proof)\]

**lemma** notin-outstanding-non-volatile-takeWhile-Un-lem':
\[ a \notin \bigcup (\lambda e.\text{outstanding-ref}s \text{ is-volatile-Write}_{sb} (\text{takeWhile (Not is-volatile-Write}_{sb}) \text{ sb})) \rightarrow a \notin \bigcup (\lambda e.\text{outstanding-ref}s \text{ is-Write}_{sb} (\text{takeWhile (Not is-volatile-Write}_{sb}) \text{ sb})) \]

\[(proof)\]

**lemma** flush-all-until-volatile-write-unchanged-addresses' :
\[ \text{assumes } \text{notin: a} \notin \bigcup (\lambda e.\text{outstanding-ref}s \text{ is-volatile-Write}_{sb} (\text{takeWhile (Not is-volatile-Write}_{sb}) \text{ sb})) \rightarrow \text{flush-all-until-volatile-write ls m a} = m a \]

\[(proof)\]

**lemma** flush-all-until-volatile-wirte-mem-independent:
\[ \forall m m'. a \in \bigcup (\lambda e.\text{outstanding-ref}s \text{ is-Write}_{sb} (\text{takeWhile (Not is-volatile-Write}_{sb}) \text{ sb})) \rightarrow \text{flush-all-until-volatile-write ls m a} = \text{flush-all-until-volatile-write ls m a} \]

\[(proof)\]

**lemma** flush-all-until-volatile-write-buffered-val-conv:
\[ \text{assumes } \text{no-volatile-Write}_{sb}: \text{outstanding-ref}s \text{ is-volatile-Write}_{sb} \text{ sb} = \{ \} \]
shows\[\forall i < \text{length } ls; ls!i = (p, is, xs, sb, D, O, R);

\forall j < \text{length } ls, i \neq j \rightarrow
\begin{align*}
&\text{(let } (\cdot, \cdot, \cdot; sb_j, \cdot, \cdot) = ls!j \\
&\text{in } a \notin \text{outstanding-refs is-non-volatile-Write}_{sb} \text{ (takeWhile (Not } \circ \text{is-volatile-Write}_{sb} \text{) sb}_j)) \implies \\
&\text{flush-all-until-volatile-write } ls \ m \ a =
\end{align*}
\text{(case buffered-val sb a of None } \Rightarrow m \ a | \text{Some } v \Rightarrow v)

\langle \text{proof} \rangle

\textbf{context} \text{ program} \\
\textbf{begin} \\
\textbf{abbreviation} sb-concurrent-step ::
\begin{align*}
&\text{(p, p store-buffer, 'dirty, 'owns, 'rels, 'shared) global-config } \Rightarrow (p, p \text{ store-buffer, 'dirty, 'owns, 'rels, 'shared) global-config } \Rightarrow \text{bool} \\
&(- \Rightarrow_{sb} - [60,60] 100)
\end{align*}
\textbf{where}
\begin{align*}
sb-concurrent-step &\equiv \\
&\text{computation.concurrent-step sb-memop-step store-buffer-step program-step } (\lambda p \ p' \text{ is sb. sb})
\end{align*}
\textbf{term} x \Rightarrow_{sb} Y

\textbf{abbreviation} (in \text{ program}) sb-concurrent-steps::
\begin{align*}
&\text{(p, p store-buffer, 'dirty, 'owns, 'rels, 'shared) global-config } \Rightarrow (p, p \text{ store-buffer, 'dirty, 'owns, 'rels, 'shared) global-config } \Rightarrow \text{bool} \\
&(- \Rightarrow_{sb} ^* - [60,60] 100)
\end{align*}
\textbf{where}
\begin{align*}
sb-concurrent-steps &\equiv sb-concurrent-step ^**
\end{align*}
\textbf{term} x \Rightarrow_{sb} ^* Y

\textbf{abbreviation} sbh-concurrent-step ::
\begin{align*}
&\text{(p, p store-buffer, bool, owns, rels, shared) global-config } \Rightarrow (p, p \text{ store-buffer, bool, owns, rels, shared) global-config } \Rightarrow \text{bool} \\
&(- \Rightarrow_{sbh} - [60,60] 100)
\end{align*}
\textbf{where}
\begin{align*}
sbh-concurrent-step &\equiv \\
&\text{computation.concurrent-step sbh-memop-step flush-step program-step } (\lambda p \ p' \text{ is sb. sb @ [Program p p' is]})
\end{align*}
\textbf{term} x \Rightarrow_{sbh} Y

\textbf{abbreviation} sbh-concurrent-steps::
\begin{align*}
&\text{(p, p store-buffer, bool, owns, rels, shared) global-config } \Rightarrow (p, p \text{ store-buffer, bool, owns, rels, shared) global-config } \Rightarrow \text{bool} \\
&(- \Rightarrow_{sbh} ^* - [60,60] 100)
\end{align*}
\textbf{where}
sbh-concurrent-steps ≡ sbh-concurrent-step* **

term x ⇒sbh* Y
end

lemma instrs-append-Readsb:
intrs (sb@[Readsb volatile a t v]) = instrs sb @ [Read volatile a t]
(proof)

lemma instrs-append-Writesb:
intrs (sb@[Writesb volatile a sop v A L R W]) = instrs sb @ [Write volatile a sop A L R W]
(proof)

lemma instrs-append-Ghostsb:
intrs (sb@[Ghostsb A L R W]) = instrs sb @ [Ghost A L R W]
(proof)

lemma prog-instrs-append-Ghostsb:
prog-intrss (sb@[Ghostsb A L R W]) = prog-intrss sb
(proof)

lemma prog-intrss-append-Readsb:
prog-intrss (sb@[Readsb volatile a t v]) = prog-intrss sb
(proof)

lemma prog-intrss-append-Writesb:
prog-intrss (sb@[Writesb volatile a sop v A L R W]) = prog-intrss sb
(proof)

lemma hd-prog-append-Readsb:
hd-prog p (sb@[Readsb volatile a t v]) = hd-prog p sb
(proof)

lemma hd-prog-append-Writesb:
hd-prog p (sb@[Writesb volatile a sop v A L R W]) = hd-prog p sb
(proof)

lemma flush-update-other: \( \forall m. a \notin \text{outstanding-refs} (\text{Not} \circ \text{is-volatile}) \) sb \( \Rightarrow \)
\( \text{outstanding-refs} (\text{is-volatile-Write}sb) \) sb = \{\} \( \Rightarrow \)
\( \text{flush} sb (m(a:=v)) = (\text{flush} sb m)(a := v) \)
(proof)

lemma flush-update-other': \( \forall m. a \notin \text{outstanding-refs} (\text{is-non-volatile-Write}sb) \) sb \( \Rightarrow \)
\( \text{outstanding-refs} (\text{is-volatile-Write}sb) \) sb = \{\} \( \Rightarrow \)
\( \text{flush} sb (m(a:=v)) = (\text{flush} sb m)(a := v) \)
(proof)

lemma flush-update-other'': \( \forall m. a \notin \text{outstanding-refs} (\text{is-non-volatile-Write}sb) \) sb \( \Rightarrow \)

88
\[ a \notin \text{outstanding-refs (is-volatile-Write}_{ab} \) sb \implies \]
\[ \text{flush sb (m(a:=v))} = (\text{flush sb m})(a := v) \]

\begin{proof}
\end{proof}

**Lemma** flush-all-until-volatile-write-update-other:
\[ \forall m. \forall j < \text{length ts}. \]
\[ (\text{let } (-,\cdot,\cdot,\cdot,\cdot,\cdot,\cdot) = \text{ts[j]} \]
\[ \text{in } a \notin \text{outstanding-refs is-non-volatile-Write}_{ab} \) sb \](j)\]
\[ \implies \]
\[ \text{flush-all-until-volatile-write ts (m(a := v))} = \]
\[ (\text{flush-all-until-volatile-write ts m})(a := v) \]

\begin{proof}
\end{proof}

**Lemma** flush-all-until-volatile-write-append-non-volatile-write-commute:
\[ \text{assumes } \neg \text{outstanding-refs is-volatile-Write}_{ab} \] sb = \{
\[ \text{shows } \forall m. \forall i. [i < \text{length ts}; \text{ts[i]} = (p, is, xs, sb, \mathcal{D}, \mathcal{O}, \mathcal{R})] \]
\[ \implies \text{flush-all-until-volatile-write (ts[i := (p',is',xs, sb @ \text{Write}_{ab} \) False a sop v A L R W],[\mathcal{D}', \mathcal{O}, \mathcal{R}']) m} = \]
\[ (\text{flush-all-until-volatile-write ts m})(a := v) \]

\begin{proof}
\end{proof}

**Lemma** flush-all-until-volatile-write-append-unflushed:
\[ \text{assumes } \neg \text{outstanding-refs is-volatile-Write}_{ab} \] sb = \{
\[ \text{shows } \forall m. \forall i. [i < \text{length ts}; \text{ts[i]} = (p, is, \theta, sb, \mathcal{D}, \mathcal{O}, \mathcal{R})] \]
\[ \implies \text{flush-all-until-volatile-write (ts[i := (p',is',\theta, sb @ sbx,\mathcal{D}', \mathcal{O}, \mathcal{R}']) m} = \]
\[ (\text{flush-all-until-volatile-write ts m}) \]

\begin{proof}
\end{proof}

**Lemma** flush-all-until-volatile-nth-update-unused:
\[ \forall m. \forall i. [i < \text{length ts}; \text{ts[i]} = (p, is, \theta, sb, \mathcal{D}, \mathcal{O}, \mathcal{R})] \]
\[ \implies \text{flush-all-until-volatile-write (ts[i := (p',is',\theta, sb, \mathcal{D}', \mathcal{O}, \mathcal{R}']) m} = \]
\[ (\text{flush-all-until-volatile-write ts m}) \]

\begin{proof}
\end{proof}

**Lemma** flush-all-until-volatile-write-append-volatile-write-commute:
\[ \text{assumes } \neg \text{outstanding-refs is-volatile-Write}_{ab} \] sb = \{
\[ \text{shows } \forall m. \forall i. [i < \text{length ts}; \text{ts[i]} = (p, is, \theta, sb, \mathcal{D}, \mathcal{O}, \mathcal{R})] \]
\[ \implies \text{flush-all-until-volatile-write (ts[i := (p',is',\theta, sb @ \text{Write}_{ab} \) True a sop v A L R W],[\mathcal{D}', \mathcal{O}, \mathcal{R}']) m} = \]
\[ (\text{flush-all-until-volatile-write ts m}) \]

\begin{proof}
\end{proof}

**Lemma** reads-consistent-update:
\[ \forall \text{pending-write O m. reads-consistent pending-write O m sb} \implies \]
\[ a \notin \text{outstanding-refs (Not o is-volatile) sb} \implies \]

89
reads-consistent pending-write $O (m(a := v)) s$ 

\langle proof \rangle

**Lemma (in program)** history-consistent-hd-prog: $\forall p. \text{history-consistent } \emptyset p' p x s \implies \text{history-consistent } \emptyset (\text{hd-prog } p \ p x s) x s$

\langle proof \rangle

**Locale** valid-program = program +

**Fixes** valid-prog

**Assumes** valid-prog-inv: $[\emptyset \vdash p \to (p',\text{is}')]$ valid-prog $p \implies$ valid-prog $p'$

**Lemma (in valid-program)** history-consistent-appendD: $\forall \emptyset y s p. \forall \text{ sop } \in \text{write-sops } x s. \text{valid-sop sop } \implies$

\begin{align*}
\text{read-tmps } x s \cap \text{read-tmps } y s &= \{\} \implies \\
\text{history-consistent } \emptyset p (x s @ y s) &\implies \\
\text{(history-consistent } \emptyset (\text{dom } \emptyset - \text{read-tmps } y s)) p x s &\land \\
\text{history-consistent } \emptyset (\text{last-prog } p x s) y s &\land \\
\text{read-tmps } y s \cap \bigcup (\text{fst } \text{write-sops } x s) &= \{\}
\end{align*}

\langle proof \rangle

**Lemma (in valid-program)** history-consistent-appendI: $\forall \emptyset y s p. \forall \text{ sop } \in \text{write-sops } x s. \text{valid-sop sop } \implies$

\begin{align*}
\text{history-consistent } \emptyset (\text{dom } \emptyset - \text{read-tmps } y s) p x s &\implies \\
\text{history-consistent } \emptyset (\text{last-prog } p x s) y s &\implies \\
\text{read-tmps } y s \cap \bigcup (\text{fst } \text{write-sops } x s) &= \{\} \implies \text{valid-prog } p \implies \\
\text{history-consistent } \emptyset p (x s @ y s)
\end{align*}

\langle proof \rangle

**Lemma (in valid-program)** history-consistent-append-conv: $\forall \emptyset y s p. \forall \text{ sop } \in \text{write-sops } x s. \text{valid-sop sop } \implies$

\begin{align*}
\text{read-tmps } x s \cap \text{read-tmps } y s &= \{\} \implies \text{valid-prog } p \implies \\
\text{history-consistent } \emptyset p (x s @ y s) = \\
\text{(history-consistent } \emptyset (\text{dom } \emptyset - \text{read-tmps } y s)) p x s &\land \\
\text{history-consistent } \emptyset (\text{last-prog } p x s) y s &\land \\
\text{read-tmps } y s \cap \bigcup (\text{fst } \text{write-sops } x s) &= \{\}
\end{align*}

\langle proof \rangle

**Lemma** instrs-takeWhile-dropWhile-conv:

\begin{align*}
\text{instrs } x s &= \text{instrs } (\text{takeWhile } P x s) @ \text{instrs } (\text{dropWhile } P x s) \\
\langle proof \rangle
\end{align*}

**Lemma (in program)** history-consistent-hd-prog-p:

$\forall p. \text{history-consistent } \emptyset p x s \implies p = \text{hd-prog } p x s$

\langle proof \rangle

**Lemma** instrs-append: $\forall y s. \text{instrs } (x s @ y s) = \text{instrs } x s @ \text{instrs } y s$

\langle proof \rangle
lemma prog-instrs-append: \( \forall y. \text{prog-instrs}(xs@ys) = \text{prog-instrs} \, xs \oplus \text{prog-instrs} \, ys \)
(proof)

lemma prog-instrs-empty: \( \forall r \in \text{set} \, xs. \neg \text{is-Prog}_{sb} \, r \implies \text{prog-instrs} \, xs = [] \)
(proof)

lemma length-dropWhile [termination-simp]: \( \text{length} \, (\text{dropWhile} \, P \, xs) \leq \text{length} \, xs \)
(proof)

lemma prog-instrs-filter-is-Prog_{sb}: \( \text{prog-instrs} \, (\text{filter} \, (\text{is-Prog}_{sb}) \, xs) = \text{prog-instrs} \, xs \)
(proof)

lemma Cons-to-snoc: \( \forall x. \exists y \, s. (x#xs) = (ys@y) \)
(proof)

lemma causal-program-history-Read:
  assumes causal-Read: causal-program-history (Read volatile a t # is_{sb}) sb
  shows causal-program-history is_{sb} (sb @ [Read_{sb} volatile a t v])
(proof)

lemma causal-program-history-Write:
  assumes causal-Write: causal-program-history (Write volatile a sop A L R W# is_{sb}) sb
  shows causal-program-history is_{sb} (sb @ [Write_{sb} volatile a sop v A L R W])
(proof)

lemma causal-program-history-Prog_{sb}:
  assumes causal-Write: causal-program-history is_{sb} sb
  shows causal-program-history (is_{sb} @ mis) (sb @ [Prog_{sb} p_1 p_2 mis])
(proof)

lemma causal-program-history-Ghost:
  assumes causal-Ghost_{sb}: causal-program-history (Ghost A L R W # is_{sb}) sb
  shows causal-program-history is_{sb} (sb @ [Ghost_{sb} A L R W])
(proof)

lemma hd-prog-last-prog-end: \[ p = \text{hd-prog} \, p \, sb ; \text{last-prog} \, p \, sb = p_{sb} \] \( \implies p = \text{hd-prog} \, p_{sb} \, sb \)
(proof)

lemma hd-prog-idem: \( \text{hd-prog} \, (\text{hd-prog} \, p \, xs) \, xs = \text{hd-prog} \, p \, xs \)
(proof)

lemma last-prog-idem: \( \text{last-prog} \, (\text{last-prog} \, p \, sb) \, sb = \text{last-prog} \, p \, sb \)
(proof)

lemma last-prog-hd-prog-append: \( \text{last-prog} \, (\text{hd-prog} \, p_{sb} \, (sb@sb')) \, sb = \text{last-prog} \, (\text{hd-prog} \, p_{sb} \, sb') \, sb \)
lemma last-prog-hd-prog: last-prog (hd-prog p xs) xs = last-prog p xs

lemma last-prog-append-Readsb:
\(\forall p. \text{last-prog} \ (sb \ @ \ [\text{Read}_{sb} \ \text{volatile} \ a \ t \ v]) = \text{last-prog} \ p \ sb\)

lemma last-prog-append-Writesb:
\(\forall p. \text{last-prog} \ (sb \ @ \ [\text{Write}_{sb} \ \text{volatile} \ a \ sop \ v \ A \ L \ R \ W]) = \text{last-prog} \ p \ sb\)

lemma last-prog-append-Progsb:
\(\forall x. \text{last-prog} \ x \ (sb @ [\text{Prog}_{sb} \ p \ p' \ mis]) = p'\)

lemma hd-prog-append-Progsb: hd-prog x (sb @ [Prog_{sb} p p' mis]) = hd-prog p sb

lemma hd-prog-append-Progsb:
\(\forall p'. \text{hd-prog} \ p' \ xs = p' \implies \text{last-prog} \ p' \ xs = p_1 \implies \text{hd-prog} \ p' \ (xs @ [\text{Prog}_{sb} \ p_1 \ p_2 \ mis]) = p'\)

lemma hd-prog-append-Ghostsb:
\(\text{hd-prog} \ p \ (sb @ [\text{Ghost}_{sb} \ A \ R \ L \ W]) = \text{hd-prog} \ p \ sb\)

lemma last-prog-append-Ghostsb:
\(\forall p. \text{last-prog} \ p \ (sb @ [\text{Ghost}_{sb} \ A \ L \ R \ W]) = \text{last-prog} \ p \ sb\)

lemma dropWhile-all-False-conv:
\(\forall x \in \text{set} \ xs. \neg \ P \ x \implies \text{dropWhile} \ P \ xs = xs\)

lemma dropWhile-append-all-False:
\(\forall y \in \text{set} \ ys. \neg \ P \ y \implies \text{dropWhile} \ P \ (xs @ ys) = \text{dropWhile} \ P \ xs @ ys\)

lemma reads-consistent-append-first:
\(\forall m \ ys. \text{reads-consistent pending-write} \ O \ m \ (xs @ ys) \implies \text{reads-consistent pending-write} \ O \ m \ xs\)
lemma reads-consistent-takeWhile:
assumes consis: reads-consistent pending-write $O m sb$
shows reads-consistent pending-write $O m (\text{takeWhile } P \text{ sb})$

proof

lemma flush-flush-all-until-volatile-write-$\text{Write}_{sb}$-volatile-commute:
$\forall \textit{i m}. \{ i < \text{length } ts; \text{ts}!i=(p,\text{is,xs,Write}_{sb}\text{ True a sop v A L R W#sb,D,O,R});$

$\forall \textit{i < \text{length } ts}. (\forall \textit{j < \text{length } ts}. \textit{i \neq j} \rightarrow$

(let (-,-,-,sb$_i$,-,-) = ts!i;

(-,-,-,sb$_j$,-,-) = ts!j

in outstanding-refs is-$\text{Write}_{sb}$ sb$_i \cap$

outstanding-refs is-$\text{Write}_{sb}$ (takeWhile (Not $\circ$ is-volatile-$\text{Write}_{sb}$ sb) sb$_j$) = \{\}));

$\forall \textit{j < \text{length } ts}. \textit{i \neq j} \rightarrow$

(let (-,-,-,sb$_j$,-,-) = ts!j in a $\notin$ outstanding-refs is-$\text{Write}_{sb}$ (takeWhile (Not $\circ$ is-volatile-$\text{Write}_{sb}$ sb) sb$_j$))$\]$

$\Rightarrow$

flush (takeWhile (Not $\circ$ is-volatile-$\text{Write}_{sb}$ sb)

((flush-all-until-volatile-write ts m)(a := v)) =

flush-all-until-volatile-write (ts[i := (p,\text{is,xs, sb, D', O',R'})])

(m(a := v))

proof

lemma (in program)
$\forall \textit{sb'} p. \text{history-consistent } \emptyset (\text{hd-prog } p (\text{sb@sb'})) (\text{sb@sb'})$ $\Longrightarrow$

last-prog p (sb@sb') = p $\Longrightarrow$

last-prog (hd-prog p (sb@sb')) sb = hd-prog p sb'$

proof

lemma last-prog-to-last-prog-same: $\forall \textit{p'. last-prog } p' \text{ sb} = p$ $\Longrightarrow$ last-prog p sb = p

proof

lemma last-prog-hd-prog-same: $[\text{last-prog } p' \text{ sb} = p; \text{ hd-prog } p' \text{ sb} = p']$ $\Longrightarrow$ hd-prog p sb = p'

proof

lemma last-prog-hd-prog-last-prog:

last-prog p' (sb@sb') = p $\Longrightarrow$ hd-prog p' (sb@sb') = p' $\Longrightarrow$

last-prog (hd-prog p sb') sb = last-prog p' sb

proof

93
lemma (in program) last-prog-hd-prog-append′:
\[ \forall sb'. p. \text{history-consistent } \theta (\text{hd-prog } p \ (\text{sb} @ sb')) (\text{sb} @ sb') \implies \\
\text{last-prog } (\text{hd-prog } p \ sb') \ sb = \text{hd-prog } p \ sb' \]

\[ \langle \text{proof} \rangle \]

lemma flush-all-until-volatile-write-Write sb-non-volatile-commute:
\[ \forall i m. [i < \text{length } ts; ts[i := (p, is, xs, Write sb False a sop v A L R W#sb, D, O, R)]; \\
\forall i < \text{length } ts. (\forall j < \text{length } ts. i \neq j \implies \\
(\text{let } (-, -, -, sb, -, -, -) = ts[i]; \\
(\text{-}, \text{-}, sb, -, -, -) = ts[j] \\
in \text{outstanding-refs is-Write sb sb} \cap \\
\text{outstanding-refs is-Write sb (takeWhile (Not o is-volatile-Write sb) sb)}) = \\
\text{}}]); \\
\forall j < \text{length } ts. i \neq j \implies \\
(\text{let } (-, -, sb, -, -, -) = ts[j] \text{ in } a / \in \text{outstanding-refs is-Write sb (takeWhile (Not o is-volatile-Write sb) sb)}) \\
\implies flush-all-until-volatile-write (ts[i := (p, is, xs, sb, D', O, R')])(m(a := v)) = \\
flush-all-until-volatile-write ts m \]

\[ \langle \text{proof} \rangle \]

lemma (in program) history-consistent-access-last-read′:
\[ \forall p. \text{history-consistent } \theta (\text{Read sb volatile a t v}) = \theta t = \text{Some v} \]

\[ \langle \text{proof} \rangle \]

lemma (in program) history-consistent-access-last-read:
\[ \text{history-consistent } \theta p (\text{rev (Read sb volatile a t v # sb)}) \implies \theta t = \text{Some v} \]

\[ \langle \text{proof} \rangle \]

lemma flush-all-until-volatile-write-Read sb-commute:
\[ \forall i m. [i < \text{length } ts; ts[i := (p, is, \emptyset, Read sb volatile a t v#sb, D, O, R)]]; \\
\implies flush-all-until-volatile-write (ts[i := (p, is, \emptyset, sb, D', O, R')]) m = \\
flush-all-until-volatile-write ts m \]

\[ \langle \text{proof} \rangle \]

lemma flush-all-until-volatile-write-Ghost sb-commute:
\[ \forall i m. [i < \text{length } ts; ts[i := (p, is, \emptyset, Ghost sb A L R W#sb, D, O, R)]]; \\
\implies flush-all-until-volatile-write (ts[i := (p', is', \emptyset', sb, D', O', R')]) m = \\
flush-all-until-volatile-write ts m \]

\[ \langle \text{proof} \rangle \]

lemma flush-all-until-volatile-write-Prog sb-commute:
\[ \forall i m. [i < \text{length } ts; ts[i := (p, is, \emptyset, Prog sb p_1 p_2 mis#sb, D, O, R)]]; \\
\implies flush-all-until-volatile-write (ts[i := (p, is, \emptyset, sb, D', O, R')]) m = \\
flush-all-until-volatile-write ts m \]

\[ \langle \text{proof} \rangle \]

lemma flush-all-until-volatile-write-append-Prog sb-commute:

94
\[ i < \text{length } ts; ts[i] = (p, is, \emptyset, sb, D, O, R) \]
\[ \implies \text{flush-all-until-volatile-write } (ts[i] = (p_2, is@mis, \emptyset, sb@[\text{Prog}_{sb} p_1 p_2 mis], D', O, R')) m \]
\[ = \text{flush-all-until-volatile-write } ts m \]  
\( \langle \text{proof} \rangle \)

**lemma (in program) history-consistent-append-\text{Prog}_{sb}:**

**assumes** step: \( \emptyset \vdash p \rightarrow p' (p', \text{mis}) \)

**shows** history-consistent \( \emptyset \) (hd-prog \( p \) xs) xs \( \implies \) last-prog \( p \) xs = \( p \) \( \implies \)

history-consistent \( \emptyset \) (hd-prog \( p' \) (xs@[\text{Prog}_{sb} p p' mis])) (xs@[\text{Prog}_{sb} p p' mis])

\( \langle \text{proof} \rangle \)

**primrec** release :: 'a memref list \( \Rightarrow \) addr set \( \Rightarrow \) rels \( \Rightarrow \) rels

**where**

release [] S R = R

| release (x#xs) S R =
  (case x of
    Write_{sb} \vdash \text{volatile} - - - A L R W \Rightarrow
        (\text{if volatile then release } xs (S \cup R - L) \text{ Map.empty}
        \text{else release } xs S R)
    | Ghost_{sb} A L R W \Rightarrow release xs (S \cup R - L) (\text{augment-rels } S R R)
    | - \Rightarrow release xs S R)

**lemma** augment-rels-shared-exchange: \( \forall a \in R. (a \in S') = (a \in S) \implies \text{augment-rels } S R R = \text{augment-rels } S' R R \)

\( \langle \text{proof} \rangle \)

**lemma** sharing-consistent-shared-exchange:

**assumes** shared-eq: \( \forall a \in \text{all-acquired } sb. S' a = S a \)

**assumes** consis: sharing-consistent \( S O sb \)

**shows** sharing-consistent \( S' O sb \)

\( \langle \text{proof} \rangle \)

**lemma** release-shared-exchange:

**assumes** shared-eq: \( \forall a \in O \cup \text{all-acquired } sb. S' a = S a \)

**assumes** consis: sharing-consistent \( S O sb \)

**shows** release sb (dom \( S' \)) R = release sb (dom S) R

\( \langle \text{proof} \rangle \)

**lemma** release-append:

95
locale xvalid-program = valid-program +

  fixes valid

assumes valid-implies-valid-prog:
  \[ i < \text{length } ts; \]
  \[ \text{ts}!i = (p,\text{is},\emptyset,\text{sb},\mathcal{D},\mathcal{O},\mathcal{R}); \text{valid } ts \implies \text{valid-prog } p \]

assumes valid-implies-valid-prog-hd:
  \[ i < \text{length } ts; \]
  \[ \text{ts}!i = (p,\text{is},\emptyset,\text{sb},\mathcal{D},\mathcal{O},\mathcal{R}); \text{valid } ts \implies \text{valid-prog } (\text{hd-prog } p \text{ sb}) \]

assumes distinct-load-tmps-prog-step:
  \[ i < \text{length } ts; \]
  \[ \text{ts}!i = (p,\text{is},\emptyset,\text{sb},\mathcal{D},\mathcal{O},\mathcal{R}); \theta \vdash p \rightarrow p (p',\text{is}'); \text{valid } ts \]
  \[ \implies \]
  \[ \text{distinct-load-tmps } \text{is}' \land \]
  \[ \text{load-tmps } \text{is}' \cap \text{load-tmps } \text{is} = \{\} \land \]
  \[ \text{load-tmps } \text{is}' \cap \text{read-tmps } \text{sb} = \{\} \]

assumes valid-data-dependency-prog-step:
  \[ i < \text{length } ts; \]
  \[ \text{ts}!i = (p,\text{is},\emptyset,\text{sb},\mathcal{D},\mathcal{O},\mathcal{R}); \theta \vdash p \rightarrow p (p',\text{is}'); \text{valid } ts \]
  \[ \implies \]
  \[ \text{data-dependency-consistent-instrs } (\text{dom } \emptyset \cup \text{load-tmps } \text{is}) \text{ is}' \land \]
  \[ \text{load-tmps } \text{is}' \cap \bigcup (\text{fst } \text{store-sops } \text{is}) = \{\} \land \]
  \[ \text{load-tmps } \text{is}' \cap \bigcup (\text{fst } \text{write-sops } \text{sb}) = \{\} \]

assumes load-tmps-fresh-prog-step:
  \[ i < \text{length } ts; \]
  \[ \text{ts}!i = (p,\text{is},\emptyset,\text{sb},\mathcal{D},\mathcal{O},\mathcal{R}); \theta \vdash p \rightarrow p (p',\text{is}'); \text{valid } ts \]
  \[ \implies \]
  \[ \text{load-tmps } \text{is}' \cap \text{dom } \emptyset = \{\} \]

assumes valid-sops-prog-step:
  \[ \theta \vdash p \rightarrow p (p',\text{is}'); \text{valid-prog } p \implies \forall \text{sop } \in \text{store-sops } \text{is}'. \text{valid-sop } \text{sop} \]

assumes prog-step-preserves-valid:
  \[ i < \text{length } ts; \]
  \[ \text{ts}!i = (p,\text{is},\emptyset,\text{sb},\mathcal{D},\mathcal{O},\mathcal{R}); \theta \vdash p \rightarrow p (p',\text{is}'); \text{valid } ts \]
  \[ \implies \]
  \[ \text{valid } (\text{ts}[i := (p',\text{is}@\text{is}',\emptyset,\text{sb}@[\text{Prog}_{\text{sb}} p p' \text{is'],}\mathcal{D},\mathcal{O},\mathcal{R}])] \]

assumes flush-step-preserves-valid:
  \[ i < \text{length } ts; \]
  \[ \text{ts}!i = (p,\text{is},\emptyset,\text{sb},\mathcal{D},\mathcal{O},\mathcal{R}); (m,\text{sb},\mathcal{O},\mathcal{R},\mathcal{S}) \rightarrow_f (m',\text{sb}',\mathcal{O}',\mathcal{R}',\mathcal{S}'); \text{valid ts} \]
  \[ \implies \]
  \[ \text{valid } (\text{ts}[i := (p,\text{is},\emptyset,\text{sb}',\mathcal{D},\mathcal{O}',\mathcal{R}'])] \]

assumes sbh-step-preserves-valid:
  \[ i < \text{length } ts; \]
\[ts!i = (p, is, \theta, sb, D, O, R)\];
\[(is, \theta, sb, m, D, O, R, S) \rightarrow_{sb} (is', \theta', sb', m', D', O', R', S')\];
valid ts] \[\Rightarrow\]
valid (ts[i:=(p, is', \theta', sb', D', O', R')])

\[\text{lemma refl'}: x = y \Rightarrow r^{*}\!
\]
\[
\text{lemma no-volatile-Read}\_sb-volatile-reads-consistent:
\[\forall m. \text{outstanding-refs is-volatile-Read}\_sb sb = \{\} \Rightarrow \text{volatile-reads-consistent m sb}\]
\[\text{proof}\]

\[\text{theorem (in program) flush-store-buffer-append:}\]
\[\text{shows} \ \forall ts p m \in O R D S \text{ is } O'.\]
\[\[i < \text{length ts};\]
\[\text{instrs} (sb@sb') @ is_{sb} = is @ \text{prog-instrs} (sb@sb');\]
\[\text{causal-program-history} is_{sb} (sb@sb');\]
\[ts!i = (p, is, \theta | (\text{dom } \theta - \text{read-tmps} (sb@sb')), x, D, O, R);\]
\[p=\text{hd-prog} p_{sb} (sb@sb');\]
\[\text{last-prog} p_{sb} (sb@sb') = p_{sb};\]
\[\text{reads-consistent} True O' m sb;\]
\[\text{history-consistent } \theta p (sb@sb');\]
\[\forall sop \in \text{write-sops} sb, \text{valid-sop} sop;\]
\[\text{distinct-read-tmps} (sb@sb');\]
\[\text{volatile-reads-consistent} m sb\]
\[\]\[\[\Rightarrow\]
\[\exists is', \text{instrs} sb' @ is_{sb} = is' @ \text{prog-instrs} sb' \land\]
\[\text{(ts,m,S)} \Rightarrow_{d^*}\]
\[\text{acquired True sb O, release sb (dom S) R]}, \text{flush sb m,share sb S}\]
\[\text{proof}\]

\[\text{corollary (in program) flush-store-buffer:}\]
\[\text{assumes i-bound: } i < \text{length ts}\]
\[\text{assumes instrs: instrs sb @ is_{sb} = is @ \text{prog-instrs} sb}\]
\[\text{assumes cph: causal-program-history is_{sb} sb}\]
\[\text{assumes ts-i: tsli = (p, is, \theta | (\text{dom } \theta - \text{read-tmps} sb), x, D, O, R)}\]
\[\text{assumes p: p=hd-prog p_{sb} sb}\]
\[\text{assumes last-prog: (last-prog p_{sb} sb) = p_{sb}}\]
\[\text{assumes reads-consis: reads-consistent} True O' m sb\]
\[\text{assumes hist-consis: history-consistent } \theta p sb\]
\[\text{assumes valid-sops: } \forall sop \in \text{write-sops} sb, \text{valid-sop sop}\]
assumes dist: distinct-read-temp sb
assumes vol-read-consis: volatile-reads-consistent m sb
shows (ts,m,S) \rightarrow^* \\
\left( ts[i:=(p_{sb},is_{sb},\emptyset,x), \\
D \lor \text{outstanding-refs is-volatile-Write}_{sb} \neq \{} \right), \text{acquired True sb } O, \text{ release sb (dom } S) R), \\
\text{flush sb m, share sb } S) \\
\langle \text{proof} \rangle

\text{lemma last-prog-same-append: } \bigwedge \text{xs } p_{sb}. \text{ last-prog } p_{sb} (sb@xs) = p_{sb} \implies \text{last-prog } p_{sb} \text{ xs} = p_{sb} \\
\langle \text{proof} \rangle

\text{lemma reads-consistent-drop-volatile-writes-no-volatile-reads: } \\
\bigwedge \text{pending-write } O m. \text{ reads-consistent pending-write } O m sb \implies \text{outstanding-refs is-volatile-Read}_{sb} ((\text{dropWhile } \text{Not } \circ \text{is-volatile-Write}_{sb}) sb) = \{} \\
\langle \text{proof} \rangle

\text{lemma reads-consistent-flush-other: } \\
\text{assumes no-volatile-Write}_{sb}-sb: \text{ outstanding-refs is-volatile-Write}_{sb} \text{ sb } = \{} \\
\text{shows } \bigwedge m \text{ pending-write } O. \text{ [outstanding-refs } (\text{Not } \circ \text{is-volatile-Read}_{sb}) \text{ xs } \cap \text{ outstanding-refs is-non-volatile-Write}_{sb} \text{ sb } = \{} ; \\
\text{reads-consistent pending-write } O m xs \text{ ] } \implies \text{reads-consistent pending-write } O (\text{flush sb m}) xs \\
\langle \text{proof} \rangle

\text{lemma reads-consistent-flush-independent: } \\
\text{assumes no-volatile-Write}_{sb}-sb: \text{ outstanding-refs is-Write}_{sb} \text{ sb } \cap \text{ outstanding-refs is-non-volatile-Read}_{sb} \text{ xs } = \{} \\
\text{assumes consis: reads-consistent pending-write } O m xs \\
\text{shows } \text{reads-consistent pending-write } O (\text{flush sb m}) xs \\
\langle \text{proof} \rangle

\text{lemma reads-consistent-flush-all-until-volatile-write-aux: } \\
\text{assumes no-reads: outstanding-refs is-volatile-Write}_{sb} \text{ xs } = \{} \\
\text{shows } \bigwedge m \text{ pending-write } O'. \text{ [reads-consistent pending-write } O' m xs; \forall i < \text{length ts. let } (p,i,s,\emptyset,D,O,R) = ts[i] \text{ in} \\
\text{outstanding-refs } (\text{Not } \circ \text{is-volatile-Read}_{sb} \text{ xs } \cap \\
\text{outstanding-refs is-non-volatile-Write}_{sb} \text{ (takeWhile } (\text{Not } \circ \text{is-volatile-Write}_{sb}) \text{ sb) } = \{} \\
\implies \text{reads-consistent pending-write } O' (\text{flush-all-until-volatile-write } ts m) xs \\
\langle \text{proof} \rangle
lemma reads-consistent-flush-other':
  assumes no-volatile-Write_{sb}: outstanding-refs is-volatile-Write_{sb} sb = {}
  shows \( \forall m. \ O \).
  \begin{align*}
    & \text{outstanding-refs is-non-volatile-Write}_{sb} sb \cap \\
    & \text{outstanding-refs is-volatile-Write}_{sb} xs \cup \\
    & \text{outstanding-refs is-non-volatile-Write}_{sb} xs \cup \\
    & \text{outstanding-refs is-non-volatile-Read}_{sb} (\text{dropWhile (Not is-volatile-Write}_{sb}) xs) \\
    & (\text{outstanding-refs is-non-volatile-Read}_{sb} (\text{takeWhile (Not is-volatile-Write}_{sb}) xs)) \\
    & \setminus \text{RO} \\
    \end{align*}
  \end{proof}

lemma reads-consistent-flush-all-until-volatile-write-aux':
  assumes no-reads: outstanding-refs is-volatile-Read_{sb} xs = {}
  assumes read-only-reads RO: read-only-reads O' (takeWhile (Not is-volatile-Write_{sb}) xs) \subseteq RO
  shows \( \forall m. \ O \m x s; \forall i < \text{length ts}.
  \begin{align*}
    & \text{let } (p_{is,\theta,\overline{sb}},D,\overline{O}) = ts!i \text{ in} \\
    & \text{outstanding-refs is-non-volatile-Write}_{sb} (\text{takeWhile (Not is-volatile-Write}_{sb}) sb) \cap \\
    & \text{outstanding-refs is-volatile-Write}_{sb} xs \cup \\
    & \text{outstanding-refs is-non-volatile-Write}_{sb} xs \cup \\
    & \text{outstanding-refs is-non-volatile-Read}_{sb} (\text{dropWhile (Not is-volatile-Write}_{sb}) xs) \\
    & (\text{outstanding-refs is-non-volatile-Read}_{sb} (\text{takeWhile (Not is-volatile-Write}_{sb}) xs)) \\
    & \setminus \text{RO} \\
    \end{align*}
  \end{proof}

lemma in-outstanding-refs-cases [consumes 1, case-names Write_{sb} Read_{sb}]:
  a \in \text{outstanding-refs P xs} \implies 
  \begin{align*}
    & (\forall \text{volatile sop v A L R W. (Write}_{sb} \text{volatile a sop v A L R W) \in set xs} \implies P \\
    & (\text{Write}_{sb} \text{volatile a sop v A L R W}) \implies C) \implies \\
    & (\forall \text{volatile t v. (Read}_{sb} \text{volatile a t v) \in set xs \implies P (Read}_{sb} \text{volatile a t v}) \implies C)
  \end{align*}
\[ \implies C \]  
\[ \text{proof} \]

**lemma** dropWhile-Cons: \((\text{dropWhile} P \, x) = x \# y s \implies \neg P \, x\)
\[ \text{proof} \]

**lemma** reads-consistent-dropWhile:
reads-consistent pending-write \(O \, m \, (\text{dropWhile} (\text{Not} \circ \text{is-volatile-Write}_{sb}) \, sb) = \)
reads-consistent True \(O \, m \, (\text{dropWhile} (\text{Not} \circ \text{is-volatile-Write}_{sb}) \, sb)\)
\[ \text{proof} \]

**theorem**
reads-consistent-flush-all-until-volatile-write:
\(\forall i \, m \, \text{pending-write. (valid-ownership-and-sharing} \, S \, ts; \)
i < \text{length} \, ts; \, ts!i = (p, \text{is}, \partial, \, sb, \, D, \, O, R); \)
reads-consistent pending-write \(O \, m \, sb \)
\(\implies \text{reads-consistent} \, \text{True} \, (\text{acquired True} \, (\text{takeWhile} (\text{Not} \circ \text{is-volatile-Write}_{sb}) \, sb) \, O) \)
\((\text{flush-all-until-volatile-write} \, ts \, m) \, (\text{dropWhile} (\text{Not} \circ \text{is-volatile-Write}_{sb}) \, sb)\)
\[ \text{proof} \]

**lemma** split-volatile-Write\(_{sb}\)-in-outstanding-refs:
\(a \in \text{outstanding-refs} \, \text{is-volatile-Write}_{sb} \, xs \implies (\exists \text{sop v y s z s A L R W. x s = y s}@(	ext{Write}_{sb}
\text{True a sop v A L R W#z s}))\)
\[ \text{proof} \]

**lemma** sharing-consistent-mono-shared:
\(\forall S \, S'. \, O. \)
\(\text{dom} \, S \subseteq \text{dom} \, S' \implies \text{sharing-consistent} \, S \, O \, sb \implies \text{sharing-consistent} \, S' \, O \, sb\)
\[ \text{proof} \]

**lemma** sharing-consistent-mono-owns:
\(\forall O \, O'. \, S. \)
\(O \subseteq O' \implies \text{sharing-consistent} \, S \, O \, sb \implies \text{sharing-consistent} \, S \, O' \, sb\)
\[ \text{proof} \]

**primrec** all-shared :: 
\(\text{'a memref list} \Rightarrow \text{addr set} \)
\[ \text{where} \]
all-shared [] = 
| all-shared (i#is) = 
| (case i of
| \text{Write}_{sb} \, \text{volatile} - - - A L R W \Rightarrow \text{(if volatile then} \, R \cup \text{all-shared is else all-shared is)}
| \text{Ghost}_{sb} A L R W \Rightarrow R \cup \text{all-shared is}
| \text{-} \Rightarrow \text{all-shared is})

**lemma** sharing-consistent-all-shared:
\(\forall S \, O. \, \text{sharing-consistent} \, S \, O \, sb \implies \text{all-shared} \, sb \subseteq \text{dom} \, S \cup O\)

100
lemma sharing-consistent-share-all-shared:
\( \forall S. \text{dom (share sb } S) \subseteq \text{dom } S \cup \text{all-shared sb} \)

\begin{proof}

primrec all-unshared :: 'a memref list \Rightarrow addr set
where
all-unshared [] = {}
| all-unshared (i#is) =
  (case i of
    Write sb volatile - - - A L R W \Rightarrow \text{(if volatile then } L \cup \text{all-unshared is else all-unshared is)}
  | Ghost sb A L R W \Rightarrow L \cup \text{all-unshared is}
  | - \Rightarrow \text{all-unshared is})

lemma all-unshared-append: all-unshared (xs @ ys) = all-unshared xs \cup \text{all-unshared ys}
\end{proof}

lemma freshly-shared-owned:
\( \forall S O. \text{sharing-consistent } S O \text{ sb } \implies \text{dom (share sb } S) - \text{dom } S \subseteq O \)
\begin{proof}

lemma unshared-all-unshared:
\( \forall S O. \text{sharing-consistent } S O \text{ sb } \implies \text{dom } S - \text{dom (share sb } S) \subseteq \text{all-unshared sb} \)
\end{proof}

lemma unshared-acquired-or-owned:
\( \forall S O. \text{sharing-consistent } S O \text{ sb } \implies \text{all-unshared sb } \subseteq \text{all-acquired sb } \cup O \)
\begin{proof}

lemma all-shared-acquired-or-owned:
\( \forall S O. \text{sharing-consistent } S O \text{ sb } \implies \text{all-shared sb } \subseteq \text{all-acquired sb } \cup O \)
\end{proof}

lemma sharing-consistent-preservation:
\( \forall S S' O.
  \begin{align*}
    & \text{sharing-consistent } S O \text{ sb;}
    & \text{all-acquired sb } \cap \text{dom } S - \text{dom } S' = \{\};
    & \text{all-unshared sb } \cap \text{dom } S' - \text{dom } S = \{\}
    \end{align*}
\implies \text{sharing-consistent } S' O \text{ sb}
\end{proof}

lemma (in sharing-consis) sharing-consis-preservation:
assumes dist:
\[
\forall i < \text{length } ts. \text{ let } (\cdot,\cdot,\cdot, sb,\cdot,\cdot,\cdot) = ts!i \text{ in }
\]
all-acquired \( sb \cap \text{dom } S - \text{dom } S' = \{ \} \) \( \land \) all-unshared \( sb \cap \text{dom } S' - \text{dom } S = \{ \} \)

shows sharing-consis \( S' \) \( ts \)

\langle proof \rangle

\textbf{lemma} (in sharing-consis) sharing-consis-shared-exchange:

\textbf{assumes} dist:
\[
\forall i < \text{length } ts. \text{ let } (\cdot,\cdot,\cdot, sb,\cdot,\cdot,\cdot) = ts!i \text{ in }
\]
all-acquired \( sb \cap \text{dom } S' a = S a \)

shows sharing-consis \( S' \) \( ts \)

\langle proof \rangle

\textbf{lemma} all-acquired-takeWhile: all-acquired \( (\text{takeWhile } P \ sb) \subseteq \text{all-acquired } sb \)

\langle proof \rangle

\textbf{lemma} all-acquired-dropWhile: all-acquired \( (\text{dropWhile } P \ sb) \subseteq \text{all-acquired } sb \)

\langle proof \rangle

\textbf{lemma} acquired-share-owns-shared:

\textbf{assumes} consis: sharing-consistent \( S \ O \ sb \)

shows acquired pending-write \( sb \ O \cup \text{dom } (\text{share } sb \ S) \subseteq O \cup \text{dom } S \)

\langle proof \rangle

\textbf{lemma} acquired-owns-shared:

\textbf{assumes} consis: sharing-consistent \( S \ O \ sb \)

shows acquired True \( sb \ O \subseteq O \cup \text{dom } S \)

\langle proof \rangle

\textbf{lemma} share-owns-shared:

\textbf{assumes} consis: sharing-consistent \( S \ O \ sb \)

shows \( \text{dom } (\text{share } sb \ S) \subseteq O \cup \text{dom } S \)

\langle proof \rangle

\textbf{lemma} all-shared-append: all-shared \( (xs@ys) = \text{all-shared } xs \cup \text{all-shared } ys \)

\langle proof \rangle

\textbf{lemma} acquired-union-notin-first:

\[ \land \text{ pending-write } A \ B. \ a \in \text{acquired pending-write } sb \ (A \cup B) \implies a \notin A \implies a \in \text{acquired pending-write } sb \ B \]

\langle proof \rangle
lemma split-all-acquired-in:
a ∈ all-acquired xs \implies
(\exists \text{sop } a' \text{ v } ys \text{ z } A \text{ L } R \text{ W}. \text{ xs } = \text{ ys } @ \text{ Write}_{ab} \text{ True } a' \text{ sop } v \text{ A } \text{ L } \text{ R } \text{ W}# \text{ z } s \land a \in A) \lor
(\exists A \text{ L } R \text{ W} \text{ y } s \text{ z } s. \text{ xs } = \text{ ys } @ \text{ Ghost}_{ab} \text{ A } \text{ L } \text{ R } \text{ W}# \text{ z } s \land a \in A)
\langle proof \rangle

lemma split-Write_{ab}-in-outstanding-refs:
a \in \text{ outstanding-refs is-Write}_{ab} \text{ xs } \implies (\exists \text{sop volatile } v \text{ y } s \text{ z } A \text{ L } R \text{ W}. \text{ xs } = \text{ y } s@ (\text{Write}_{ab} \text{ volatile } a \text{ sop } v \text{ A } \text{ L } \text{ R } \text{ W}# \text{ z } s))
\langle proof \rangle

lemma outstanding-refs-is-Write_{ab}-union:
outstanding-refs is-Write_{ab} \text{ xs } =
(\text{ outstanding-refs is-volatile-Write}_{ab} \text{ xs } \cup \text{ outstanding-refs is-non-volatile-Write}_{ab} \text{ xs})
\langle proof \rangle

lemma rtranclp-r-rtranclp: [ [r \times y; r y z] ] \implies r \times x z
\langle proof \rangle

lemma r-rtranclp-rtranclp: [ [r x y; r \times y z] ] \implies r \times x z
\langle proof \rangle

lemma unshared-is-non-volatile-Write_{ab}: \bigwedge S.
[\text{non-volatile-writes-unshared } S \text{ sb}; a \in \text{ dom } S; a \notin \text{ all-unshared sb}] \implies
a \notin \text{ outstanding-refs is-non-volatile-Write}_{ab} \text{ sb}
\langle proof \rangle

lemma outstanding-non-volatile-Read_{ab}-acquired-or-read-only-reads:
\bigwedge O S \text{ pending-write}.
[\text{non-volatile-owned-or-read-only pending-write } S \text{ O } \text{ sb}; a \in \text{ outstanding-refs is-non-volatile-Read}_{ab} \text{ sb}]\n\implies a \in \text{ acquired-reads True } \text{ sb } O \lor a \in \text{ read-only-reads } O \text{ sb}
\langle proof \rangle

lemma acquired-reads-union: \bigwedge \text{ pending-writes } A \text{ B}.
[a \in \text{ acquired-reads pending-writes sb } (A \cup B); a \notin A] \implies a \in \text{ acquired-reads pending-writes sb B}
\langle proof \rangle

lemma non-volatile-writes-unshared-no-outstanding-non-volatile-Write_{ab}: \bigwedge S S'.
[\text{non-volatile-writes-unshared } S \text{ sb}; \forall a \in \text{ dom } S' \land \text{ dom } S. a \notin \text{ outstanding-refs is-non-volatile-Write}_{ab} \text{ sb }]
\implies \text{ non-volatile-writes-unshared } S' \text{ sb}
\langle proof \rangle

103
theorem sharing-consis-share-all-until-volatile-write:
∀ S ts' [ownership-distinct ts; sharing-consis S ts; length ts' = length ts;
"∀ i < length ts. (let (-,-,-,sb,-,O,-) = ts!i;
(-,-,sb',-,O',-) = ts'!i
in O' = acquired True (takeWhile (Not ◦ is-volatile-Write a sb) O ∧
sb' = dropWhile (Not ◦ is-volatile-Write a sb)]] ⟹
sharing-consis (share-all-until-volatile-write ts S) ts' ∧

〈proof〉

corollary sharing-consistent-share-all-until-volatile-write:
assumes dist: ownership-distinct ts
assumes consis: sharing-consis S ts
assumes i-bound: i < length ts
assumes ts-i: ts!i = (p, is, θ, sb, D, O, R)

shows sharing-consistent (share-all-until-volatile-write ts S) (acquired True (takeWhile (Not ◦ is-volatile-Write a sb) O) ∧
(dropWhile (Not ◦ is-volatile-Write a sb)) sb)

〈proof〉

lemma restrict-map-UNIV [simp]: S |' UNIV = S

〈proof〉

lemma share-all-until-volatile-write-Read-commute:
shows ∀ S i. [i < length ls; ls!i=(p,Read volatile a t#is,θ,sb,D,O)]

〈proof〉

lemma share-all-until-volatile-write-Write-commute:
shows ∀ S i. [i < length ls; ls!i=(p,Write volatile a (D,f) A L R W#is,θ,sb,D,O)]

〈proof〉
\[ \text{lemma share-all-until-volatile-write-RMW-commute:} \]
\[ \text{shows } \forall i. \ [i < \text{length } ls; \text{ls}!i = (p,\text{RMW } a \ t \ (D,f) \ \text{cond ret } A \ L \ R \ W#is,\emptyset,[]),D,O) \]
\[ \implies \]
\[ \text{share-all-until-volatile-write (ls[i := (p',is, \emptyset', [],D',O'])]) S = } \]
\[ \text{share-all-until-volatile-write ls S} \]
\[ \langle \text{proof} \rangle \]

\[ \text{lemma share-all-until-volatile-write-Fence-commute:} \]
\[ \text{shows } \forall i. \ [i < \text{length } ls; \text{ls}!i = (p,\text{Fence#is},\emptyset, [],D,O,R) \]
\[ \implies \]
\[ \text{share-all-until-volatile-write (ls[i := (p,is, \emptyset, [],D',O',R'])]) S = } \]
\[ \text{share-all-until-volatile-write ls S} \]
\[ \langle \text{proof} \rangle \]

\[ \text{lemma unshared-share-in: } \forall S. \ a \in \text{dom } S \implies a \notin \text{ all-unshared sb } \implies a \in \text{ dom (share sb S)} \]
\[ \langle \text{proof} \rangle \]

\[ \text{lemma dom-eq-dom-share-eq: } \forall S S'. \ \text{dom S} = \text{dom S'} \implies \text{dom (share sb S)} = \text{dom (share sb S')} \]
\[ \langle \text{proof} \rangle \]

\[ \text{lemma share-union:} \]
\[ \forall A B. \ [a \in \text{dom (share sb (A} \oplus_z B)); a \notin \text{dom A}] \implies a \in \text{dom (share sb (Map.empty} \oplus_z B)) \]
\[ \langle \text{proof} \rangle \]

\[ \text{lemma share-unshared-in:} \]
\[ \forall S. \ a \in \text{dom (share sb S)} \implies a \in \text{dom (share sb Map.empty)} \lor (a \in \text{dom S} \land a \notin \text{all-unshared sb}) \]
\[ \langle \text{proof} \rangle \]
lemma dom-augment-rels-shared-eq: dom (augment-rels S R R) = dom (augment-rels S' R R)
⟨proof⟩

lemma dom-eq-SomeD1: dom m = dom n ⇒ m x = Some y ⇒ n x ≠ None
⟨proof⟩

lemma dom-eq-SomeD2: dom m = dom n ⇒ n x = Some y ⇒ m x ≠ None
⟨proof⟩

lemma dom-augment-rels-rels-eq: dom R' = dom R ⇒ dom (augment-rels S R R') = dom (augment-rels S R R)
⟨proof⟩

lemma dom-release-rels-eq: ⋀ S R R'. dom R' = dom R ⇒ dom (release sb S R') = dom (release sb S R)
⟨proof⟩

lemma dom-release-shared-eq: ⋀ S S'. dom (release sb S R) = dom (release sb S' R)
⟨proof⟩

lemma share-other-untouched:
⋀ O S. sharing-consistent S O sb ⇒ a ∉ O ∪ all-acquired sb⇒ share sb S a = S a
⟨proof⟩

lemma shared-owned: ⋀ O S. sharing-consistent S O sb ⇒ a ∉ dom S ⇒ a ∈ dom (share sb S)
a ∈ O ∪ all-acquired sb
⟨proof⟩

lemma share-all-shared-in: a ∈ dom (share sb S) ⇒ a ∈ dom S ∨ a ∈ all-shared sb
⟨proof⟩

lemma share-all-until-volatile-write-unowned:
assumes dist: ownership-distinct ts
assumes consis: sharing-consis S ts
assumes other: ∀ i p is ⊥ sb D O R. i < length ts ⇒ tsi = (p, is, ⊥, sb, D, O, R) ⇒ a ∉ O ∪ all-acquired sb
shows share-all-until-volatile-write ts S a = S a
⟨proof⟩

lemma share-shared-eq: ⋀ S' S. S' a = S a ⇒ share sb S' a = share sb S a
⟨proof⟩
lemma share-all-until-volatile-write-thread-local:
assumes dist: ownership-distinct ts
assumes consis: sharing-consis \( S \) ts
assumes i-bound: \( i < \) length ts
assumes ts-i: ts\!i = (p, is, 0, sb, D, O, R)
assumes a-owned: a \in O \cup all-acquired sb
shows share-all-until-volatile-write ts \( S \) a = share \( (\text{takeWhile} (\text{Not} \circ \text{is-volatile-Write}_{sb}) \) sb) \( S \) a
⟨proof⟩

lemma share-all-until-volatile-write-thread-local':
assumes dist: ownership-distinct ts
assumes consis: sharing-consis \( S \) ts
assumes i-bound: \( i < \) length ts
assumes ts-i: ts\!i = (p, is, 0, sb, D, O, R)
assumes a-owned: a \in O \cup all-acquired sb
shows \( \text{share} \) \( (\text{dropWhile} (\text{Not} \circ \text{is-volatile-Write}_{sb}) \) sb) \( (\text{share-all-until-volatile-write ts} \) \( S \) a = \text{share sb} \( S \) a
⟨proof⟩

lemma (in ownership-distinct) in-shared-sb-share-all-until-volatile-write:
assumes consis: sharing-consis \( S \) ts
assumes i-bound: \( i < \) length ts
assumes ts-i: ts\!i = (p, is, 0, sb, D, O, R)
assumes a-owned: a \in O \cup all-acquired sb
assumes a-share: a \in \text{dom} \( \text{share sb} \) \( S \) a
shows a \in \text{dom} \( \text{share} \) \( (\text{dropWhile} (\text{Not} \circ \text{is-volatile-Write}_{sb}) \) sb) \( (\text{share-all-until-volatile-write ts} \) \( S \) a
⟨proof⟩

lemma owns-unshared-share-acquired:
\( \forall S \ O. \ [\text{sharing-consistent} \ S \ O \ sb; a \in O; a \notin \text{all-unshared sb}] \)
\implies a \in \text{dom} \( \text{share sb} \) \( S \) a \cup \text{acquired True sb O}
⟨proof⟩

lemma shared-share-acquired: \( \forall S \ O. \ \text{sharing-consistent} \ S \ O \ sb \implies a \in \text{dom} \ S \implies a \in \text{dom} \ (\text{share sb} \ S) \cup \text{acquired True sb O}
⟨proof⟩

lemma dom-release-takeWhile:
\( \forall S \ R. \ \text{dom} \ (\text{release (takeWhile} (\text{Not} \circ \text{is-volatile-Write}_{sb}) \) sb) \ S \ R) = \text{dom} \ R \cup \text{all-shared} \ (\text{takeWhile} (\text{Not} \circ \text{is-volatile-Write}_{sb}) \) sb)
⟨proof⟩

lemma share-all-until-volatile-write-share-acquired:
assumes dist: ownership-distinct ts
assumes consis: sharing-consis \( S \) ts

107
assumes a-notin: \( a \notin \text{dom } S \)
assumes a-in: \( a \in \text{dom } (\text{share-all-until-volatile-write ts } S) \)
shows \( \exists i < \text{length ts}. \)
\[
\text{let } (\cdot,\cdot,\cdot,\cdot,\cdot,\cdot) = \text{ts}!i \\
\text{in } a \in \text{all-shared } (\text{takeWhile } (\text{Not } \circ \text{is-volatile-Write}_{sb}) \text{ sb})
\]
\langle proof \rangle

lemma all-shared-share-acquired: \( \forall S O. \text{sharing-consistent } S O \text{ sb } \implies \)
\( a \in \text{all-shared sb } \implies a \in \text{dom } (\text{share sb } S) \cup \text{acquired True sb } O \)
\langle proof \rangle

lemma (in ownership-distinct) share-all-until-volatile-write-share-acquired:
assumes consis: \( \text{sharing-consis } S \text{ ts} \)
assumes i-bound: \( i < \text{length ts} \)
assumes ts-i: \( \text{ts}!i = (p,\cdot,\cdot,\cdot,\cdot,\cdot,\cdot) \) \( \text{ts} \) \( i \)
assumes a-in: \( a \in \text{dom } (\text{share-all-until-volatile-write ts } S) \)
shows \( a \in \text{dom } (\text{share sb } S) \lor a \in \text{acquired True sb } O \lor \)
\( (\exists j < \text{length ts}. \ j \neq i \land \)
\( \text{let } (\cdot,\cdot,\cdot,\cdot,\cdot,\cdot) = \text{ts}!j \\
\text{in } a \in \text{all-shared } (\text{takeWhile } (\text{Not } \circ \text{is-volatile-Write}_{sb}) \text{ sb}_j)) \)
\langle proof \rangle

lemma acquired-all-shared-in:
\( \forall A. \ a \in \text{acquired True sb } A \implies a \in \text{acquired True sb } \{ \} \lor (a \in A \land a \notin \text{all-shared sb}) \)
\langle proof \rangle

lemma all-shared-acquired-in: \( \forall A. \ a \in A \implies a \notin \text{all-shared sb } \implies a \in \text{acquired True sb } A \)
\langle proof \rangle

lemma owned-share-acquired: \( \forall S O. \text{sharing-consistent } S O \text{ sb } \implies \)
\( a \in O \implies a \in \text{dom } (\text{share sb } S) \cup \text{acquired True sb } O \)
\langle proof \rangle

lemma outstanding-refs-non-volatile-Read\_\text{ab}-all-acquired:
\( \forall m S O \text{ pending-write.} \)
\text{reads-consistent pending-write } O \text{ m sb;non-volatile-owned-or-read-only pending-write } S O \text{ sb;}
\( a \in \text{outstanding-refs is-non-volatile-Read\_\text{ab } sb}] \)
\implies a \in O \lor a \in \text{all-acquired sb } \lor \)
\( a \in \text{read-only-reads } O \text{ sb} \)
\langle proof \rangle
lemma outstanding-refs-non-volatile-Read_{sb}-all-acquired-dropWhile:
assumes consis: reads-consistent pending-write O m sb
assumes nvo: non-volatile-owned-or-read-only pending-write S O sb
assumes out: a ∈ outstanding-refs is-non-volatile-Read_{sb} (dropWhile (Not o is-volatile-Write_{sb}) sb)
shows a ∈ O ∨ a ∈ all-acquired sb ∨ a ∈ read-only-reads O sb
⟨proof⟩

lemma share-commute:
\[ \bigwedge L R S O. [sharing-consistent S O sb; all-shared sb ∩ L = \{\}; all-shared sb ∩ A = \{\}; all-acquired sb ∩ R = \{\}; all-unshared sb ∩ R = \{\}] \rightarrow \]
\[ (share sb (S ⊕ W R ⊖ A L)) = (share sb S) ⊕ W R ⊖ A L \]
⟨proof⟩

lemma share-append-Ghost_{sb}:
\[ \bigwedge S. \text{outstanding-refs is-volatile-Write}_{sb} sb = \{\} \implies (share (sb @ [Ghost_{sb} A L R W])) S = (share sb S) ⊕ W R ⊖ A L \]
⟨proof⟩

lemma share-append-Ghost_{sb}′:
\[ \bigwedge S. \text{outstanding-refs is-volatile-Write}_{sb} sb ≠ \{\} \implies \]
\[ (share (takeWhile (Not o is-volatile-Write_{sb}) (sb @ [Ghost_{sb} A L R W]))) S) = (share (takeWhile (Not o is-volatile-Write_{sb}) sb) S) \]
⟨proof⟩

lemma share-all-until-volatile-write-append-Ghost_{sb}:
\textbf{assumes} no-out-VWrite\textsubscript{sb}: outstanding-refs is-volatile-Write\textsubscript{sb} \text{ sb} = \{\}

\textbf{shows} \bigwedge S \text{ i. [ownership-distinct ts; sharing-consis S ts; i < length ts; tsli = (p, is, \emptyset, sb, D, O, R);}
\forall j p is \mathcal{O} \mathcal{R} D \emptyset sb. j < length ts \rightarrow i \neq j \rightarrow tslj = (p, is, \emptyset, sb, D, O, R) \rightarrow
all-shared (takeWhile (Not is-volatile-Write\textsubscript{sb}) sb) \cap L = \{\};
\forall j p is \mathcal{O} \mathcal{R} D \emptyset sb. j < length ts \rightarrow i \neq j \rightarrow tslj = (p, is, \emptyset, sb, D, O, R) \rightarrow
all-shared (takeWhile (Not is-volatile-Write\textsubscript{sb}) sb) \cap A = \{\};
\forall j p is \mathcal{O} \mathcal{R} D \emptyset sb. j < length ts \rightarrow i \neq j \rightarrow tslj = (p, is, \emptyset, sb, D, O, R) \rightarrow
all-acquired (takeWhile (Not is-volatile-Write\textsubscript{sb}) sb) \cap R = \{\};
\forall j p is \mathcal{O} \mathcal{R} D \emptyset sb. j < length ts \rightarrow i \neq j \rightarrow tslj = (p, is, \emptyset, sb, D, O, R) \rightarrow
all-shared (takeWhile (Not is-volatile-Write\textsubscript{sb}) sb) \cap R = \{\}
\implies
share-all-until-volatile-write (ts[i := (p', is', \emptyset', sb @ [Ghost\textsubscript{sb} A L R W], D', O)]) S
= share-all-until-volatile-write ts S \oplus W R \ominus A L
\langle proof \rangle

\textbf{lemma} share-domain-changes:
\bigwedge S S'. a \in all-shared sb \cup all-unshared sb \implies share sb S' a = share sb S a
\langle proof \rangle

\textbf{lemma} share-domain-changesX:
\bigwedge S S' X. \forall a \in X. S' a = S a
\implies a \in all-shared sb \cup all-unshared sb \cup X \implies share sb S' a = share sb S a
\langle proof \rangle

\textbf{lemma} share-unchanged:
\bigwedge S. a \notin all-shared sb \cup all-unshared sb \cup all-acquired sb \implies share sb S a = S a
\langle proof \rangle

\textbf{lemma} share-augment-release-commute:
\textbf{assumes} dist: (R \cup L \cup A) \cap (all-shared sb \cup all-unshared sb \cup all-acquired sb) = \{\}
\textbf{shows} (share sb S \oplus W R \ominus A L) = share sb (S \oplus W R \ominus A L)
\langle proof \rangle

\textbf{lemma} share-append-commute:
\bigwedge ys S. (all-shared xs \cup all-unshared xs \cup all-acquired xs) \cap
(all-shared ys \cup all-unshared ys \cup all-acquired ys) = \{\}
\implies share xs (share ys S) = share ys (share xs S)
\langle proof \rangle

\textbf{lemma} share-append-commute':
\textbf{assumes} dist: (all-shared xs \cup all-unshared xs \cup all-acquired xs) \cap
shows \((\text{all-shared } ys \cup \text{all-unshared } ys \cup \text{all-acquired } ys) = \{\}\)

\(\text{lemma share-all-until-volatile-write-share-commute:}\)

\(\text{shows } \forall S. \left( (\text{all-shared } (\text{takeWhile } (\text{Not } \circ \text{is-volatile-Write}_{sb}) sb) \cup \text{all-unshared } (\text{takeWhile } (\text{Not } \circ \text{is-volatile-Write}_{sb}) sb) \cup \text{all-acquired } (\text{takeWhile } (\text{Not } \circ \text{is-volatile-Write}_{sb}) sb)) \cap (\text{all-shared } sb' \cup \text{all-unshared } sb' \cup \text{all-acquired } sb') = \{\}\right)\)

\(\Rightarrow\)

\(\text{share-all-until-volatile-write } ts (\text{share } sb' S) = \text{share } sb' (\text{share-all-until-volatile-write } ts S)\)

\(\text{lemma all-shared-takeWhile-subset: all-shared } (\text{takeWhile } P sb) \subseteq \text{all-shared } sb\)

\(\text{lemma all-shared-dropWhile-subset: all-shared } (\text{dropWhile } P sb) \subseteq \text{all-shared } sb\)

\(\text{lemma all-unshared-takeWhile-subset: all-unshared } (\text{takeWhile } P sb) \subseteq \text{all-unshared } sb\)

\(\text{lemma all-unshared-dropWhile-subset: all-unshared } (\text{dropWhile } P sb) \subseteq \text{all-unshared } sb\)

\(\text{lemma all-acquired-takeWhile-subset: all-acquired } (\text{takeWhile } P sb) \subseteq \text{all-acquired } sb\)

\(\text{lemma all-acquired-dropWhile-subset: all-acquired } (\text{dropWhile } P sb) \subseteq \text{all-acquired } sb\)

\(\text{lemma share-all-until-volatile-write-flush-commute:}\)

\(\text{assumes takeWhile-empty: } (\text{takeWhile } (\text{Not } \circ \text{is-volatile-Write}_{sb}) sb) = []\)

\(\text{shows } \forall S R L W A i. \left( (\text{ownership-distinct } ts; \text{sharing-consis } S ts; i < \text{length } ts;\right)\)

\(\Rightarrow\)

\(\forall j p is O R D \emptyset (sb::'a memref list). j < \text{length } ts \rightarrow i \neq j\)

\(\Rightarrow\)

\(\forall j p is O R D \emptyset (sb::'a memref list). j < \text{length } ts \rightarrow i \neq j\)

\(\Rightarrow\)

\(\forall j p is O R D \emptyset (sb::'a memref list). j < \text{length } ts \rightarrow i \neq j\)

\(\Rightarrow\)

\(\forall j p is O R D \emptyset (sb::'a memref list). j < \text{length } ts \rightarrow i \neq j\)

\(\Rightarrow\)

\(\forall j p is O R D \emptyset (sb::'a memref list). j < \text{length } ts \rightarrow i \neq j\)
\[
\text{share-all-until-volatile-write} \ (\text{ts}[i := (p', \text{is}', \theta', \text{sb}', D', O', R')]) \ (S \oplus W R \ominus A L) = \\
\text{share} \ (\text{takeWhile} \ (\text{Not} \circ \text{is-volatile-Write}_{\text{sb}}) \ \text{sb}') \ (\text{share-all-until-volatile-write} \ \text{ts} \ S \oplus W R \ominus A L) \\
\langle \text{proof} \rangle
\]

**Lemma** share-all-until-volatile-write-Ghost\(_{\text{sb}}\)-commute:

**shows** \(\forall S. \ [\text{ownership-distinct ts}; \ \text{sharing-consis} \ S \ \text{ts}; \ i < \text{length ts}; \)

\[
\text{ts}[i] = (p, \text{is}, \theta, \text{Ghost}_{\text{sb}} A L R W, D, O, R)
\]

\[
\forall j \ p \ \text{is-ORD} \ \theta \ \text{sb}. \ j < \text{length ts} \rightarrow i \neq j \rightarrow \text{ts}[j] = (p, \text{is}, \theta, \text{sb}, D, O, R) \rightarrow \\
(\text{all-shared} \ (\text{takeWhile} \ (\text{Not} \circ \text{is-volatile-Write}_{\text{sb}}) \ \text{sb}) \cup \text{all-unshared} \ (\text{takeWhile} \ (\text{Not} \circ \text{is-volatile-Write}_{\text{sb}}) \ \text{sb}) \cup \text{all-acquired} \ (\text{takeWhile} \ (\text{Not} \circ \text{is-volatile-Write}_{\text{sb}}) \ \text{sb})) \cap
\]

\[
(R \cup L \cup A) = \{\}
\]

\[
\implies \text{share-all-until-volatile-write} \ (\text{ts}[i := (p', \text{is}', \theta', \text{sb}', D', O', R')]) \ (S \oplus W R \ominus A L) = \\
\text{share-all-until-volatile-write} \ \text{ts} \ S
\]

\langle \text{proof} \rangle

**Lemma** share-all-until-volatile-write-update-sb:

**assumes** congr:

\[
\forall S. \ [\text{share} \ (\text{takeWhile} \ (\text{Not} \circ \text{is-volatile-Write}_{\text{sb}}) \ \text{sb}') \ S = \text{share} \ (\text{takeWhile} \ (\text{Not} \circ \text{is-volatile-Write}_{\text{sb}}) \ \text{sb}) \ S]
\]

**shows** \(\forall S. \ i < \text{length ts}; \ \text{ts}[i] = (p, \text{is}, \theta, \text{sb}, D, O, R)
\]

\[
\implies \text{share-all-until-volatile-write} \ \text{ts} \ S = \\
\text{share-all-until-volatile-write} \ (\text{ts}[i := (p', \text{is}', \theta', \text{sb}, D', O', R')]) \ S
\]

\langle \text{proof} \rangle

**Lemma** acquired-append-Prog\(_{sb}\):

\[
\forall S. \ (\text{acquired pending-write} \ (\text{takeWhile} \ (\text{Not} \circ \text{is-volatile-Write}_{\text{sb}}) \ (\text{sb} \ @ \ [\text{Prog}_{\text{sb}} p_1 p_2 \ \text{mis}]))) \ S) = \\
(\text{acquired pending-write} \ (\text{takeWhile} \ (\text{Not} \circ \text{is-volatile-Write}_{\text{sb}}) \ \text{sb}) \ S)
\]

\langle \text{proof} \rangle

**Lemma** outstanding-refs-non-empty-dropWhile:

\[
\text{outstanding-refs} \ P \ \text{xs} \neq \{\} \implies \text{outstanding-refs} \ P \ (\text{dropWhile} \ (\text{Not} \circ P) \ \text{xs}) \neq \{\}
\]

\langle \text{proof} \rangle

**Lemma** ex-not: Ex Not

112
lemma (in computation) concurrent-step-append:
  assumes step: \((ts,m,S) \Rightarrow (ts',m',S')\)
  shows \((xs@ts,m,S) \Rightarrow (xs@ts',m',S')\)
⟨proof⟩

primrec weak-sharing-consistent:: owns ⇒ 'a memref list ⇒ bool
where
weak-sharing-consistent \(O []\) = True
| weak-sharing-consistent \(O (r#rs)\) =
  (case r of
    Write\(_ab\) volatile - - \(-\) A L R W ⇒
      (if volatile then L ⊆ A ∧ A ∩ R = \{\} ∧ R ⊆ O ∧
        weak-sharing-consistent \((O ∪ A − R) rs\)
      else weak-sharing-consistent \(O rs\))
  | Ghost\(_ab\) A L R W ⇒ L ⊆ A ∧ A ∩ R = \{\} ∧ R ⊆ O ∧ weak-sharing-consistent \((O ∪ A − R) rs\)
  | - ⇒ weak-sharing-consistent \(O rs\))

lemma sharing-consistent-weak-sharing-consistent:
\(\forall S O.\) sharing-consistent \(S O sb\) ⇒ weak-sharing-consistent \(O sb\)
⟨proof⟩

lemma weak-sharing-consistent-append:
\(\forall O.\) weak-sharing-consistent \(O (xs @ ys)\) =
  (weak-sharing-consistent \(O xs\) ∧ weak-sharing-consistent (acquired True \(xs O\)) \(ys\))
⟨proof⟩

lemma read-only-share-unowned: \(\forall O. S.\)
\[\text{[weak-sharing-consistent } O sb; a \notin O ∪ \text{all-acquired } sb; a \in \text{read-only } (\text{share } sb S)\]
  ⇒ a ∈ read-only \(S\)
⟨proof⟩
lemma share-read-only-mono-in:
  assumes a-in: a ∈ read-only (share sb S)
  assumes ss: read-only S ⊆ read-only S'
  shows a ∈ read-only (share sb S')
⟨proof⟩

lemma read-only-unacquired-share:
  \(\forall S \ O. \ [O \cap \text{read-only } S = \{\} ; \text{weak-sharing-consistent } O \ sb; a \in \text{read-only } S; a \notin \text{all-acquired } sb]\)
  \(\implies a \in \text{read-only (share sb S)}\)
⟨proof⟩

lemma read-only-share-unacquired:
  \(\forall O \ S. \ [O \cap \text{read-only } S = \{\} \implies\text{weak-sharing-consistent } O \ sb \implies a \in \text{read-only (share sb S)} \implies a \notin \text{acquired True sb } O\)
⟨proof⟩

lemma read-only-share-all-acquired-in:
  \(\forall S \ O. \ [O \cap \text{read-only } S = \{\} ; \text{weak-sharing-consistent } O \ sb; a \in \text{read-only (share sb S)}]\)
  \(\implies a \in \text{read-only (share sb Map.empty) } \lor (a \in \text{read-only } S \land a \notin \text{all-acquired sb})\)
⟨proof⟩

lemma weak-sharing-consistent-preserves-distinct:
  \(\forall O \ S. \ \text{weak-sharing-consistent } O \ sb \implies O \cap \text{read-only } S = \{\} \implies a \in \text{acquired True sb } O \implies\text{read-only (share sb S)} = \{\}\)
⟨proof⟩

locale weak-sharing-consis =
  fixes ts::('p, 'p store-buffer, bool, owns, rels) thread-config list
  assumes weak-sharing-consis:
  \(\forall i \ p \ is \ O \ R \ D \ \partial sb. \ [i < \text{length } ts; ts!i = (p, is, \partial sb, D, O, R)] \implies \text{weak-sharing-consistent } O \ sb\)

sublocale sharing-consis ⊆ weak-sharing-consis
⟨proof⟩

lemma weak-sharing-consis-tl: weak-sharing-consis (t#ts) \(\implies\) weak-sharing-consis ts
⟨proof⟩
lemma read-only-share-all-until-volatile-write-unacquired:
\[ \forall S. \text{[ownership-distinct ts; read-only-unowned S ts; weak-sharing-consis ts; \forall i < \text{length ts}. (let (\_\_\_\_\_, sb, \_\_\_\_\_, O, R) = ts!i in a \notin \text{all-acquired} (\text{takeWhile} (\text{Not} \circ \text{is-volatile-Write}_{sb}) sb)); a \in \text{read-only S}] \implies a \in \text{read-only (share-all-until-volatile-write ts S)}} \]
\[ \langle \text{proof} \rangle \]

lemma read-only-share-unowned-in:
\[ [\text{weak-sharing-consistent O sb; a \in \text{read-only (share sb S)}]} \implies a \in \text{read-only S} \cup O \cup \text{all-acquired sb} \]
\[ \langle \text{proof} \rangle \]

lemma read-only-shared-all-until-volatile-write-subset:
\[ \forall S. \text{[ownership-distinct ts; weak-sharing-consis ts]} \implies \text{read-only (share-all-until-volatile-write ts S)} \subseteq \text{read-only S} \cup O \cup \text{all-acquired (takeWhile (\text{Not} \circ \text{is-volatile-Write}_{sb}) sb)} \]
\[ \langle \text{proof} \rangle \]

lemma weak-sharing-consistent-preserves-distinct-share-all-until-volatile-write:
\[ \forall S i. \text{[ownership-distinct ts; read-only-unowned S ts;weak-sharing-consis ts; i < \text{length ts}; ts!i = (p, is, \_\_\_\_\_, sb, \_\_\_\_\_, O, R)]} \implies \text{acquired True (\text{takeWhile} (\text{Not} \circ \text{is-volatile-Write}_{sb}) sb) O \cap read-only (share-all-until-volatile-write ts S) = \{\}} \]
\[ \langle \text{proof} \rangle \]

lemma in-read-only-share-all-until-volatile-write:
assumes dist: ownership-distinct ts
assumes consis: sharing-consis S ts
assumes ro-unowned: read-only-unowned S ts
assumes i-bound: i < \text{length ts}
assumes ts-i: ts!i = (p, is, \_\_\_\_\_, sb, D, O, R)
assumes a-unacquired-others: \forall j < \text{length ts}. i \neq j \rightarrow
\[ \text{(let (\_\_\_\_\_, sb, \_\_\_\_\_, O) = ts!j in a \notin \text{all-acquired} (\text{takeWhile} (\text{Not} \circ \text{is-volatile-Write}_{sb}) sb))} \]
assumes a-ro-share: a \in \text{read-only (share sb S)}
shows a \in \text{read-only (share (dropWhile (\text{Not} \circ \text{is-volatile-Write}_{sb}) sb) (share-all-until-volatile-write ts S))}
\[ \langle \text{proof} \rangle \]

lemma all-acquired-dropWhile-in: x \in \text{all-acquired (dropWhile P sb)} \implies x \in \text{all-acquired sb}
\[ \langle \text{proof} \rangle \]
lemma all-acquired-takeWhile-in: \( x \in \text{all-acquired} \text{ (takeWhile P sb)} \implies x \in \text{all-acquired} \text{ sb} \)

\(\langle \text{proof} \rangle\)

lemmas all-acquired-takeWhile-dropWhile-in = all-acquired-takeWhile-in all-acquired-dropWhile-in

lemma split-in-read-only-reads:
\( \bigwedge O. \ a \in \text{read-only-reads} \ O \ xs \implies \)

(\( \exists t \ v \ ys \ zs. \ xs = ys @ \text{Read}_{\text{sb}} \text{ False} \ a \ t \ \# \ zs \ \& \ a \ \notin \text{acquired} \text{ True} \ ys \ O) \)

\(\langle \text{proof} \rangle\)

lemma insert-monoD: \( W \subseteq W' \implies \text{insert} \ a \ W \subseteq \text{insert} \ a \ W' \)

\(\langle \text{proof} \rangle\)

primrec unforwarded-non-volatile-reads:: 'a memref list \Rightarrow \text{addr set} \Rightarrow \text{addr set}

where
unforwarded-non-volatile-reads [] W = {}

| unforwarded-non-volatile-reads (x#xs) W =

\( \text{(case x of} \)

Read_{\text{sb}} \text{ volatile} \ a \ - \ - \ \Rightarrow \ (\text{if} \ a \ \notin \ W \ \& \ \neg \ \text{volatile}

\text{then} \ \text{insert} \ a \ (\text{unforwarded-non-volatile-reads} \text{ xs} \ W)

\text{else} \ (\text{unforwarded-non-volatile-reads} \text{ xs} \ W)) \)

| Write_{\text{sb}} \ - \ a \ - \ - \ - \ - \ \Rightarrow \ \text{unforwarded-non-volatile-reads} \text{ xs} \ (\text{insert} \ a \ W)

| - \ \Rightarrow \ \text{unforwarded-non-volatile-reads} \text{ xs} \ W) \)

lemma unforwarded-non-volatile-reads-non-volatile-Read_{\text{sb}}:
\( \bigwedge W. \ \text{unforwarded-non-volatile-reads} \text{ sb} \ W \subseteq \text{outstanding-refs} \text{ is-non-volatile-Read}_{\text{sb}} \text{ sb} \)

\(\langle \text{proof} \rangle\)

lemma in-unforwarded-non-volatile-reads-non-volatile-Read_{\text{sb}}:
\( a \in \text{unforwarded-non-volatile-reads} \text{ sb} \ W \implies a \in \text{outstanding-refs} \text{ is-non-volatile-Read}_{\text{sb}} \text{ sb} \)

\(\langle \text{proof} \rangle\)

lemma unforwarded-non-volatile-reads-antimono:
\( \bigwedge W \ W'. \ W \subseteq W' \implies \text{unforwarded-non-volatile-reads} \text{ xs} \ W' \subseteq \text{unforwarded-non-volatile-reads} \text{ xs} \ W \)

\(\langle \text{proof} \rangle\)

lemma unforwarded-non-volatile-reads-antimono-in:
\( x \in \text{unforwarded-non-volatile-reads} \text{ xs} \ W' \implies W \subseteq W' \implies x \in \text{unforwarded-non-volatile-reads} \text{ xs} \ W \)
lemma unforwarded-non-volatile-reads-append: \( \forall W. \) unforwarded-non-volatile-reads \((xs @ ys) W = (\text{unforwarded-non-volatile-reads } xs W \cup \text{unforwarded-non-volatile-reads } ys (W \cup \text{outstanding-refs is-Write}_{sb} xs)) \)

(\textit{proof})

lemma reads-consistent-mem-eq-on-unforwarded-non-volatile-reads:
  \textbf{assumes} \text{mem-eq}: \( \forall a \in A \cup W. \ m' a = m a \)
  \textbf{assumes} \text{subset}: \text{unforwarded-non-volatile-reads } sb W \subseteq A
  \textbf{assumes} \text{consis-m}: \text{reads-consistent pending-write } \mathcal{O} m sb
  \textbf{shows} \text{reads-consistent pending-write } \mathcal{O} m' sb
(\textit{proof})

lemma reads-consistent-mem-eq-on-unforwarded-non-volatile-reads-drop:
  \textbf{assumes} \text{mem-eq}: \( \forall a \in A \cup W. \ m' a = m a \)
  \textbf{assumes} \text{subset}: \text{unforwarded-non-volatile-reads } (\text{dropWhile } (\text{Not } \circ \text{is-volatile-Write}_{sb}) \) sb) W \subseteq A
  \textbf{assumes} \text{subset-acq}: \text{acquired-reads } \text{True } (\text{takeWhile } (\text{Not } \circ \text{is-volatile-Write}_{sb}) \) sb) \mathcal{O} \subseteq A
  \textbf{assumes} \text{consis-m}: \text{reads-consistent } \text{False } \mathcal{O} m sb
  \textbf{shows} \text{reads-consistent } \text{False } \mathcal{O} m' sb
(\textit{proof})

lemma read-only-read-witness: \( \forall S \mathcal{O}. \)
  \text{[non-volatile-owned-or-read-only } True S \mathcal{O} sb; \)
  \( a \in \text{read-only-reads } \mathcal{O} sb \]
  \( \implies \exists xs ys t v. \ sb=xs@ \text{Read}_{sb} \text{False } a t v \# ys \land a \in \text{read-only } (\text{share } xs S) \land a \notin \text{read-only-reads } \mathcal{O} xs \)
(\textit{proof})

lemma read-only-read-acquired-witness: \( \forall S \mathcal{O}. \)
  \text{[non-volatile-owned-or-read-only } True S \mathcal{O} sb; \text{sharing-consistent } S \mathcal{O} sb; \)
  \( a \notin \text{read-only } S; \ a \notin \mathcal{O}; \ a \in \text{read-only-reads } \mathcal{O} sb \]
  \( \implies \exists xs ys t v. \ sb=xs@ \text{Read}_{sb} \text{False } a t v \# ys \land a \in \text{all-acquired } xs \land a \in \text{read-only } (\text{share } xs S) \land a \notin \text{read-only-reads } \mathcal{O} xs \)
(\textit{proof})
lemma unforwarded-not-written: \( \forall W. \ a \in \text{unforwarded-non-volatile-reads sb } W \Rightarrow a \notin W \)
\( \langle \text{proof} \rangle \)

lemma unforwarded-witness: \( \forall X. \ a \in \text{unforwarded-non-volatile-reads sb } X \)
\[ \Rightarrow \exists xs \ ys \ t \ v. \ \text{sb=xs@ Read}_{ab} \ False \ t \ v \ # \ ys \land a \notin \text{outstanding-refs is-Write}_{ab} \ xs \]
\( \langle \text{proof} \rangle \)

lemma read-only-read-acquired-unforwarded-witness: \( \forall S \ O \ X. \)
\[ \text{non-volatile-owned-or-read-only True } S \ O \ \text{sb; sharing-consistent } S \ O \ \text{sb; } a \notin \text{read-only } S; \ a \notin O; \ a \in \text{read-only-reads } O \ \text{sb; } a \in \text{unforwarded-non-volatile-reads sb } X \]
\[ \Rightarrow \exists xs \ ys \ t \ v. \ \text{sb=xs@ Read}_{ab} \ False \ t \ v \ # \ ys \land a \in \text{all-acquired } xs \land a \notin \text{outstanding-refs is-Write}_{ab} \ xs \]
\( \langle \text{proof} \rangle \)

lemmatakeWhile-prefix: \( \exists ys. \ \text{takeWhile } P \ xs \ @ \ ys = xs \)
\( \langle \text{proof} \rangle \)

lemma unforwarded-empty-extend:
\[ \forall W. \ x \in \text{unforwarded-non-volatile-reads sb } \{ \} \Rightarrow x \notin W \Rightarrow x \in \text{unforwarded-non-volatile-reads sb } W \]
\( \langle \text{proof} \rangle \)

lemma notin-unforwarded-empty:
\[ \forall W. \ a \notin \text{unforwarded-non-volatile-reads sb } W \Rightarrow a \notin W \Rightarrow a \notin \text{unforwarded-non-volatile-reads sb } \{ \} \]
\( \langle \text{proof} \rangle \)

lemma
\begin{align*}
\text{assumes } & \text{ro}: \ a \in \text{read-only } S \rightarrow a \in \text{read-only } S' \\
\text{assumes } & \text{a-in: } a \in \text{read-only } (S \oplus_W R) \\
\text{shows } & a \in \text{read-only } (S' \oplus_W R)
\end{align*}
\( \langle \text{proof} \rangle \)

lemma
\begin{align*}
\text{assumes } & \text{ro}: \ a \in \text{read-only } S \rightarrow a \in \text{read-only } S' \\
\text{assumes } & \text{a-in: } a \in \text{read-only } (S \ominus_A L) \\
\text{shows } & a \in \text{read-only } (S' \ominus_A L)
\end{align*}
\( \langle \text{proof} \rangle \)

lemma non-volatile-owned-or-read-only-read-only-reads-eq:
\[ \forall S \ S' \ O \ \text{pending-write.} \]
\[\forall a \in \text{read-only-reads} \ O \ sb; \ a \in \text{read-only} \ S \rightarrow a \in \text{read-only} \ S'\]
\[\Rightarrow \text{non-volatile-owned-or-read-only pending-write} \ S' \ O \ sb\]

**lemma** non-volatile-owned-or-read-only-read-only-reads-eq:
\[\land S \ S' \ O,\]
\[\forall a \in \text{read-only-reads} \ O \ sb; \ a \in \text{read-only} \ S \rightarrow a \in \text{read-only} \ S'\]
\[\Rightarrow \text{non-volatile-owned-or-read-only} \ False \ S' \ O \ sb\]

**lemma** no-write-to-read-only-memory-read-only-reads-eq:
\[\land S \ S' \ O,\]
\[\forall a \in \text{read-only-reads} \ O \ sb; \ a \in \text{read-only} \ S \rightarrow a \in \text{read-only} \ S'\]
\[\Rightarrow \text{no-write-to-read-only-memory} \ False \ S' \ O \ sb\]

**lemma** reads-consistent-drop:
reads-consistent False \ O \ m \ sb
\[\Rightarrow \text{reads-consistent} \ True\]
\[(\text{acquired True} \ \text{takeWhile} \ (\text{Not} \ \circ \ \text{is-volatile-Write}_{sb}) \ sb) \ \text{O})\]
\[(\text{dropWhile} \ (\text{Not} \ \circ \ \text{is-volatile-Write}_{sb}) \ sb) \ \text{m})\]
\[(\text{flush} \ (\text{takeWhile} \ (\text{Not} \ \circ \ \text{is-volatile-Write}_{sb}) \ sb) \ m)\]

**lemma** outstanding-refs-non-volatile-Read_{sb}-all-acquired-dropWhile:
\[\land m \ S \ O \ \text{pending-write},\]
\[\text{[reads-consistent pending-write} \ O \ m \ sb;\text{non-volatile-owned-or-read-only pending-write} \ S \ O \ sb;\]
a \in \text{outstanding-refs is-non-volatile-Read}_{sb} \ \text{dropWhile} \ (\text{Not} \ \circ \ \text{is-volatile-Write}_{sb}) \ sb)]
\[\Rightarrow \ a \in \text{O} \lor a \in \text{all-acquired} \ sb \lor \]
a \in \text{read-only-reads} \ \text{acquired True} \ \text{takeWhile} \ (\text{Not} \ \circ \ \text{is-volatile-Write}_{sb}) \ sb) \ \text{O})\]
\[(\text{dropWhile} \ (\text{Not} \ \circ \ \text{is-volatile-Write}_{sb}) \ sb)\]

**end**

theory ReduceStoreBufferSimulation
locale initial_{sb} = simple-ownership-distinct + read-only-unowned + unowned-shared +
constrains ts: { p, p store-buffer, bool.owns, rels} thread-config list
assumes empty-sb: [ i < length ts; ts! = ( p, is, xs, sb, D, O, R) ] =⇒ sb = []
assumes empty-is: [ i < length ts; ts! = ( p, is, xs, sb, D, O, R) ] =⇒ is = []
assumes empty-rels: [ i < length ts; ts! = ( p, is, xs, sb, D, O, R) ] =⇒ R = Map.empty

sublocale initial_{sb} ⊆ outstanding-non-volatile-refs-owned-or-read-only
 ⟨proof⟩

sublocale initial_{sb} ⊆ outstanding-volatile-writes-unowned-by-others
 ⟨proof⟩

sublocale initial_{sb} ⊆ read-only-reads-unowned
 ⟨proof⟩

sublocale initial_{sb} ⊆ ownership-distinct
 ⟨proof⟩

sublocale initial_{sb} ⊆ valid-ownership
 ⟨proof⟩

sublocale initial_{sb} ⊆ outstanding-non-volatile-writes-unshared
 ⟨proof⟩

sublocale initial_{sb} ⊆ sharing-consis
 ⟨proof⟩

sublocale initial_{sb} ⊆ no-outstanding-write-to-read-only-memory
 ⟨proof⟩

sublocale initial_{sb} ⊆ valid-sharing
 ⟨proof⟩

sublocale initial_{sb} ⊆ valid-ownership-and-sharing
 ⟨proof⟩

sublocale initial_{sb} ⊆ load-tmps-distinct
 ⟨proof⟩

sublocale initial_{sb} ⊆ read-tmps-distinct
 ⟨proof⟩

sublocale initial_{sb} ⊆ load-tmps-read-tmps-distinct
 ⟨proof⟩

sublocale initial_{sb} ⊆ load-tmps-read-tmps-distinct
 ⟨proof⟩

sublocale initial_{sb} ⊆ valid-write-sops
 ⟨proof⟩

sublocale initial_{sb} ⊆ valid-store-sops
 ⟨proof⟩

sublocale initial_{sb} ⊆ valid-sops
 ⟨proof⟩

sublocale initial_{sb} ⊆ valid-reads
 ⟨proof⟩
sublocale initial\(_{sb}\) \(\subseteq\) valid-history
\(\langle proof\rangle\)

sublocale initial\(_{sb}\) \(\subseteq\) valid-data-dependency
\(\langle proof\rangle\)

sublocale initial\(_{sb}\) \(\subseteq\) load-tmps-fresh
\(\langle proof\rangle\)

sublocale initial\(_{sb}\) \(\subseteq\) enough-flushs
\(\langle proof\rangle\)

sublocale initial\(_{sb}\) \(\subseteq\) valid-program-history
\(\langle proof\rangle\)

inductive
sim-config:: (\(\p, p\) store-buffer,\(\_\), bool,\(\_\),\(\_\),\(\_\)) thread-config list \(\times\) memory \(\times\) shared \(\Rightarrow\) (\(\p, p\) store-buffer,\(\_\), bool,\(\_\),\(\_\),\(\_\)) thread-config list \(\times\) memory \(\times\) shared \(\Rightarrow\) bool
\((-\sim\_\{60,60\}100)\)
where
\([\_]\)
\([\_]\)
\([\_]\)
\(\langle proof\rangle\)

The machine without history only stores writes in the store-buffer.

inductive
sim-history-config:: (\(\p, p\) store-buffer,\(\_\),\(\_\),\(\_\),\(\_\)) thread-config list \(\Rightarrow\) (\(\p, p\) store-buffer,\(\_\), bool,\(\_\),\(\_\)) thread-config list \(\Rightarrow\) bool
\((-\sim\_\{60,60\}100)\)
where
\([\_]\)
\([\_]\)
\([\_]\)
\(\langle proof\rangle\)

lemma (in initial\(_{sb}\))
history-refl:: ts \(\sim\_h\) ts
\(\langle proof\rangle\)

lemma share-all-empty:: \(\forall\ p\ is\ xs\ sb\ D\ \_\ R\).\ i < length ts \(\rightarrow\) ts!\(=(p, is, xs, sb, D, O, R)\) \(\rightarrow\) sb\(=[]\)
\(\Rightarrow\) share-all-until-volatile-write ts \(\sim\_h\) S
\(\Rightarrow\) share-all-until-volatile-write ts \(\sim\_h\) S
\(\langle proof\rangle\)
lemma flush-all-empty: \( \forall i p \text{ is } xs \in \mathcal{D} \cup \mathcal{O} \cup \mathcal{R}. \ i < \text{length } ts \rightarrow ts'! = (p, is, xs, sb, D, O, R) \rightarrow sb = [] \)
\( \Rightarrow \) flush-all-until-volatile-write ts m = m
\( \langle \text{proof} \rangle \)

lemma sim-config-emptyE:
assumes empty:
\( \forall i p \text{ is } xs \in \mathcal{D} \cup \mathcal{O} \cup \mathcal{R}. \ i < \text{length } ts_{ab} \rightarrow ts_{ab}! = (p, is, xs, sb, D, O, R) \rightarrow sb = [] \)
assumes sim: \( ts_{ab}, m_{ab}, S_{ab} \sim (ts, m, S) \)
shows \( S = S_{ab} \land m = m_{ab} \land \text{length } ts = \text{length } ts_{ab} \land \)
(\( \forall i < \text{length } ts_{ab}. \)
let \( (p, is, \emptyset, \emptyset, \emptyset, (D, O, R)) = ts_{ab}! \)
in \( ts! = (p, is, \emptyset, (D, O, R)) \)
\( \langle \text{proof} \rangle \)

lemma sim-config-emptyI:
assumes empty:
\( \forall i p \text{ is } xs \in \mathcal{D} \cup \mathcal{O} \cup \mathcal{R}. \ i < \text{length } ts_{ab} \rightarrow ts_{ab}! = (p, is, xs, sb, D, O, R) \rightarrow sb = [] \)
assumes leq: \( \text{length } ts = \text{length } ts_{ab} \)
assumes ts: \( (\forall i < \text{length } ts_{ab}. \)
let \( (p, is, \emptyset, \emptyset, \emptyset, (D, O, R)) = ts_{ab}! \)
in \( ts! = (p, is, \emptyset, (D, O, R)) \)
shows \( ts_{ab}, m_{ab}, S_{ab} \sim (ts, m_{ab}, S_{ab}) \)
\( \langle \text{proof} \rangle \)

lemma mem-eq-un-eq: \( [\text{length } ts' = \text{length } ts; \forall i < \text{length } ts'. \ P (ts'i! = Q(ts'i!))] \Rightarrow (\bigcup x \in \text{set} ts'. P x) = (\bigcup x \in \text{set} ts. Q x) \)
\( \langle \text{proof} \rangle \)

lemma (in program) trace-to-steps:
assumes trace: trace c 0 k
shows steps: c 0 \( \Rightarrow_{a}^{*} \) c k
\( \langle \text{proof} \rangle \)

lemma (in program) safe-reach-to-safe-reach-upto:
assumes safe-reach: safe-reach-direct safe c 0
shows safe-reach-upto n safe c 0
\( \langle \text{proof} \rangle \)

lemma (in program-progress) safe-free-flowing-implies-safe-delayed':
assumes init: initial_{ab} ts_{ab}, S_{ab}
assumes sim: \( ts_{ab}, m_{ab}, S_{ab} \sim (ts, m, S) \)
assumes safe-free-flowing: safe-reach-direct safe-free-flowing (ts, m, S)
says safe-reach-direct safe-delayed (ts, m, S)
\( \langle \text{proof} \rangle \)

lemma map-onws-sb-owned: \( \forall j. j < \text{length } ts \Rightarrow \text{map } O-sb ts j = (O_j, sb_j) \Rightarrow \text{map owned } ts j = O_j \)
\( \langle \text{proof} \rangle \)

lemma map-onws-sb-owned': \( \forall j. j < \text{length } ts \Rightarrow O-sb (ts j) = (O_j, sb_j) \Rightarrow \text{owned } (ts j) = O_j \)
\( \langle \text{proof} \rangle \)

lemma read-only-read-acquired-unforwarded-acquire-witness:
\( \forall S O X. \text{non-volatile-owned-or-read-only True } S O \in \mathcal{X} \)
sharing-consistent \( S O \in \mathcal{X}; a \notin \text{read-only } S; a \notin O; \)
a \( \in \text{unforwarded-non-volatile-reads } sb X \)
\( \Rightarrow (\exists \text{sop } a' v y s z A L R W. \)
sb = ys @ Write_{ab} True a' \text{sop } v A L R W \# z s \land \)
a = A \land a \notin \text{outstanding-refs is-Write}_{ab} y s A' \land a' \neq a) \lor \)
lemma release-shared-exchange-weak:
assumes shared-eq: \( \forall a \in O \cup \text{all-acquired sb}. (S':\!:shared) a = S a \)
assumes consis: weak-sharing-consistent O sb
shows release sb (dom S') R = release sb (dom S) R
⟨proof⟩

lemma read-only-share-all-shared: \( \bigwedge S. \ [a \in \text{read-only sb S}] \)
\( \implies \ a \in \text{read-only S} \cup \text{all-shared sb} \)
⟨proof⟩

lemma read-only-shared-all-until-volatile-write-subset':
\( \bigwedge S. \text{read-only sb S} \subseteq \bigcup (\{(\lambda (-, -, sb, -, -). \text{all-shared (takeWhile (Not \circ \text{is-volatile-Write}_{sb}) sb)) ' set ts}\) \)
⟨proof⟩

lemma read-only-share-acquired-all-shared:
\( \bigwedge O S. \ \text{weak-sharing-consistent O sb} \implies O \cap \text{read-only S} = {} \implies \ a \in \text{read-only S} \cup \text{all-acquired sb} \implies \ a \in \text{all-shared sb} \)
⟨proof⟩

lemma read-only-share-unowned': \( \bigwedge O S. \ [\text{weak-sharing-consistent O sb}; O \cap \text{read-only S} = {}; \ a \notin O \cup \text{all-acquired sb}; a \in \text{read-only S}] \)
\( \implies a \in \text{read-only sb S} \)
⟨proof⟩

lemma release-False-mono:
\( \bigwedge S R. \ R a = \text{Some False} \implies \text{outstanding-refs is-volatile-Write}_{sb} \text{ sb} = {} \implies \)
release sb S R a = Some False
⟨proof⟩

lemma release-False-mono-take:
\( \bigwedge S R. \ R a = \text{Some False} \implies \text{release (takeWhile (Not \circ \text{is-volatile-Write}_{sb}) sb) S R a = Some False} \)
⟨proof⟩

lemma shared-switch:
\( \bigwedge O S. \ [\text{weak-sharing-consistent O sb}; \text{read-only S} \cap O = {}]; \ S a \neq \text{Some False}; \text{share sb S a = Some False}] \)
\( \implies a \in O \cup \text{all-acquired sb} \)
⟨proof⟩

lemma shared-switch-release-False:
\( \bigwedge S R. \ [\text{outstanding-refs is-volatile-Write}_{sb} \text{ sb} = {}]; \ a \notin \text{dom S}; \ a \in \text{dom (share sb S)}] \)
\( \implies \text{release sb (dom S) R a = Some False} \)
⟨proof⟩
lemma release-not-unshared-no-write:
\[ \forall S, R. \ [\text{outstanding-refs}\ is-volatile-Write_{ab}\ sb = \{\}; \non-volatile-writes-unshared\ S\ sb; \release\ sb\ (dom\ S)\ R\ a \neq \text{Some False}; \ a \in dom\ (share\ sb\ S)]\]
\[ \implies \ a \notin\ outstanding-refs\ is-non-volatile-Write_{ab}\ sb\]
\[\langle \text{proof}\rangle\]

corollary release-not-unshared-no-write-take:
\[\forall S, R. \ [\text{takeWhile}\ (\Not\ is-volatile-Write_{ab})\ sb]; \\text{assume}\ rel; \\text{release}\ (takeWhile\ (\Not\ is-volatile-Write_{ab})\ sb)\ (dom\ S)\ R\ a \neq \text{Some False}; \ a \in\ dom\ (share\ (takeWhile\ (\Not\ is-volatile-Write_{ab})\ sb)\ S)]\]
\[\implies \ a \notin\ outstanding-refs\ is-non-volatile-Write_{ab}\ (takeWhile\ (\Not\ is-volatile-Write_{ab})\ sb)\]
\[\langle \text{proof}\rangle\]

lemma read-only-unacquired-share-
\[ \forall S, O. \ [\text{O}\ \&\ \text{read-only}\ S = \{\}; \weak-sharing-consistent\ O\ sb; \ a \in\ read-only\ S; \ a \notin\ all-shared\ sb; \ a \notin\ acquired\ True\ sb\ O]\]
\[\implies \ a \in\ read-only\ (share\ sb\ S)\]
\[\langle \text{proof}\rangle\]

lemma read-only-share-all-until-volatile-write-unacquired-
\[ \forall i < \text{length}\ ts. \ (let\ (\cdot,\cdot,\cdot,\cdot,\cdot,\cdot,\cdot,\cdot,\cdot,\cdot,\cdot,\cdot,\cdot,\cdot,\cdot,\cdot,\cdot,\cdot,\cdot,\cdot,\cdot,\cdot) = \text{tsi}\ in\]
\[a \notin\ acquired\ True\ (takeWhile\ (\Not\ is-volatile-Write_{ab})\ sb)\ O\ \& 
\[a \notin\ all-shared\ (takeWhile\ (\Not\ is-volatile-Write_{ab})\ sb)\]
\[\text{)}];
\[\ a \in\ read-only\ S]\]
\[\implies \ a \in\ read-only\ (\text{share-all-until-volatile-write}\ ts\ S)\]
\[\langle \text{proof}\rangle\]

lemma not-shared-not-acquired-switch:
\[ \forall X, Y. \ [a \notin\ all-shared\ sb; \ a \notin\ X; \ a \notin\ acquired\ True\ sb\ X; \ a \notin\ Y] \implies \ a \notin\ acquired\ True\ sb\ Y\]
\[\langle \text{proof}\rangle\]

lemma read-only-share-all-acquired-in-
\[ \forall S, O. \ [\text{O}\ \&\ \text{read-only}\ S = \{\}; \weak-sharing-consistent\ O\ sb; \ a \in\ read-only\ (share\ sb\ S)]\]
\[\implies \ a \in\ read-only\ (\text{share}\ sb\ \text{Map.empty})\ \vee\ (a \in\ read-only\ S\ \&\ a \notin\ acquired\ True\ sb\ O\ \&\ a \notin\ all-shared\ sb)\]
\[\langle \text{proof}\rangle\]

lemma in-read-only-share-all-until-volatile-write-
\[\forall X. \ [a \notin\ all-shared\ sb; \ a \notin\ X; \ a \notin\ acquired\ True\ sb\ X; \ a \notin\ Y] \implies \ a \notin\ acquired\ True\ sb\ Y\]
\[\langle \text{proof}\rangle\]
lemma all-acquired-unshared-acquired:
\[ \forall O. \ a \in \text{all-acquired} \iff a \notin \text{all-shared} \iff a \in \text{acquired} \ True \ O \]

lemma safe-RMW-common:
\[ \begin{align*}
\text{assumes safe: } & O, R, s, b, (\text{RMW} a \ t (D, f) \ \text{cond ret} \ A \ L \ R \ W \# \ is, \ \theta, \ m, D, O, S) \\
\text{shows (a \in O \lor a \in \text{dom} S) \land (\forall j < \text{length O}. i \neq j \rightarrow (R[s][j]) a \neq \text{Some False})}
\end{align*} \]

lemma acquired-reads-all-acquired':
\[ \forall O. \ \text{acquired-reads} \ True \ O \subseteq \text{acquired} \ True \ O \cup \text{all-shared} \]

lemma release-all-shared-exchange:
\[ \forall R, S'. \ \forall a \in \text{all-shared} \ sb. \ (a \in S') = (a \in S) \implies \text{release} \ sb \ S' R = \text{release} \ sb \ S \ R \]

lemma release-append-Prog:
\[ \begin{align*}
\text{assumes step-sb: } & (ts_{sb}, m_{sb}, S_{sb}) \Rightarrow_{sb} (ts_{sb}', m_{sb}', S_{sb}') \\
\text{assumes valid-own: } & \text{valid-ownership} \ S_{sb} ts_{sb} \\
\text{assumes valid-sb-reads: } & \text{valid-reads} m_{sb} ts_{sb} \\
\text{assumes valid-hist: } & \text{valid-history} \ \text{program-step} ts_{sb} \\
\text{assumes valid-sharing: } & \text{valid-sharing} \ S_{sb} ts_{sb} \\
\text{assumes tmps-distinct: } & \text{tmps-distinct} \ ts_{sb} \\
\text{assumes valid-sops: } & \text{valid-sops} \ ts_{sb} \\
\text{assumes valid-dd: } & \text{valid-data-dependency} \ ts_{sb} \\
\text{assumes load-tmps-fresh: } & \text{load-tmps-fresh} \ ts_{sb} \\
\text{assumes enough-flushs: } & \text{enough-flushs} \ ts_{sb} \\
\text{assumes valid-program-history: } & \text{valid-program-history} \ ts_{sb} \\
\text{assumes valid: } & \text{valid} \ ts_{sb} \\
\text{assumes sim: } & (ts_{sb}, m_{sb}, S_{sb}) \sim (ts, m, S) \\
\text{assumes safe-reach: } & \text{safe-reach-direct} \ \text{safe-delayed} \ (ts, m, S) \\
\text{shows valid-ownership} \ S_{sb}' ts_{sb}' \ \text{valid-reads} m_{sb}' ts_{sb}' \ \text{valid-history} \ \text{program-step} ts_{sb}' \\
\end{align*} \]

A.5 Simulation of Store Buffer Machine with History by Virtual Machine with Delayed Releases

\[ \text{theorem (in xvalid-program) concurrent-direct-steps-simulates-store-buffer-history-step:} \]
\[ \text{assumes step-sb: } (ts_{sb}, m_{sb}, S_{sb}) \Rightarrow_{sb} (ts_{sb}', m_{sb}', S_{sb}') \]
\[ \text{assumes valid-own: } \text{valid-ownership} \ S_{sb} ts_{sb} \]
\[ \text{assumes valid-sb-reads: } \text{valid-reads} m_{sb} ts_{sb} \]
\[ \text{assumes valid-hist: } \text{valid-history} \ \text{program-step} ts_{sb} \]
\[ \text{assumes valid-sharing: } \text{valid-sharing} \ S_{sb} ts_{sb} \]
\[ \text{assumes tmps-distinct: } \text{tmps-distinct} \ ts_{sb} \]
\[ \text{assumes valid-sops: } \text{valid-sops} \ ts_{sb} \]
\[ \text{assumes valid-dd: } \text{valid-data-dependency} \ ts_{sb} \]
\[ \text{assumes load-tmps-fresh: } \text{load-tmps-fresh} \ ts_{sb} \]
\[ \text{assumes enough-flushs: } \text{enough-flushs} \ ts_{sb} \]
\[ \text{assumes valid-program-history: } \text{valid-program-history} \ ts_{sb} \]
\[ \text{assumes valid: } \text{valid} \ ts_{sb} \]
\[ \text{assumes sim: } (ts_{sb}, m_{sb}, S_{sb}) \sim (ts, m, S) \]
\[ \text{assumes safe-reach: } \text{safe-reach-direct} \ \text{safe-delayed} \ (ts, m, S) \]
\[ \text{shows valid-ownership} \ S_{sb}' ts_{sb}' \ \text{valid-reads} m_{sb}' ts_{sb}' \ \text{valid-history} \ \text{program-step} ts_{sb}' \\
\text{valid-sharing} S_{sb}' ts_{sb}' \ \text{tmps-distinct} ts_{sb}' \ \text{valid-data-dependency} ts_{sb}' \\
\text{valid-sops} ts_{sb}' \ \text{load-tmps-fresh} ts_{sb}' \ \text{enough-flushs} ts_{sb}' \\
\text{valid-program-history} ts_{sb}' \ \text{valid} ts_{sb}' \ \\
(\exists ts' S' m'. (ts, m, S) \Rightarrow^* (ts', m', S') \ \\
(ts_{sb}', m_{sb}', S_{sb}') \sim (ts', m', S')) \]

125
\[\text{proof}\]

**Theorem (in xvalid-program) concurrent-direct-steps-simulates-store-buffer-history-steps:**

\[\begin{align*}
\text{assumes } & \text{step-sb: } (ts_{sb},m_{sb},S_{sb}) \Rightarrow_{sb}^* (ts_{sb}',m_{sb}',S_{sb}') \\
\text{assumes } & \text{valid-ownership } S_{sb} \text{ ts}_{sb} \\
\text{assumes } & \text{valid-sb-reads: } \text{valid-reads } m_{sb} \text{ ts}_{sb} \\
\text{assumes } & \text{valid-sharing: } \text{valid-sharing } S_{sb} \text{ ts}_{sb} \\
\text{assumes } & \text{tmpls-distinct: } \text{tmpls-distinct } ts_{sb} \\
\text{assumes } & \text{valid-sops: } \text{valid-sops } ts_{sb} \\
\text{assumes } & \text{valid-dd: } \text{valid-data-dependency } ts_{sb} \\
\text{assumes } & \text{load-tmps-fresh: } \text{load-tmps-fresh } ts_{sb} \\
\text{assumes } & \text{enough-flushs: } \text{enough-flushs } ts_{sb} \\
\text{assumes } & \text{valid-program-history: } \text{valid-program-history } ts_{sb} \\
\text{assumes } & \text{valid: } \text{valid } ts_{sb} \\
\text{shows } & \forall ts \ S \ m. \ (ts_{sb},m_{sb},S_{sb}) \sim (ts,m,S) \implies \text{safe-reach-direct safe-delayed } (ts,m,S) \\
\implies & \text{valid-ownership } S_{sb}' \text{ ts}_{sb}' \land \text{valid-reads } m_{sb}' \text{ ts}_{sb}' \land \text{valid-history program-step } ts_{sb}' \\
\land & \text{valid-sharing } S_{sb}' \text{ ts}_{sb}' \land \text{tmpls-distinct } ts_{sb}' \land \text{valid-data-dependency } ts_{sb}' \land \\
\land & \text{valid-sops } ts_{sb}' \land \text{load-tmps-fresh } ts_{sb}' \land \text{enough-flushs } ts_{sb}' \land \\
\land & \text{valid-program-history } ts_{sb}' \land \text{valid } ts_{sb}' \\
& (\exists ts' m' S'. \ (ts,m,S) \Rightarrow_d^* (ts',m',S') \land (ts_{sb}',m_{sb}',S_{sb}') \sim (ts',m',S'))
\end{align*}\]

\[\text{proof}\]

**Sublocale** initial_{sb} \subseteq tmpls-distinct (proof)

**Locale** xvalid-program-progress = program-progress + xvalid-program

**Theorem (in xvalid-program-progress) concurrent-direct-execution-simulates-store-buffer-history-execution:**

\[\begin{align*}
\text{assumes } & \text{exec-sb: } (ts_{sb},m_{sb},S_{sb}) \Rightarrow_{sb}^* (ts_{sb}',m_{sb}',S_{sb}') \\
\text{assumes } & \text{init: } \text{initial}_{sb} \text{ ts}_{sb} S_{sb} \\
\text{assumes } & \text{valid: } \text{valid } ts_{sb} \\
\text{assumes } & \text{sim: } (ts_{sb},m_{sb},S_{sb}) \sim (ts,m,S) \\
\text{assumes } & \text{safe: } \text{safe-reach-direct safe-free-flowing } (ts,m,S) \\
\text{shows } & \exists ts' m' S'. \ (ts,m,S) \Rightarrow_d^* (ts',m',S') \land \\
& (ts_{sb}',m_{sb}',S_{sb}') \sim (ts',m',S')
\end{align*}\]

\[\text{proof}\]

**Lemma** filter-is-Write_{sb}-Cons-Write_{sb}: filter is-Write_{sb} xs = \text{Write}_{sb} \text{ volatile a sop } v \ A \ L \ R \ W \ W#ys \\
\implies \exists rs rws. (\forall r \in \text{set rs. is-Read}_{sb} r \lor \text{is-Program}_{sb} r \lor \text{is-Ghost}_{sb} r) \land \\
xs=rs@\text{Write}_{sb} \text{ volatile a sop } v \ A \ L \ R \ W \ W#rws \land ys=\text{filter is-Write}_{sb} \text{ rws}

\[\text{proof}\]
lemma filter-is-Write\sb-empty: \text{filter is-Write}_{\sb} \text{xs} = [\]
\quad \implies (\forall r \in \text{set} \text{xs}. \text{is-Read}_{\sb} r \lor \text{is-Prog}_{\sb} r \lor \text{is-Ghost}_{\sb} r)
⟨proof⟩

lemma flush-reads-program: \exists \text{O} \text{ S} \text{ R} .
\quad \forall r \in \text{set} \text{sb}. \text{is-Read}_{\sb} r \lor \text{is-Prog}_{\sb} r \lor \text{is-Ghost}_{\sb} r \implies
\quad \exists \text{O}' \text{ S}' . (\text{m}, \text{sb}, \text{O}, \text{R}, \text{S}) \rightarrow r^* (\text{m}, [\], \text{O}', \text{R}', \text{S}')
⟨proof⟩

lemma flush-progress: \exists \text{m}' \text{ O}' \text{ S}' . (\text{m}, \text{r}\#\text{sb}, \text{O}, \text{R}, \text{S}) \rightarrow f (\text{m}', \text{sb}, \text{O}', \text{R}', \text{S}')
⟨proof⟩

lemma flush-empty: \assumes steps: (\text{m}, \text{sb}, \text{O}, \text{R}, \text{S}) \rightarrow f (\text{m}', \text{sb}', \text{O}', \text{R}', \text{S}')
\shows \text{sb}=[\] \implies \text{m}'=\text{m} \land \text{sb}'=[\] \land \text{O}'=\text{O} \land \text{R}'=\text{R} \land \text{S}'=\text{S}
⟨proof⟩

lemma flush-append:
\assumes steps: (\text{m}, \text{sb}, \text{O}, \text{R}, \text{S}) \rightarrow f (\text{m}', \text{sb}', \text{O}', \text{R}', \text{S}')
\shows \lambda \text{xs}. (\text{m}, \text{sb}@\text{xs}, \text{O}, \text{R}, \text{S}) \rightarrow f (\text{m}', \text{sb}'@\text{xs}, \text{O}', \text{R}', \text{S}')
⟨proof⟩

lemmas store-buffer-step-induct =
\text{store-buffer-step} \text{.induct} [\text{split-format} \text{ (complete)}],
\text{consumes} 1, \text{case-names} \text{SBWrite}_{\sb}]

theorem flush-simulates-filter-writes:
\assumes step: (\text{m}, \text{sb}, \text{O}, \text{R}, \text{S}) \rightarrow w (\text{m}', \text{sb}', \text{O}', \text{R}', \text{S}')
\shows \lambda \text{sb}h. \text{sb}h=\text{filter is-Write}_{\sb} \text{sb}h
\quad \implies \exists \text{sb}h' \text{ O}h' \text{ R}h' \text{ S}h . (\text{m}, \text{sb}h, \text{O}h, \text{R}h, \text{S}h) \rightarrow r^* (\text{m}', \text{sb}h', \text{O}h', \text{R}h', \text{S}h') \land
\quad \text{sb}h'=\text{filter is-Write}_{\sb} \text{sb}h' \land (\text{sb}h=[\] \implies \text{sb}h'=[\])
⟨proof⟩

lemma buffered-val-filter-is-Write\sb-eq-ext:
\quad \text{buffered-val} (\text{filter is-Write}_{\sb} \text{sb}) \text{ a} = \text{buffered-val} \text{ sb} \text{ a}
⟨proof⟩

lemma buffered-val-filter-is-Write\sb-eq:
\quad \text{buffered-val} (\text{filter is-Write}_{\sb} \text{sb}) = \text{buffered-val} \text{ sb}
⟨proof⟩

lemma outstanding-refs-is-volatile-Write\sb-filter-writes:
\quad \text{outstanding-refs is-volatile-Write}_{\sb} (\text{filter is-Write}_{\sb} \text{xs}) =
\quad \text{outstanding-refs is-volatile-Write}_{\sb} \text{xs}
⟨proof⟩

127
A.6 Simulation of Store Buffer Machine without History by Store Buffer Machine with History

**Theorem (in valid-program) concurrent-history-steps-simulates-store-buffer-step:**

assumes step-sb: \((ts, m, S) \Rightarrow_{sb} (ts', m', S')\)

assumes sim: \(ts \sim_{h} ts_h\)

shows \(\exists ts_h', S_h'. (ts_h, m, S_h) \Rightarrow_{sb} (ts_h', m', S_h') \land ts' \sim_{h} ts_h'\)

**Proof**

**Theorem (in valid-program) concurrent-history-steps-simulates-store-buffer-steps:**

assumes step-sb: \((ts, m, S) \Rightarrow_{sb} (ts', m', S')\)

shows \(ts \sim_{h} ts_h\) \(\Rightarrow\) \(\exists ts_h', S_h'. (ts_h, m, S_h) \Rightarrow_{sb} (ts_h', m', S_h') \land ts' \sim_{h} ts_h'\)

**Proof**

**Theorem (in valid-program-progress) concurrent-direct-execution-simulates-store-buffer-execution:**

assumes exec-sb: \((ts_{sb}, m_{sb}, x) \Rightarrow_{sb} (ts_{sb}', m_{sb}', x')\)

assumes init: initial \(ts_{sb}\)

assumes valid: valid \(ts_{sb}\)

assumes sim: \((ts_{sb}, m_{sb}, S_{sb}) \sim (ts, m, S)\)

assumes safe: safe-reach-direct safe-free-flowing \((ts, m, S)\)

shows \(\exists ts_h', S_h'. ts' \sim_{h} ts_h'\)

\((ts_{sb}, m_{sb}, S_{sb}) \Rightarrow_{sb} (ts_{sb}', m_{sb}', S_{sb}') \land ts_{sb} \sim_{h} ts_h' \land (ts, m, S) \Rightarrow_{d} (ts', m', S') \land (ts_{sb}', m_{sb}', S_{sb}') \sim_{h} (ts', m', S')\)

**Proof**

**Inductive sim-direct-config::**

\((p, p \text{ store-buffer}, \text{dirty}, \text{owns}, \text{rels}) \text{ thread-config list } \Rightarrow (\text{unit}, \text{bool}, \text{owns}', \text{rels}')\)

**Thread-config list \Rightarrow bool**

\((- \sim_{d} - [60,60] 100)\)

**Where**

\[\begin{align*}
\text{length ts} &= \text{length ts}_{d}; \\
\forall i &< \text{length ts}. \\
(\exists O', D', R'). & \text{ let } (p, is, \emptyset, sb, D, O, R) = ts_{d}[i] \text{ in} \\
& \quad ts[i]=(p, is, \emptyset, \emptyset, D', O', R') \\
& \Rightarrow \text{ length ts}_{d} \\
\end{align*}\]

**Lemma empty-sb-sims:**

**Assumes empty:**

\(\forall i p \text{ is xs sb } D \ O \ R. i < \text{length ts}_{sb} \Rightarrow ts_{sb}[i]=(p, is, xs, sb, D, O, R) \Rightarrow sb=\emptyset\)

**Assumes sim-h:** \(ts_{sb} \sim_{h} ts_h\)

**Assumes sim-d:** \((ts_{h}, m_{h}, S_{h}) \sim (ts, m, S)\)

128
shows $ts_{sb} \sim_d ts \land m_h = m \land \text{length} ts_{sb} = \text{length} ts$

\text{⟨proof⟩}

\textbf{lemma} empty-d-sims:
\textbf{assumes} sim: $ts_{sb} \sim_d ts$
\textbf{shows} $\exists ts_h. ts_{sb} \sim_h ts_h \land (ts_h, m, S) \sim (ts, m, S)$
\text{⟨proof⟩}

\textbf{theorem} (in xvalid-program-progress) concurrent-direct-execution-simulates-store-buffer-execution-empty:
\textbf{assumes} exec-sb: $(ts_{sb}, m_{sb}, x) \Rightarrow_{sb}^* (ts_{sb}', m_{sb}', x')$
\textbf{assumes} init: $\text{initial}_{sb} ts_{sb} S_{sb}$
\textbf{assumes} valid: valid $ts_{sb}$
\textbf{assumes} empty: empty:
$\forall i \ p \text{ is } xs \ sib \ D \ O \ R. \ i < \text{length} ts_{sb}' \rightarrow ts_{sb}' \forall!i=\{p, is, xs, sb, D, O, R\} \rightarrow \text{sb}=[]$
\textbf{assumes} sim: $(ts_{sb}, m_{sb}, S_{sb}) \sim (ts, m, S)$
\textbf{assumes} safe: safe-reach-direct safe-free-flowing $(ts, m, S)$
\textbf{shows} $\exists ts' S'$:
$(ts, m, S) \Rightarrow_d^* (ts', m_{sb}', S') \land ts_{sb}' \sim_d ts'$
\text{⟨proof⟩}

\textbf{locale} initial_d = simple-ownership-distinct + read-only-unowned + unowned-shared + fixes valid
\textbf{assumes} empty-is: $[i < \text{length} ts; ts!i=\{p, is, xs, sb, D, O, R\} \rightarrow is=[]$  
\textbf{assumes} empty-rels: $[i < \text{length} ts; ts!i=\{p, is, xs, sb, D, O, R\} \rightarrow R=\text{Map.empty}$
\textbf{assumes} valid-init: valid $(\lambda(p, is, \emptyset, sb, D, O, R). (p, is, \emptyset, [], D, O, R)) ts$

\textbf{locale} empty-store-buffers =
\textbf{fixes} ts::('p, 'p store-buffer, bool, owns, rels) thread-config list
\textbf{assumes} empty-sb: $[i < \text{length} ts; ts!i=\{p, is, xs, sb, D, O, R\} \rightarrow sb=[]$

\textbf{lemma} initial-d-sb:
\textbf{assumes} init: initial_d $ts \ S$ valid
\textbf{shows} initial_d $(\lambda(p, is, \emptyset, sb, D, O, R). (p, is, \emptyset, [], D, O, R)) ts) S$
\text{(is initial_d ?map S)}$
\text{⟨proof⟩}

\textbf{theorem} (in xvalid-program-progress) store-buffer-execution-result-sequential-consistent:
\textbf{assumes} exec-sb: $(ts_{sb}, m, x) \Rightarrow_{sb}^* (ts_{sb}', m', x')$
\textbf{assumes} empty': empty-store-buffers $ts_{sb}'$
\textbf{assumes} sim: $ts_{sb} \sim_d ts$
\textbf{assumes} init: initial_d $ts \ S$ valid
\textbf{assumes} safe: safe-reach-direct safe-free-flowing $(ts, m, S)$
\textbf{shows} $\exists ts' S'$:
$(ts, m, S) \Rightarrow_d^* (ts', m', S') \land ts_{sb}' \sim_d ts'$
\text{⟨proof⟩}

\textbf{locale} initial_d = simple-ownership-distinct + read-only-unowned + unowned-shared + fixes valid
assumes empty-is: \[ [i < \text{length } ts; ts!i = (p, is, xs, sb, D, O, R)] \implies is=[] \]
assumes valid-init: valid (map (\(\lambda(p, is, \emptyset, sb, D, O, R)\)) ts)

**Theorem** (in xvalid-program-progress) store-buffer-execution-result-sequential-consistent:
assumes exec-sb: \( ts_b, m, x \mapsto ts_b' \)
assumes empty': empty-store-buffers ts
assumes init: initial ts S valid
assumes safe: safe-reach-virtual safe-free-flowing (ts, m, S)
shows \( \exists ts', S' \). (ts, m, S) \mapsto_v^* (ts', m', S') \land ts_b' \sim_d ts'

〈proof〉

A.7 Plug Together the Two Simulations

corollary (in xvalid-program) concurrent-direct-steps-simulates-store-buffer-step:
assumes step-sb: \( ts_{sb}, m_{sb}, S_{sb} \mapsto_{sb} ts_{sb}', m_{sb}', S_{sb}' \)
assumes sim-h: ts_{sbh} \sim_h ts_{sbh}
assumes sim: \( ts_{sbh}, m_{sb}, S_{sbh} \mapsto (ts, m, S) \)
assumes valid-own: valid-ownership S_{sbh} ts_{sbh}
assumes valid-reads: valid-reads m_{sb} ts_{sbh}
assumes valid-hist: valid-history program-step ts_{sbh}
assumes valid-sharing: valid-sharing S_{sbh} ts_{sbh}
assumes tmps-distinct: tmps-distinct ts_{sbh}
assumes valid-sops: valid-sops ts_{sbh}
assumes valid-dd: valid-data-dependency ts_{sbh}
assumes load-tmps-fresh: load-tmps-fresh ts_{sbh}
assumes enough-flushs: enough-flushs ts_{sbh}
assumes valid-program-history: valid-program-history ts_{sbh}
assumes valid: valid ts_{sbh}
assumes safe-reach: safe-reach-direct safe-delayed (ts, m, S)
shows \( \exists ts_{sbh}', S_{sbh}' \).
\( (ts_{sbh}, m_{sb}, S_{sbh}) \mapsto_{sbh}^* (ts_{sbh}', m_{sb}', S_{sbh}') \land ts_{sbh}' \sim_h ts_{sbh}' \land \)
valid-ownership S_{sbh}' ts_{sbh}' \land valid-reads m_{sb}' ts_{sbh}' \land \valid-history program-step ts_{sbh}' \land \valid-sharing S_{sbh}' ts_{sbh}' \land 
tmps-distinct ts_{sbh}' \land valid-data-dependency ts_{sbh}' \land \valid-sops ts_{sbh}' \land load-tmps-fresh ts_{sbh}' \land enough-flushs ts_{sbh}' \land \valid-program-history ts_{sbh}' \land valid ts_{sbh}' \land 
(\exists ts', S', m', (ts, m, S) \mapsto_d^* (ts', m', S') \land 
(ts_{sbh}', m_{sb}', S_{sbh}') \sim (ts', m', S'))

〈proof〉

**Lemma** conj-commI: \( P \land Q \implies Q \land P \)

〈proof〉
lemma def-to-eq: \( P = Q \iff P \equiv Q \)

(proof)

category xvalid-program
begin

definition
invariant ts \( S \) m \( \equiv \)
valid-ownership \( S \) ts \land valid-reads m ts \land valid-history program-step ts \land
valid-sharing \( S \) ts \land tmprs-distinct ts \land valid-data-dependency ts \land
valid-sops ts \land load-tmps-fresh ts \land enough-flushs ts \land valid-program-history ts \land
valid ts

definition ownership-inv \( \equiv \) valid-ownership

definition sharing-inv \( \equiv \) valid-sharing

definition temporaries-inv ts \( \equiv \) tmprs-distinct ts \land load-tmps-fresh ts

definition history-inv ts m \( \equiv \) valid-history program-step ts \land valid-program-history ts \land
valid-reads m ts

definition data-dependency-inv ts \( \equiv \) valid-data-dependency ts \land load-tmps-fresh ts \land
valid-sops ts

definition barrier-inv \( \equiv \) enough-flushs

lemma invariant-grouped-def: invariant ts \( S \) m \( \equiv \)
ownership-inv \( S \) ts \land sharing-inv \( S \) ts \land temporaries-inv ts \land data-dependency-inv ts \land
history-inv ts m \land barrier-inv ts \land valid ts

(proof)

\( \text{theorem (in xvalid-program) simulation':} \)
\begin{itemize}
\item \textbf{assumes} step-sb: \((ts_{sb},m_{sb},S_{sb}) \Rightarrow_{sbh} (ts_{sb}',m_{sb}',S_{sb}')\)
\item \textbf{assumes} sim: \((ts_{sb},m_{sb},S_{sb}) \sim (ts,m,S)\)
\item \textbf{assumes} inv: invariant ts_{sb} S_{sb} m_{sb}
\item \textbf{assumes} safe-reach: safe-reach-direct safe-delayed (ts,m,S)
\item \textbf{shows} invariant ts_{sb}' S_{sb}' m_{sb}' \land
\begin{equation}
(\exists ts' \ S' \ m'. (ts,m,S) \Rightarrow_{d^*} (ts',m',S') \land (ts_{sb}',m_{sb}',S_{sb}') \sim (ts',m',S'))
\end{equation}
\end{itemize}

(proof)

\( \text{lemmas (in xvalid-program) simulation = conj-commI [OF simulation']} \)
end

end

A.8 PIMP

definition expr = Const val | Mem bool addr | Tmp sop
| Unop val ⇒ val expr
datatype stmt =
  Skip
|
  Assign bool expr expr tmprs ⇒ owns tmprs ⇒ owns tmprs ⇒ owns tmprs ⇒
owns
|
  CAS expr expr expr tmprs ⇒ owns tmprs ⇒ owns tmprs ⇒ owns tmprs ⇒ owns
|
  Seq stmt stmt
|
  Cond expr stmt stmt
|
  While expr stmt
|
  SGhost tmprs ⇒ owns tmprs ⇒ owns tmprs ⇒ owns tmprs ⇒ owns
|
  SFence

primrec used-tmps:: expr ⇒ nat — number of temporaries used
where
used-tmps (Const v) = 0
| used-tmps (Mem volatile addr) = 1
| used-tmps (Tmp sop) = 0
| used-tmps (Unop f e) = used-tmps e
| used-tmps (Binop f e_1 e_2) = used-tmps e_1 + used-tmps e_2

primrec issue-expr:: tmp ⇒ expr ⇒ instr list — load operations
where
issue-expr t (Const v) = []
| issue-expr t (Mem volatile a) = [Read volatile a t]
| issue-expr t (Tmp sop) = []
| issue-expr t (Unop f e) = issue-expr t e
| issue-expr t (Binop f e_1 e_2) = issue-expr t e_1 @ issue-expr (t + (used-tmps e_1)) e_2

primrec eval-expr:: tmp ⇒ expr ⇒ sop — calculate result
where
eval-expr t (Const v) = (\{\},λθ. v)
| eval-expr t (Mem volatile a) = (\{t\},λθ. the (θ t))
| eval-expr t (Tmp sop) = sop
  — trick to enforce sop to be sensible in the current context, without
having to include wellformedness constraints
| eval-expr t (Unop f e) = (let (D,f_e) = eval-expr t e in (D,λθ. f (f_e θ)))
| eval-expr t (Binop f e_1 e_2) = (let (D_1,f_1) = eval-expr t e_1;
  (D_2,f_2) = eval-expr (t + (used-tmps e_1)) e_2
  in (D_1 ∪ D_2,λθ. f (f_1 θ) (f_2 θ)))

primrec valid-sops-expr:: nat ⇒ expr ⇒ bool
where
valid-sops-expr t (Const v) = True
| valid-sops-expr t (Mem volatile a) = True
| valid-sops-expr t (Tmp sop) = ((∀ t′ ∈ fst sop. t′ < t) ∧ valid-sop sop)
|valid-sops-expr t (Unop f e) = valid-sops-expr t e |
|valid-sops-expr t (Binop f e₁ e₂) = (valid-sops-expr t e₁ ∧ valid-sops-expr t e₂) |

**primrec** valid-sops-stmt:: nat ⇒ stmt ⇒ bool

**where**
valid-sops-stmt t Skip = True
valid-sops-stmt t (Assign volatile a e A L R W) = (valid-sops-expr t a ∧ valid-sops-expr t e)
valid-sops-stmt t (CAS a c₁ c₂ e A L R W) = (valid-sops-expr t a ∧ valid-sops-expr t c₁ ∧ valid-sops-expr t c₂) ∧ valid-sops-stmt t s₁ ∧ valid-sops-stmt t s₂
valid-sops-stmt t (Seq s₁ s₂) = (valid-sops-expr t e₁ ∧ valid-sops-stmt t s₁ ∧ valid-sops-stmt t s₂)
valid-sops-stmt t (Cond e s₁ s₂) = (valid-sops-expr t e ∧ valid-sops-stmt t s₁ ∧ valid-sops-stmt t s₂)
valid-sops-stmt t (While e s) = (valid-sops-expr t e ∧ valid-sops-stmt t s)
valid-sops-stmt t (SGhost A L R W) = True
valid-sops-stmt t SFence = True

**type-synonym** stmt-config = stmt × nat
**consts** isTrue:: val ⇒ bool

**inductive** stmt-step:: tmps ⇒ stmt-config ⇒ stmt-config × instrs ⇒ bool
(- ⊢ - →s - [60,60,60] 100)
**for** θ

**where**

AssignAddr:
∀ sop, a ≠ Tmp sop ⇒
θ ⊢ (Assign volatile a e A L R W, t) →s
((Assign volatile (Tmp (eval-expr t a)) e A L R W, t + used-tmps a), issue-expr t a)

Assign:
D ⊆ dom θ ⇒
θ ⊢ (Assign volatile (Tmp (D,a)) e A L R W, t) →s
((Skip, t + used-tmps e),
issue-expr t e@0|Write volatile (a θ) (eval-expr t e) (A θ) (L θ) (R θ) (W θ)])

CASAddr:
∀ sop, a ≠ Tmp sop ⇒
θ ⊢ (CAS a c₁ c₂ e A L R W, t) →s
((CAS (Tmp (eval-expr t a)) c₁ c₂ e A L R W, t + used-tmps a), issue-expr t a)

CASComp:
∀ sop, c₁ ≠ Tmp sop ⇒
θ ⊢ (CAS (Tmp (D₁,a)) c₁ c₂ e A L R W, t) →s
\[
(CAS \ (Tmp \ (D_a, a)) \ (Tmp \ (eval-expr \ t \ c_e)) \ s_e \ A \ L \ R \ W, \ t + \ used-tmps \ c_e), \ issuexpr \ t \ c_e)
\]

| CAS:  
| \[D_a \subseteq dom \ \emptyset; \ D_c \subseteq dom \ \emptyset; \ eval-expr \ t \ s_e = (D,f) \]  
| \[\emptyset \vdash (CAS \ (Tmp \ (D_a,a)) \ (Tmp \ (D_c,c)) \ s_e \ A \ L \ R \ W, \ t) \rightarrow_s \]
| \[(\text{Skip, Suc} \ (t + \ used-tmps \ s_e)), \ issuexpr \ t \ s_e \]  
| \[\text{RMW} \ (a \ \emptyset) \ (t + \ used-tmps \ s_e) \ (D,f) \ (\lambda \ \emptyset. \ \text{the} \ (\emptyset \ (t + \ used-tmps \ s_e)) = c \ \emptyset) \ (\lambda v_1 \ v_2. \ v_1)\]
| \[(A \ \emptyset) \ (L \ \emptyset) \ (R \ \emptyset) \ (W \ \emptyset) \]  

| Seq:  
| \[\emptyset \vdash (s_1, t) \rightarrow_s ((s_1', t'), \ is) \]
| \[\emptyset \vdash (Seq \ s_1 \ s_2, t) \rightarrow_s ((Seq \ s_1', s_2', \ t'), is)\]

| SeqSkip:  
| \[\emptyset \vdash (Seq \ Skip \ s_2, t) \rightarrow_s ((s_2, t), [])\]

| Cond:  
| \[\forall \ sop. \ e \neq Tmp \ sop \]
| \[\emptyset \vdash (Cond \ e \ s_1 \ s_2, t) \rightarrow_s \]
| \[(\text{Cond} \ (Tmp \ (eval-expr \ t \ e)) \ s_1 \ s_2, \ t + \ used-tmps \ e), \ issuexpr \ t \ e) \]

| CondTrue:  
| \[D \subseteq dom \ \emptyset; \ isTrue \ (e \ \emptyset)]  
| \[\emptyset \vdash (Cond \ (Tmp \ (D,e)) \ s_1 \ s_2, t) \rightarrow_s ((s_1, t), [])\]

| CondFalse:  
| \[D \subseteq dom \ \emptyset; \ \neg \ isTrue \ (e \ \emptyset)]  
| \[\emptyset \vdash (Cond \ (Tmp \ (D,e)) \ s_1 \ s_2, t) \rightarrow_s ((s_2, t), [])\]

| While:  
| \[\emptyset \vdash (While \ e \ s, t) \rightarrow_s \]
| \[(\text{Cond} \ e \ (Seq \ s \ (While \ e \ s)) \ \text{Skip, t}, [])\]

| SGhost:  
| \[\emptyset \vdash (SGhost \ A \ L \ R \ W, t) \rightarrow_s ((\text{Skip, t}, [\text{Ghost} \ (A \ \emptyset) \ (L \ \emptyset) \ (R \ \emptyset) \ (W \ \emptyset)])\]

| SFence:  
| \[\emptyset \vdash (SFence, t) \rightarrow_s ((\text{Skip, t}), []\text{Fence})\]

**Inductive-Cases** stmt-step-cases [cases set]:  
\[\emptyset \vdash (Skip, t) \rightarrow_s c\]
\[\emptyset \vdash (Assign \ volatile \ a \ e \ A \ L \ R \ W, t) \rightarrow_s c\]
\textbf{lemma} valid-sops-expr-mono: \( \forall t t'. \text{valid-sops-expr } t \ e \implies t \leq t' \implies \text{valid-sops-expr } t' \ e \) 
\textit{(proof)}

\textbf{lemma} valid-sops-stmt-mono: \( \forall t t'. \text{valid-sops-stmt } t \ s \implies t \leq t' \implies \text{valid-sops-stmt } t' \ s \) 
\textit{(proof)}

\textbf{lemma} valid-sops-stmt-invariant: 
\textit{assumes} step: \( \emptyset \vdash (s,t) \rightarrow_s ((s',t'),\text{is}) \) 
\textit{shows} \( t \leq t' \) 
\textit{(proof)}

\textbf{lemma} stmt-step-tmps-count-mono: 
\textit{assumes} step: \( \emptyset \vdash (s,t) \rightarrow_s ((s',t'),\text{is}) \) 
\textit{shows} \( t \leq t' \) 
\textit{(proof)}

\textbf{lemma} map-le-restrict-map-eq: \( m_1 \subseteq m \implies D \subseteq \text{dom } m_1 \implies m_2 |^r D = m_1 |^r D \) 
\textit{(proof)}

\textbf{lemma} sbh-step-preserves-load-tmps-bound: 
\textit{assumes} step: \( (is,\mathcal{O},D,\emptyset,\text{sb},\mathcal{S},m) \rightarrow_{\text{sbh}} (is',\mathcal{O}',D',\emptyset',\text{sb}',\mathcal{S}',m') \) 
\textit{assumes} less: \( \forall i \in \text{load-tmps } is. \ i < n \) 
\textit{shows} \( \forall i \in \text{load-tmps } is'. \ i < n \) 
\textit{(proof)}

\textbf{lemma} sbh-step-preserves-read-tmps-bound: 
\textit{assumes} step: \( (is,\emptyset,\text{sb},m,\mathcal{D},\mathcal{O},\mathcal{S}) \rightarrow_{\text{sbh}} (is',\emptyset',\text{sb}',m',\mathcal{D}',\mathcal{O}',\mathcal{S}') \) 
\textit{assumes} less-is: \( \forall i \in \text{load-tmps } is. \ i < n \) 
\textit{assumes} less-sb: \( \forall i \in \text{read-tmps } sb. \ i < n \)
shows \( \forall i \in \text{read-tmps } s b', i < n \)
\(\langle \text{proof} \rangle \)

**lemma** sbh-step-preserves-tmps-bound:
**assumes** step: \((i s', 0, s b, m, D, O, S) \rightarrow_{\text{sbh}} (i s', 0', s b', m', D', O', S')\)
**assumes** less-dom: \( \forall i \in \text{dom } 0. \ i < n \)
**assumes** less-is: \( \forall i \in \text{load-tmps } i s. \ i < n \)
**shows** \( \forall i \in \text{dom } 0'. \ i < n \)
\(\langle \text{proof} \rangle \)

**lemma** flush-step-preserves-read-tmps:
**assumes** step: \((m, s b, O) \rightarrow_f (m', s b', O')\)
**assumes** less-sb: \( \forall i \in \text{read-tmps } s b. \ i < n \)
**shows** \( \forall i \in \text{read-tmps } s b'. \ i < n \)
\(\langle \text{proof} \rangle \)

**lemma** flush-step-preserves-write-sops:
**assumes** step: \((m, s b, O) \rightarrow_f (m', s b', O')\)
**assumes** less-sb: \( \forall i \in \bigcup \ (\text{fst ' write-sops } s b). \ i < t \)
**shows** \( \forall i \in \bigcup \ (\text{fst ' write-sops } s b'). \ i < t \)
\(\langle \text{proof} \rangle \)

**lemma** issue-expr-load-tmps-range':
\( \bigwedge t. \ \text{load-tmps } (\text{issue-expr } t \ e) = \{ i. \ t \leq i \land i < t + \text{used-tmps } e \} \)
\(\langle \text{proof} \rangle \)

**lemma** issue-expr-load-tmps-range:
\( \bigwedge t. \ \forall i \in \text{load-tmps } (\text{issue-expr } t \ e). \ t \leq i \land i < t + (\text{used-tmps } e) \)
\(\langle \text{proof} \rangle \)

**lemma** stmt-step-load-tmps-range':
**assumes** step: \( 0 \vdash (s, t) \rightarrow_s ((s', t'), i s) \)
**shows** load-tmps is = \( \{ i. \ t \leq i \land i < t' \} \)
\(\langle \text{proof} \rangle \)

**lemma** stmt-step-load-tmps-range:
**assumes** step: \( 0 \vdash (s, t) \rightarrow_s ((s', t'), i s) \)
**shows** \( \forall i \in \text{load-tmps } i s. \ t \leq i \land i < t' \)
\(\langle \text{proof} \rangle \)

**lemma** distinct-load-tmps-issue-expr:
\( \bigwedge t. \ \text{distinct-load-tmps } (\text{issue-expr } t \ e) \)
\(\langle \text{proof} \rangle \)

**lemma** max-used-load-tmps:
\( t + \text{used-tmps } e \notin \text{load-tmps } (\text{issue-expr } t \ e) \)
\(\langle \text{proof} \rangle \)
lemma stmt-step-distinct-load-tmps:
assumes step: \( \emptyset \vdash (s, t) \rightarrow_s ((s', t'), is) \)
shows distinct-load-tmps is
(proof)

lemma store-sops-issu-expr [simp]: \( \forall t. \text{store-sops (issue-expr } t \ e) = \{\} \)
(proof)

lemma stmt-step-data-store-sops-range:
assumes step: \( \emptyset \vdash (s, t) \rightarrow_s ((s', t'), is) \)
assumes valid: valid-sops-stmt t s
shows \( \forall (D, f) \in \text{store-sops is}. \forall i \in D. i < t' \)
(proof)

lemma sbh-step-distinct-load-tmps-prog-step:
assumes step: \( \emptyset \vdash (s, t) \rightarrow_s ((s', t'), is') \)
assumes load-tmps-le: \( \forall i \in \text{load-tmps is}. i < t \)
assumes read-tmps-le: \( \forall i \in \text{read-tmps sb}. i < t \)
shows distinct-load-tmps is' \( \wedge (\text{load-tmps is'} \cap \text{load-tmps is} = \{\}) \wedge (\text{load-tmps is'} \cap \text{read-tmps sb}) = \{\}) \)
(proof)

lemma data-dependency-consistent-instrs-issue-expr:
\( \forall t T. \text{data-dependency-consistent-instrs } t \text{ } (\text{issue-expr } t \ e) \)
(proof)

lemma dom-eval-expr:
\( \forall t. \text{[valid-sops-expr } t \ e; x \in \text{fst (eval-expr } t \ e)] \implies x \in \{i. i < t\} \cup \text{load-tmps (issue-expr } t \ e) \)
(proof)

lemma Cond-not-s1: \( s_1 \neq \text{Cond } e s_1 s_2 \)
(proof)

lemma Cond-not-s2: \( s_2 \neq \text{Cond } e s_1 s_2 \)
(proof)

lemma Seq-not-s1: \( s_1 \neq \text{Seq } s_1 s_2 \)
(proof)

lemma Seq-not-s2: \( s_2 \neq \text{Seq } s_1 s_2 \)
(proof)

lemma prog-step-progress:
assumes step: \( \emptyset \vdash (s, t) \rightarrow_s ((s', t'), is) \)
shows \((s', t') \neq (s, t) \lor is \neq \[]\)
(proof)
**Lemma stmt-step-data-dependency-consistent-instrs:**

**Assumes** step: \( \emptyset \vdash (s, t) \rightarrow_s ((s', t'), is) \)

**Assumes** valid: valid-sops-stmt t s

**Shows** data-dependency-consistent-instrs \( \{i. i < t\} \) is

\( \langle \text{proof} \rangle \)

**Lemma sbh-valid-data-dependency-prog-step:**

**Assumes** step: \( \emptyset \vdash (s, t) \rightarrow_s ((s', t'), is) \)

**Assumes** store-sops-le: \( \forall i \in \bigcup (\text{fst} \ '+\text{store-sops is}) \cdot i < t \)

**Assumes** write-sops-le: \( \forall i \in \bigcup (\text{fst} \ '+\text{write-sops sb}) \cdot i < t \)

**Assumes** valid: valid-sops-stmt t s

**Shows** data-dependency-consistent-instrs \( \{i. i < t\} \) is

\( \langle \text{proof} \rangle \)

\[\text{load-tmps is}' \cap \bigcup (\text{fst} \ '+\text{store-sops is}) = \{\} \wedge \text{load-tmps is}' \cap \bigcup (\text{fst} \ '+\text{write-sops sb}) = \{\} \]

**Lemma sbh-load-tmps-fresh-prog-step:**

**Assumes** step: \( \emptyset \vdash (s, t) \rightarrow_s ((s', t'), is) \)

**Assumes** tmps-le: \( \forall i \in \text{dom } \emptyset. i < t \)

**Shows** load-tmps is' \( \cap \text{dom } \emptyset = \{\} \)

\( \langle \text{proof} \rangle \)

**Lemma sbh-valid-sops-prog-step:**

**Assumes** step: \( \emptyset \vdash (s, t) \rightarrow_s ((s', t'), is) \)

**Assumes** valid: valid-sops-stmt t s

**Assumes** \( \forall \text{sop} \in \text{store-sops is}. \text{valid-sop sop} \)

\( \langle \text{proof} \rangle \)

**Primrec procs:**

\( 'a \ \text{memref list} \Rightarrow 'a \ \text{set} \)

**Where**

\( \text{procs } [] = \{\} \)

\( \text{procs } (x \# xs) = (\text{case } x \text{ of} \) \( \text{Progsb } p \ p' \text{ is } \Rightarrow \{p, p'\} \cup \text{procs } xs \)

\( \text{ - } \Rightarrow \text{procs } xs) \)

**Lemma procs-append:** \( \forall ys. \text{procs } (xs \circ@ ys) = \text{procs } xs \cup \text{procs } ys \)

\( \langle \text{proof} \rangle \)

**Lemma procs-in1:** \( \text{Progsb } p_1 p_2 \text{ is } \in \text{ set } xs \Rightarrow p_1 \in \text{procs } xs \)

\( \langle \text{proof} \rangle \)

**Lemma procs-in2:** \( \text{Progsb } p_1 p_2 \text{ is } \in \text{ set } xs \Rightarrow p_2 \in \text{procs } xs \)

\( \langle \text{proof} \rangle \)

**Lemma procs-mono:** \( \forall ys. \text{set } xs \subseteq \text{ set } ys \Rightarrow \text{procs } xs \subseteq \text{procs } ys \)

\( \langle \text{proof} \rangle \)

138
locale separated-tmps =
fixes ts
assumes valid-sops-stmt: \[ i < \text{length} \text{ ts}; \text{tsli} = ((s,t),is,\emptyset,\text{sb},D,O)] \implies \text{valid-sops-stmt t s}
assumes valid-sops-stmt-sb: \[ i < \text{length} \text{ ts}; \text{tsli} = ((s,t),is,\emptyset,\text{sb},D,O); (s',t') \in \text{prog-configs sb}] \implies \text{valid-sops-stmt t' s'}
assumes load-tmps-le: \[ i < \text{length} \text{ ts}; \text{tsli} = ((s,t),is,\emptyset,\text{sb},D,O)] \implies \forall i \in \text{load-tmps is}. i < t
assumes read-tmps-le: \[ i < \text{length} \text{ ts}; \text{tsli} = ((s,t),is,\emptyset,\text{sb},D,O)] \implies \forall i \in \text{read-tmps sb}. i < t
assumes store-sops-le: \[ i < \text{length} \text{ ts}; \text{tsli} = ((s,t),is,\emptyset,\text{sb},D,O)] \implies \forall i \in \bigcup (\text{fst ' store-sops is}). i < t
assumes write-sops-le: \[ i < \text{length} \text{ ts}; \text{tsli} = ((s,t),is,\emptyset,\text{sb},D,O)] \implies \forall i \in \bigcup (\text{fst ' write-sops sb}). i < t
assumes tmps-le: \[ i < \text{length} \text{ ts}; \text{tsli} = ((s,t),is,\emptyset,\text{sb},D,O)] \implies \text{dom } \emptyset \cup \text{load-tmps is} = \{i. i < t\}

lemma (in separated-tmps) tmps-le':
assumes i-bound: i < \text{length ts}
assumes ts-i: tsli = ((s,t),is,\emptyset,\text{sb},D,O)
s shows \forall i \in \text{dom } \emptyset. i < t
⟨proof⟩

lemma (in separated-tmps) separated-tmps-nth-update:
\[ i < \text{length ts}; \text{valid-sops-stmt t s}; \forall (s',t') \in \text{prog-configs sb}. \text{valid-sops-stmt t' s'}; \forall i \in \text{load-tmps is}. i < t; \forall i \in \text{read-tmps sb}. i < t; \text{dom } \emptyset \cup \text{load-tmps is} = \{i. i < t\}\]
\implies
\text{separated-tmps (ts[i:=(s,t),is,\emptyset,\text{sb},D,O])}
⟨proof⟩

lemma hd-prog-app-in-first: \forall ys. \text{Prog}_{\text{sb}} p p' is \in \text{set} xs \implies \text{hd-prog q (xs @ ys)} = \text{hd-prog q xs}
⟨proof⟩

lemma hd-prog-app-in-eq: \forall ys. \text{Prog}_{\text{sb}} p p' is \in \text{set} xs \implies \text{hd-prog q xs} = \text{hd-prog q xs}
⟨proof⟩

lemma hd-prog-app-notin-first: \forall ys. \forall p p' is. \text{Prog}_{\text{sb}} p p' is /\in \text{set} xs \implies \text{hd-prog q (xs @ ys)} = \text{hd-prog q ys}
⟨proof⟩

lemma union-eq-subsetD: A \cup B = C \implies A \cup B \subseteq C \land C \subseteq A \cup B
⟨proof⟩
lemma prog-step-preserves-separated-tmps:
  assumes i-bound: i < length ts
  assumes ts-i: ts[i] = (p, is, 0, sb, D, O)
  assumes prog-step: \( \theta \cdot p \rightarrow_s (p', is') \)
  assumes sep: separated-tmps ts
  shows separated-tmps
    (ts[i] = (p', is', 0, sb, [Prog sb p p' is'], D, O))
  \( \langle proof \rangle \)

lemma flush-step-sb-subset:
  assumes step: (m, sb, O) \( \rightarrow_f (m', sb', O') \)
  shows set sb' \( \subseteq \) set sb
  \( \langle proof \rangle \)

lemma flush-step-preserves-separated-tmps:
  assumes i-bound: i < length ts
  assumes ts-i: ts[i] = (p, is, 0, sb, D, O, R)
  assumes flush-step: (m, sb, O, R, S) \( \rightarrow_f (m', sb', O', R', S') \)
  assumes sep: separated-tmps ts
  shows separated-tmps (ts[i] = (p, is, 0, sb, D, O, R'))
  \( \langle proof \rangle \)

lemma sbh-step-preserves-store-sops-bound:
  assumes step: (is, 0, sb, m, D, O, R, S) \( \rightarrow_{sbh} (is', 0', sb', m', D', O', R', S') \)
  assumes store-sops-le: \( \forall i \in \bigcup (\text{fst} i \text{ store-sops is}). \ i < t \)
  shows \( \forall i \in \bigcup (\text{fst} i \text{ store-sops is'}) . \ i < t \)
  \( \langle proof \rangle \)

lemma sbh-step-preserves-write-sops-bound:
  assumes step: (is, 0, sb, m, D, O, R, S) \( \rightarrow_{sbh} (is', 0', sb', m', D', O', R', S') \)
  assumes store-sops-le: \( \forall i \in \bigcup (\text{fst} i \text{ store-sops is}). \ i < t \)
  assumes write-sops-le: \( \forall i \in \bigcup (\text{fst} i \text{ write-sops sb}). \ i < t \)
  shows \( \forall i \in \bigcup (\text{fst} i \text{ write-sops sb'}). \ i < t \)
  \( \langle proof \rangle \)

lemma sbh-step-prog-configs-eq:
  assumes step: (is, 0, sb, m, D, O, R, S) \( \rightarrow_{sbh} (is', 0', sb', m', D', O', R', S') \)
  shows prog-configs sb' = prog-configs sb
  \( \langle proof \rangle \)

lemma sbh-step-preserves-tmps-bound':
  assumes step: (is, 0, sb, m, D, O, R, S) \( \rightarrow_{sbh} (is', 0', sb', m', D', O', R', S') \)
  shows dom 0 \( \cup \) load-tmps is = dom 0' \( \cup \) load-tmps is'
  \( \langle proof \rangle \)

lemma sbh-step-preserves-separated-tmps:
  assumes i-bound: i < length ts
  assumes ts-i: ts[i] = (p, is, 0, sb, D, O, R)
  assumes memop-step: (is, 0, sb, m, D, O, R, S) \( \rightarrow_{sbh} \)
\[ (i', \varnothing', s'b', m', D', O', R', S') \]

**assumes** instr: separated-tmps ts
**shows** separated-tmps \( (ts[i:= (p, i', s'b', D', O', R')] ) \)

\( \langle \text{proof} \rangle \)

**definition**
valid-pimp ts \( \equiv \) separated-tmps ts

**lemma** prog-step-preserves-valid:
**assumes** i-bound: \( i < \text{length ts} \)
**assumes** ts-i: ts[i] = (p, i', s'b::stmt-config store-buffer, D, O, R)
**assumes** prog-step: \( \varnothing \vdash p \rightarrow_s (p', i') \)
**assumes** valid: valid-pimp ts
**shows** valid-pimp \( (ts[i:= (p', i', s'b', D, O, R')] ) \)

\( \langle \text{proof} \rangle \)

**lemma** flush-step-preserves-valid:
**assumes** i-bound: \( i < \text{length ts} \)
**assumes** ts-i: ts[i] = (p, i', s'b::stmt-config store-buffer, D, O, R)
**assumes** flush-step: \( (m, s'b, O, R, S) \rightarrow_{f} (m', s'b', O', R', S') \)
**assumes** valid: valid-pimp ts
**shows** valid-pimp \( (ts[i:= (p', i', s'b', D, O', R')] ) \)

\( \langle \text{proof} \rangle \)

**lemma** sbh-step-preserves-valid:
**assumes** i-bound: \( i < \text{length ts} \)
**assumes** ts-i: ts[i] = (p, i', s'b::stmt-config store-buffer, D, O, R)
**assumes** memop-step: \( (i, \varnothing, s'b, m, D, O, R, S) \rightarrow_{sbh} (i', \varnothing', s'b', m', D', O', R', S') \)
**assumes** valid: valid-pimp ts
**shows** valid-pimp \( (ts[i:= (p', i', s'b', D', O', R')] ) \)

\( \langle \text{proof} \rangle \)

**lemma** hd-prog-prog-configs: \( \text{hd-prog p s b} = p \lor \text{hd-prog p s b} \in \text{prog-configs sb} \)

\( \langle \text{proof} \rangle \)

**interpretation** PIMP: \( \lambda (s, t). \text{valid-sops-stmt t s} \)
valid-pimp

\( \langle \text{proof} \rangle \)

**thm** PIMP.concurrent-direct-steps-simulates-store-buffer-history-step
**thm** PIMP.concurrent-direct-steps-simulates-store-buffer-history-steps
**thm** PIMP.concurrent-direct-steps-simulates-store-buffer-step

We can instantiate PIMP with the various memory models.

**interpretation** direct:
computation direct-memop-step empty-storebuffer-step stmt-step \( \lambda p \ p' \) is sb. \( \langle \text{proof} \rangle \)

**interpretation** virtual:
computation virtual-memop-step empty-storebuffer-step stmt-step \( \lambda p \ p' \) is sb. \( \langle \text{proof} \rangle \)

**interpretation** store-buffer:
computation sb-memop-step store-buffer-step stmt-step \( \lambda p \ p' \) is sb. sb \( \langle \text{proof} \rangle \)
interpretation store-buffer-history:
computation sbh-memop-step flush-step stmt-step λp p′ is sb. sb ⊕ [Prog sb p p′]

abbreviation direct-pimp-step::
(stmt-config, unit, bool, owns, rels, shared) global-config ⇒
(stmt-config, unit, bool, owns, rels, shared) global-config ⇒ bool
(- ⇒_{dp} - [60,60] 100)

where
c ⇒_{dp} d ≡ direct.concurrent-step c d

abbreviation direct-pimp-steps::
(stmt-config, unit, bool, owns, rels, shared) global-config ⇒
(stmt-config, unit, bool, owns, rels, shared) global-config ⇒ bool
(- ⇒_{dp} ∗ - [60,60] 100)

where
direct-pimp-steps == direct-pimp-step^∗

Execution examples lemma Assign-Const-ex:

\[\begin{align*}
((\text{Assign True (Tmp (\{ \},λθ. a)) (Const c) (λθ. A) (λθ. L) (λθ. R) (λθ. W}}, t), [], [], (\mathcal{D}, \mathcal{O}, \mathcal{R}]), m, S) &\Rightarrow_{dp}^∗ \\
((\text{Skip}, t), [], [], (\mathcal{D}, \mathcal{O}, \mathcal{R})), m(a := c), S \oplus_w R \ominus_A L)
\end{align*}\]

⟨proof⟩

lemma

\[\begin{align*}
((\text{Assign True (Tmp (\{ \},λθ. a)) (Binop (+) (Mem True x) (Mem True y)) (λθ. A) (λθ. L) (λθ. R) (λθ. W}), t), [], [], (\mathcal{D}, \mathcal{O}, \mathcal{R})), m, S) &\Rightarrow_{dp}^∗ \\
((\text{Skip}, t + 2), [], [], (\mathcal{D}, \mathcal{O}, \mathcal{R})), m(a := m x + m y), S \oplus_w R \ominus_A L)
\end{align*}\]

⟨proof⟩

lemma assumes isTrue: isTrue c

shows

\[\begin{align*}
((\text{Cond (Const c) (Assign True (Tmp (\{ \},λθ. a)) (Assign True (Tmp (\{ \},λθ. a)) (Const c) (λθ. A) (λθ. L) (λθ. R) (λθ. W)}, Skip), t), [], [], (\mathcal{D}, \mathcal{O}, \mathcal{R})), m, S) &\Rightarrow_{dp}^∗ \\
((\text{Skip}, t), [], [], (\mathcal{D}, \mathcal{O}, \mathcal{R})), m(a := c), S \oplus_w R \ominus_A L)
\end{align*}\]

⟨proof⟩

end

References


