Implementing and Verifying Release-Acquire Transactional Memory (Extended Version)

SADEGH DALVANDI, University of Surrey, UK
BRIJESH DONGOL, University of Surrey, UK

Transactional memory (TM) is an intensively studied synchronisation paradigm with many proposed implementations in software and hardware, and combinations thereof. However, TM under relaxed memory, e.g., C11 (the 2011 C/C++ standard) is still poorly understood, lacking rigorous foundations that support verifiable implementations. This paper addresses this gap by developing TMS2-RA, a relaxed operational TM specification. We integrate TMS2-RA with RC11 (the repaired C11 memory model that disallows load-buffering) to provide a formal semantics for TM libraries and their clients. We develop a logic, TARO, for verifying client programs that use TMS2-RA for synchronisation. We also show how TMS2-RA can be implemented by a C11 library, TML-RA, that uses relaxed and release-acquire atomics, yet guarantees the synchronisation properties required by TMS2-RA. We benchmark TML-RA and show that it outperforms its sequentially consistent counterpart in the STAMP benchmarks. Finally, we use a simulation-based verification technique to prove correctness of TML-RA. Our entire development is supported by the Isabelle/HOL proof assistant.

Additional Key Words and Phrases: Weak Memory, Transactional Memory, C11, Verification, Refinement

1 INTRODUCTION

The advent and proliferation of architectures implementing relaxed memory models has resulted in many new challenges in the development of concurrent programs. In the context of the C/C++ relaxed memory model defined by C11, over a decade’s worth of research has resulted in rigorous semantic foundations [Batty et al. 2016, 2011; Kang et al. 2017; Lahav et al. 2017; Lee et al. 2020; Paviotti et al. 2020], and more recently, logics for reasoning about the correctness of concurrent programs [Dalvandi et al. 2020a, 2022; Doherty et al. 2019; Doko and Vafeiadis 2017; He et al. 2016; Kaiser et al. 2017; Kang et al. 2017; Lahav and Vafeiadis 2015; Vafeiadis and Narayan 2013; Wright et al. 2021]. These works have provided the background necessary to develop high-level abstractions and concurrency libraries over relaxed-memory architectures. Recent works have included reimplementations of concurrent data structures [Dalvandi and Dongol 2021; Dongol et al. 2018b; Emmi and Enea 2019; Krishna et al. 2020; Raad et al. 2019a], including those with relaxed specifications that aim to exploit the additional behaviours allowed by relaxed memory.

Our aim for this paper is to implement and verify synchronisation abstractions, fine-tuned for C11, in the form of transactional memory (TM) libraries, which provide reusable foundations for high-performance, yet easy to manage concurrency control [Guerraoui and Kapalka 2010; Herlihy and Moss 1993; Shavit and Touitou 1997]. Implementations include those in software (as STM libraries) and hardware (Intel-RTM and Armv9). Other variations include hybrid TM that combine software and hardware TMs and implementations that are natively supported by the compiler (e.g., the continued C++ TM Lite development). In addition to supporting general-purpose concurrency, TM has also been used to develop transactional concurrent objects and data structures [Assa et al. 2020, 2021; Bronson et al. 2010; Lesani et al. 2022]. Intel’s persistent memory development kit (PMDK) [Scargall 2020] extensively promotes the transactional paradigm (though multi-threaded

1C11 refers to the 2011 ISO specification of C/C++.
transactions are not directly supported by PMDK’s transactions). These prior works have assumed SC transactions, i.e., that transactional access provide the same guarantees as sequentially consistent memory. Our focus is the verification of STMs implemented as a programming language library with relaxed, release, acquire and release-acquire accesses providing a pathway towards simplified development of transactional objects (including concurrent data structures) for relaxed memory.

TM implementations provide fine-grained interleaving (for efficiency) that execute with an illusion of atomicity (for correctness). A completed transaction may be committed or aborted so that all or none of its effects are externally visible. TM implementations are designed to satisfy a variety of correctness conditions such as (strict) serialisability, opacity, and snapshot isolation, which restrict ordering possibilities of completed transactions. TM has been extensively studied for sequentially consistent (SC) architectures [Lamport 1979], but implementations over relaxed memory are limited.

Prior works on relaxed memory transactions (e.g., [Chong et al. 2018; Dongol et al. 2018a]) have focussed on foundations of hardware transactions and their interaction with relaxed memory models, e.g., the expected isolation guarantees, reordering possibilities etc. The work of Chong et al [Chong et al. 2018] also provides for semantics of native C++ transactions. However, native TM support in C++ is still in a state of flux [Spear et al. 2020; Zardoshti et al. 2019] and the underlying designs have changed since the original works by Chong et al [Chong et al. 2018]. Moreover, these semantics are presented in an axiomatic (aka declarative) style, which cannot be used to verify TM implementations, where we require operational descriptions of correctness. Therefore, our point of departure is a separate set of works on TM specifications, in particular the TMS2 specification [Doherty et al. 2013], which has been used extensively as a TM specification for standard (i.e., SC) architectures.

More recent works have taken steps towards C++ implementations, including native support of TM within C++ [Zardoshti et al. 2019] and STMs implemented using C++ relaxed memory [Rodriguez and Spear 2020]. However, Zardoshti et al. [2019] do not describe interactions with the C11 relaxed memory model, while Rodriguez and Spear [Rodriguez and Spear 2020] focus on data race freedom and privatisation guarantees. Neither of these works have a formal semantics, nor are they supported by a verification methodology. (See §7 for a more comprehensive survey of related works.)

Our work addresses several gaps in the current state-of-the-art of transactions for C/C++. We work with RC11, i.e., the repaired C11 memory model [Lahav et al. 2017]. The RC11 memory model disallows program-order and reads-from cycles, and hence disallows load-buffering behaviour. This restriction greatly simplifies reasoning and variants of RC11 are supported by a number of different logics [Dalvandi et al. 2020a; Dalvandi and Dongol 2021; Dalvandi et al. 2022; Dang et al. 2022; Kaiser et al. 2017; Lahav and Vafeiadis 2015]. Logics that address the full C11 memory model (allowing load buffering) have also been developed, but proofs in these logics are limited to small litmus tests [Svendsen et al. 2018; Wright et al. 2021].

We develop: (i) a reusable specification of TM that provides well-defined guarantees to those developing client programs; (ii) techniques for verifying client programs in C11 that use such TM abstractions; (iii) implementations of TM in C11, including their rigorous verification; and (iv) mechanisation of the verification described above in the theorem prover Isabelle/HOL. We discuss these contributions in more detail below.

Correctness specifications. To enable verification, we start with the TMS2 specification [Doherty et al. 2013]. TMS2 implies the TMS1 specification, which is known to be both necessary and sufficient for observational refinement (of client programs) [Attiya et al. 2018]. The main difference between TMS1 and TMS2 is that TMS1 allows aborted transactions to observe different serialization
Implementing and Verifying Release-Acquire Transactional Memory (Extended Version) 1:3

orders [Lesani et al. 2012]. In contrast, TMS2, like opacity [Guerraoui and Kapalka 2010], ensures strict serializability of the committed transactions and furthermore that aborted transactions are consistent with the serialisation order. Although more restrictive than TMS1, TMS2 has been shown to be a robust correctness condition that is useful in practice, providing a specification for a number of TM implementations under SC [Armstrong and Dongol 2017; Armstrong et al. 2017; Derrick et al. 2018; Doherty et al. 2016].

Under relaxed memory, the TMS2 specification is inadequate since it does not provide any of the client-side guarantees required by relaxed memory libraries [Dalvandi and Dongol 2021; Dongol et al. 2018b; Raad et al. 2019a, 2018]. Such client-side guarantees are required under relaxed memory since writes in one thread are not guaranteed to be propagated to other threads unless the library is properly synchronised (cf. the message passing litmus tests [Alglave et al. 2014]).

Our first contribution is the adaptation of TMS2 to address this issue. In particular, our specification, TMS2-ra, provides a flexible meaning of correctness, allowing a client to specify relaxed, releasing, acquiring and release-acquiring transactions (see §3), mimicking the memory annotations of C11 atomics [Batty et al. 2011]. This provides greater flexibility in TM design; we develop a model in which these different types of transactions co-exist within the same TM system.

Client verification. Our second contribution (see §5) is a verification technique for relaxed-memory client programs that use TMS2-ra. In particular, we prove correctness of several variations of the message passing litmus test, synchronised through TMS2-ra transactions, to show that TMS2-ra behaves as expected. In particular, we show how different client-side guarantees are achieved depending on the type of synchronisation guarantee (relaxed, releasing or acquiring) guaranteed by the transaction in question.

Our verification framework includes a new logic, TARO, capable of efficiently reasoning about the views of a client programs [Dalvandi et al. 2022; Kaiser et al. 2017]. This means that the correctness of programs can be established using a standard Owicki-Gries reasoning framework [Dalvandi et al. 2020a; Dalvandi and Dongol 2021; Owicki and Gries 1976].

Implementation, benchmarking and verification. Our third contribution is the implementation and full verification of an STM algorithm that uses C11 relaxed/release-acquire atomics and implements TMS2-ra. Our implementation is an adaptation of Dalessandro et al.’s Transactional Mutex Lock (TML) [Dalessandro et al. 2010], which presents a simple mechanism for synchronising transactions optimised for read-heavy workloads. TML is synchronised using a single global lock, and allows multiple concurrent read-only transactions, but at most one writing transaction, i.e., a writing transaction causes all other concurrent transactions to abort.

Interestingly, our adapted algorithm, which we call TML-ra, allows more concurrency than TML by exploiting the parallelism afforded by relaxed and release-acquire C11 atomics. Moreover, a writing transaction does not force other read-only transactions to abort, allowing greater read/write parallelism (see §4). We show that this theoretical speedup manifests in real implementations and TML-ra outperforms its SC counterpart in all STAMP benchmarks (see §4.3).

We use a simulation-based verification method for the C11 memory model [Dalvandi and Dongol 2021] to prove correctness of TML-ra. This proof establishes a refinement between TML-ra and TMS2-ra, which ensures that all observable behaviours of TML-ra are observable behaviours of TMS2-ra. Thus, if a client program C is proved correct when it uses TMS2-ra, then C will also be correct if we replace calls to TMS2-ra in C by calls to TML-ra.

Mechanisation. Our fourth contribution is the mechanisation of all proofs presented in the paper in the Isabelle/HOL proof assistant (available as supplementary material). This includes the operational semantics of C11 integrated with TMS2-ra, soundness of all TARO rules, the use
Sadegh Dalvandi and Brijesh Dongol

1:4 Thread $\tau_1$
1: $d := 5$;
2: $f := 1$;
3: do $r_1 \leftarrow f$
until $r_1 = 1$;
4: $r_2 \leftarrow d$;
\{ $r_2 = 0 \lor r_2 = 5$ \}

(a) Unsynchronised MP

Thread $\tau_2$
1: $d := 5$;
2: $f := R$;
3: $f := A$ $r_1 \leftarrow f$
until $r_1 = 1$;
4: $r_2 \leftarrow d$;
\{ $r_2 = 5$ \}

(b) Synchronised MP

Fig. 1. Message passing (MP) in C11

Overview. This paper is structured as follows. We describe our requirements for relaxed and release-acquire transactions in §2. We formalise this semantics in §3 via the TMS2-ra specification, and describe its integration with a view-based semantics for RC11 with release-acquire atomics [Dalvandi et al. 2020a]. In §4, we provide an examplar implementation and benchmarking results for TML-ra. In §5, we present our logic for reasoning about release-acquire transactional memory, which provides a method of reasoning about client programs that use the TMS2-ra specification. Finally, in §6, we present a proof of correctness of TML-ra via refinement w.r.t. TMS2-ra.

2 TRANSACTIONAL GUARANTEES IN C11

A TM specification in a relaxed memory setting has two distinct sets of goals. The first set must guarantee the expected behaviours of transactions, e.g., serializability, opacity etc. The second must provide client-side guarantees, e.g., release-acquire synchronisation, observational refinement etc. We consider both in our TMS2-ra specification (see Fig. 4).

2.1 Release-acquire synchronisation

Prior to detailing the design choices of TMS2-ra, we recap the basics of release-acquire synchronisation in C11, including a recently developed timestamp-based operational semantics, which is the semantics assumed by TMS2-ra.

The fragment of C11 we focus on is the RC11-RAR fragment. The first “R” denotes the repairing model [Lahav et al. 2017], which precludes ‘thin-air’ behaviour by disallowing memory operations within a thread to be reordered. The “RAR” refers to the fact that the model includes release-acquire as well as relaxed atomics [Dalvandi et al. 2020b; Doherty et al. 2019].

For the remainder of this paper, we simply write C11 to refer to RC11-RAR.

We explain the main ideas behind release-acquire synchronisation using the message passing (MP) litmus test in Figs. 1a and 1b. It comprises two shared variables: $d$ (for data) and $f$ (for a flag), both of which are initially 0. Under SC, the postcondition of the program is $r_2 = 5$ because the loop in thread $\tau_2$ only terminates after $f$ has been updated to 1 in thread $\tau_1$, which in turn happens after $d$ is set to 5. Therefore, the only possible value of $d$ that thread $\tau_2$ can read is 5.

However, in Fig. 1a, all read/write accesses of $d$ and $f$ are relaxed, and hence the program can only establish the weaker postcondition $r_2 = 0 \lor r_2 = 5$ since it is possible for thread $\tau_2$ to read 0 for $d$ at line 4. In particular, reading 1 for $f$ does not guarantee that thread $\tau_2$ will read 5 for $d$.

2 Our development may be found in [Dalvandi and Dongol 2022].

3 Note that extending this model to include other types of C11 synchronisation (e.g., SC fences) and relaxations that allow intra-thread ordering is possible [Wright et al. 2021], but these extended models are not so interesting for the purposes of this paper, and the additional complexity that they induce detracts from our main contributions.
We illustrate the implications of these annotations via the examples in Fig. 2, where the highlighted code depicts the necessary changes.

**2.2 Transactional message passing**

We now describe the guarantees provided by our transactional model in the context of a client program. Like standard reads and writes in C11, we allow transactions to be combined with a synchronisation annotation, which may be one of relaxed (RX), releasing (R), acquiring (A), or release-acquiring (RA). These annotations dictate whether or not transactional (non-transactional) relaxed read of $f$ within a loop that terminates if $r_2$ reads 1 for $f$. After the loop terminates, $r_2$ performs a (non-transactional) relaxed read of $d$. In this example, like Fig. 1b, the release and acquire annotations induce a happens-before relation from $r_1$ to $r_2$ and hence ensure that the read of $d$ in $r_2$ does not return the stale value, 0.
Fig. 2b describes a program that uses a relaxed transaction. The postcondition of the program considers the case where the transaction in \( \tau_1 \) occurs before the transaction in \( \tau_2 \) since the antecedent assumes that \( r_1 = 1 \), i.e., the read of \( f \) at line 7 reads the write of \( f \) at line 4. In this example, both transactions are relaxed, and hence, the ordering of transactions above does not induce a happens before from \( \tau_1 \) to \( \tau_2 \). Thus, the read of \( d_1 \) at line 11 is not guaranteed to see the write of \( d_1 \) at line 1, i.e., the final value of \( r_3 \) is either 0 or 5. However, since the write and read of \( d_5 \) occurs within the transactions of \( \tau_1 \) and \( \tau_2 \), respectively, if \( r_1 = 1 \), then \( \tau_2 \) is guaranteed to read 10 for \( d_2 \).

Finally, Fig. 2c demonstrates a program with an RA transaction. The antecedent of the program’s postcondition implies that the transaction in \( \tau_3 \) occurs after the transaction in \( \tau_2 \), which in turn occurs after the transaction in \( \tau_1 \). Here, the transaction annotations ensure that the writes to \( d_1 \) and \( d_2 \) (at lines 1 and 5) performed by the client are seen by the client reads at lines 15 and 16. This is because the transaction in \( \tau_2 \) (annotated by RA) is guaranteed to synchronise with the transaction in \( \tau_1 \) (annotated by R), and similarly, the transaction in \( \tau_2 \) (annotated by A) is guaranteed to synchronise with the transaction in \( \tau_2 \) (annotated by RA). Note that if the transaction in \( \tau_2 \) was only releasing, then \( \tau_1 \) and \( \tau_2 \) would not synchronise, and the read at line 15 may return either 0 or 5. Yet, the read at line 16 would still be guaranteed to return 10 for \( d_2 \) since \( \tau_2 \) and \( \tau_3 \) synchronise. If the transaction in \( \tau_2 \) was only acquiring, then \( \tau_2 \) and \( \tau_3 \) would not synchronise. In this case, although \( \tau_1 \) and \( \tau_2 \) have synchronised, neither of the reads at lines 15 and 16 are guaranteed to return the new writes at lines 1 and 5.

Deciding a transaction’s synchronisation flag ultimately comes down to the needs of a client program, much like memory_order parameters on atomic_compare_exchange instructions in C11 [cppreference.com 2022]. Client programs that require message passing through transactions would use release-acquire, while others may only require relaxed annotations.

### 3 RELEASE-ACQUIRE TM SPECIFICATION

With the basic requirements for release-acquire and transactional synchronisation in place, we work towards a formal TM specification. Our specification will be closely tied to an operational semantics for C11 with timestamped writes and per-thread views [Dalvandi et al. 2020a; Dolan et al. 2018; Kaiser et al. 2017; Kang et al. 2017; Podkopaev et al. 2016] (see §3.1). We integrate this model with a TM specification in §3.3.

#### 3.1 View-based operational semantics

As discussed above, in our model, the C11 relaxed memory state is formalised by timestamped writes. Instead of mapping each location to a value, the state contains a set of writes \( \text{writes} \subseteq \text{Write} \), where \( \text{Write} = \text{Loc} \times \text{Val} \times \text{TS} \) represents a write to a location \( \text{Loc} \) with value \( \text{Val} \) and \( \text{TS} \triangleq \mathbb{Q} \) is the set of possible timestamps. If \( w \in \text{Write} \) and \( w = (x, v, \text{tst}) \), then we let \( \text{loc}(w) \triangleq x \), \( \text{val}(w) \triangleq v \), \( \text{tst}(w) \triangleq \text{tst} \), be the functions that extract the location, value and timestamp of \( w \), respectively.

A view is a mapping from a location to a write of that location, i.e., \( \text{View} \triangleq \text{Loc} \rightarrow \text{Write} \). To define the allowable reads by each thread to each location, the state also records a thread view for each thread define by a function

\[
\text{tview}: \text{TId} \rightarrow \text{View}
\]

where \( \text{TId} \triangleq \mathbb{N} \) is the set of thread identifiers. A thread may read from any write whose timestamp is no smaller than the thread’s current view. Thus, the observable values (OV), i.e., the set of values that thread \( \tau \) can read for location \( x \) is

\[
\text{OV}_\tau(x) \triangleq \{ w \in \text{writes} \mid \text{loc}(w) = x \land \text{tst}(w) \geq \text{tst}(\text{tview}_\tau(x)) \}
\]

\[
\text{OW}_\tau(x) \triangleq \{ \text{val}(w) \mid w \in \text{OV}_\tau(x) \}
\]
A write may be introduced at any timestamp greater than the thread’s current view (with a caveat that ensures atomicity of read-modify-writes, see [Dalvandi et al. 2020a; Doherty et al. 2019] for details).

Finally, to formalise release-acquire synchronisation, a state in the timestamp model also includes a notion of a modification view,

\[ mview : Write \rightarrow View \]

which is a function that records the thread view of the executing thread when a new write is introduced to \( \text{writes} \). In particular, if thread \( \tau \) introduces a new write \( w \) to \( \text{writes} \) and \( tview_\tau \) is updated to \( \text{view} \) in this new state, then \( mview \) is also updated so that \( mview_w = \text{view} \) in the new state. This information is used to update thread views in case release-acquire synchronisation occurs.

Formally, when threads synchronise, a new view is calculated using \( \otimes \), which is defined as follows. Given \( V_1, V_2 \in View \), we have

\[ V_1 \otimes V_2 \equiv \lambda x. \text{if} \ \text{tst}(V_2(x)) \leq \text{tst}(V_1(x)) \ \text{then} \ V_1(x) \ \text{else} \ V_2(x) \]

which constructs a new view by taking the write with the larger timestamp for each location \( x \).

**Example 1 (Synchronised MP).** Consider Fig. 3, which depicts a possible execution of the program in Fig. 1b. Each “\( v, i \)” represents a “value, timestamp” pair for the location in question. The initial state is \( \sigma_0 \), where the views of threads \( \tau_1 \) and \( \tau_2 \) are both the initial writes. State \( \sigma_1 \) occurs after executing line 1, where the view of \( \tau_1 \) is updated to the new write on \( d \). Similarly, \( \sigma_2 \) occurs after executing line 2. Note that the new write is tagged with a release annotation. Moreover, the operational semantics guarantees that in \( \sigma_2 \), we have \( \sigma_2.mview_{(f,1,1)}(d) = (d, 5, 1) \), i.e., the modification view of the write \( (f, 1, 1) \) returns \( (d, 5, 1) \) for \( d \) (since this was the thread view of \( \tau_1 \) for \( d \) when the write at line 2 occurred).

Finally, \( \sigma_3 \) depicts the state after execution of line 3, where the read returns the value 1 for \( f \). In this case, the thread view of \( \tau_2 \) for \( f \) is updated to the new read. More importantly, due to release-acquire annotations the semantics enforces that the thread view of \( \tau_2 \) for \( d \) in \( \sigma_3 \) is also updated to the new modification view, i.e., \( \sigma_2.mview_{(f,1,1)}(d) \). Thus, after state \( \sigma_3 \), \( \tau_2 \) will no longer be able to return the stale value 0 for \( d \).

The key difference in execution of the unsynchronised example (Fig. 1a) is that the read at line 3 does not update \( tview_{\tau_2}(d) \). Hence, for the state of Fig. 1a analogous to \( \sigma_3 \), the view of \( \tau_2 \) for \( d \) will remain at the initial write, allowing it to return a stale value.

### 3.2 TMS2

First, we consider the TMS2 specification, which is our TMS2-ra specification *without* any client-side release-acquire guarantees. This is given by the unhighlighted components of Fig. 4, which

---

**Fig. 3. Synchronised message passing views**

---
correspond precisely to the internal actions of TMS2 [Doherty et al. 2013].\footnote{TMS2-ra, like TMS2 is presented as an I/O automaton [Lynch 1996]. For simplicity, we eschew the external actions, but they can easily be included to formalise the TM interface.} Note that each action of Fig. 4 is atomic and guarded by the conditions defined in $\textbf{pre}$. If all the conditions in $\textbf{pre}$ hold the transition is enabled, and the corresponding action atomically updates the state according to the assignments and functions in $\textbf{eff}$. If some condition in $\textbf{pre}$ does not hold then the transition is blocked. We use $\land$ to denote a non-deterministic choice (see [Lynch 1996] for details).

TMS2 is a close operational approximation of opacity [Guerraoui and Kapalka 2010]. The differences between TMS2 and opacity are minor [Lesani et al. 2012], and much of the discussion below applies equally to opacity. TMS2 (and opacity) distinguishes between completed and live transactions, where completed transaction may either be committed or aborted. TMS2 guarantees the existence of a total order $\prec$ over all transactions such that:

1. if transaction $t_1$ executes $\text{TxEnd}$ before $t_2$ executes $\text{TxBegin}$, then $t_1 \prec t_2$;
2. for any transaction $t$, if $\prec_t$ is the strict downclosure of $\prec$ w.r.t. $t$ and $m$ is the memory obtained by applying the committed transactions in $\prec_t$ in order, then
   - all internal reads in $t$ for a variable $x$ are consistent with the last write to $x$ in $t$, and
   - all external reads of $t$ are consistent with $m$.

Note that conditions (1) and (2) together imply strict serialisability of the transactions. Condition (2) additionally ensures that no transaction reads from an aborted or live transaction since all external writes can be explained by the prior writes of committed transactions only. Moreover, reads of all transactions (including aborted and live transactions) never return a spurious value, i.e., each non-aborting read can be explained by prior committed transactions.

The existence of the total order mentioned above is guaranteed by the TMS2 specification as follows. Each transaction $t$ comprises a local read set, $\text{rdSet}_t$, local write set, $\text{wrSet}_t$, and variable, $\text{status}_t$, that is used to model control flow within a transaction. If the status of $t$ is $\text{NOTSTARTED}$, $t$ may transition to status $\text{READY}$ if a thread $\tau$ executes $\text{TxBegin}_t$. Once ready, $\tau$ may execute some number of $\text{TxRead}$ and $\text{TxWrite}$ operations, or $\text{TxEnd}$, which sets the status of $t$ (the transaction that $\tau$ is executing) to $\text{COMMITTED}$. Note that if transaction $t$ is $\text{READY}$, it may transition to status $\text{ABORT}$ at any time. Moreover, in some circumstances, $t$ may be forced to abort because all other transitions of $t$ are blocked. For example, if $t$ is a writing transaction and $t$’s read set is not a subset of $\text{last}(M)$, then $t$ must abort.

To ensure read/write consistency, TMS2 uses a sequence of memories $M$, where a memory is a mapping from locations to values. A transaction $t$ records the earliest memory it can read from by setting $\text{beginIdx}_t$ to the last index of $M$ when $t$ executed $\text{TxBegin}_t$. Moreover, each committing writing transaction $t$ constructs a new memory $N = \text{last}(M) \oplus \text{wrSet}_t$, which is the memory $\text{last}(M)$ overwritten with the write set of $t$. It then appends $N$ to the end of $M$ (see $\text{TxEndWR}$).

We differentiate between internal reads $\text{TxReadInt}$ and external reads $\text{TxReadExt}$, by whether the read location $x$ is in the write set of the executing transaction, $t$. An internal read of $x$ simply returns the value of $x$ in the write set of $t$. An external read of $x$ non-deterministically picks a memory index $i$. This read is enabled iff $i$ is a valid index (i.e., is between $\text{beginIdx}_t$ and the last memory index, $|M| - 1$) and the read set of $t$ is consistent with $M_i$ (i.e., the memory at index $i$). In case an external read occurs, the read set is updated and the value read is returned. This means that all external reads in $t$ are validated with respect to some memory snapshot between $\text{beginIdx}_t$ and the maximum memory index. Note that it is possible for two different reads to validate w.r.t. different memory snapshots.

TMS2 prescribes a lazy write-back strategy via $\text{TxWrite}$, where writes are cached in a local write set until the commit occurs (as described above). However, as we shall see, this does not preclude
implementations that use \textit{eager} write-backs, where writes occur in memory at the time of writing (see \cite{Derrick2018}). In fact, the TML-RA algorithm, our main case study in this paper, is such an eager algorithm (see §4).

We split the commit phase into two cases: \textit{read-only} (modelled by TxEndRO) and \textit{writing} (modelled by TxEndWR). Since all reads are validated at the time of reading, a read-only transaction can simply commit the transaction. On the other hand, the writing transaction must ensure its reads are valid w.r.t. the last memory snapshot. The effect of this transition is to install a new memory snapshot as described above.

The final component of $t$ is a local set $\text{regs}_t$ that is used to keep track of the set of registers that the transaction has written to. A client provides the set of registers to be used by each transaction when the transaction begins. These registers are set to a special value $\bot$ when a transaction aborts to ensure that no value read by $t$ is seen outside $t$.

3.3 TMS2-RA

We now discuss the release-acquire extensions of TMS2-RA, as defined by the I/O automata algorithm in Fig. 4, including the highlighted components. The key extension of TMS2-RA is its ability to synchronise client threads, thus allowing it to cope with the examples in Fig. 2. Formally, this is achieved by ensuring TMS2-RA synchronises the \textit{thread view} of the client whenever transactional release-acquire synchronisation occurs.

We introduce two new local variables in transaction $t$. Namely, $\text{syncType}_t$, which records the type of synchronisation of $t$, and $\text{seenIdxs}_t$, which records the set of all memory indices seen by $t$ that are either releasing or release-acquiring. We also introduce a new thread local variable $\text{tview}_t$, which records the \textit{transaction thread view} of $t$. The transaction thread view is similar to \textit{thread view} introduced in §3.1. The difference here is in the definition of View. In this context the View is a function that maps the threads to memory indexes of $M$. The transaction view of $t$ is the smallest memory in $M$ that can be read by any transaction $t$ that was begun by thread $\tau$. We also introduce two global variables. Namely $S$, which is a sequence recording the type of each committed writing transaction that installs each new memory in $M$, and $V$ which is a sequence of modification views for each new memory in $M$. Thus, in TMS2-RA, memory $M_i$ has synchronisation type $S_i$, and modification view $V_i$.

The transactional operations of TMS2 are modified as follows. In $\text{TxBegin}_t$, we take as input the type of synchronisation transaction $t$ is to perform, and store this value in $\text{syncType}_t$. Another input to $\text{TxBegin}_t$ is $m$, an index to a visible memory $M$. We also initialise $\text{seenIdxs}_t$ to the empty set. In $\text{TxReadExt}_t(x, i)$, i.e., a transition for external read of $x$ from memory index $i$, we record the index $i$ in $\text{seenIdxs}_t$ if the memory $M_i$ is releasing or release-acquiring.

When a transaction ends (for both read-only and writing transactions), if the transaction is acquiring or release-acquiring and $\text{seenIdxs}_t$ is non-empty, we construct a new view $nv$ to be the maximum modification view for each transaction in $\text{seenIdxs}_t$ using the function View. We use this to synchronise the client thread’s view by updating $\text{tview}_t$ to $\text{tview}_t \otimes nv$. For a writing transaction, we record this new view of the client in $V$ so that any future transactions that synchronise with this new transaction does so with respect to this view. Finally, once a transaction ends, it updates $\text{tview}_t$ to the largest index in $\text{seenIdxs}_t$.

We demonstrate the interaction of TMS2-RA and a client program by considering the views of three possible executions of the programs in Fig. 5. Unlike the trace considered in Fig. 3, we only show the most critical transitions. The memory sequence $M$ of TMS2-RA is clear from the figures. We represent $S$ by the superscripts on each state of $M$, and the modification views $V$ by the dotted arrows $\cdots \text{→}$ from each state of $M$. 

Proc. ACM Program. Lang., Vol. 1, No. OOPSLA, Article 1. Publication date: December 2022.
Highlighted components are extensions necessary for client synchronisation for C11 transactions. We assume that the transactions are executed by thread \( \tau \). Moreover, let \( Q \cdot a \) be the sequence \( Q \) appended with element \( a \) and \( f \oplus g \) be the function \( f \) overridden by function \( g \). Finally, let \( \text{maxWr} \) be a function that returns the write with the largest timestamp in the given set of writes.

Fig. 5a represents part of an execution of the program in Fig. 2a. In the execution depicted, we assume that all of thread \( \tau_1 \) executes before \( \tau_2 \). Here, \( \sigma_2 \) is the state after executing line 4, where
When \( \tau_1 \) introduces a new write to \( d \) and then executed its (releasing) transaction, introducing a new memory snapshot whose modification view becomes the new write of \( d \) (since \( \tau_1 \)'s thread view is at this new write). Then, when \( \tau_2 \) executes its (acquiring) transaction that reads 1 from \( f \), it synchronises with the latest memory snapshot, causing \( \tau_2 \)'s thread view to be the new write of \( d \) as well. This is analogous, as required, to the way in which views are updated in C11 (see Fig. 3).

Fig. 5b represents a part execution of the program in Fig. 2b. Again, we assume a complete execution of thread \( \tau_1 \) followed by \( \tau_2 \). State \( \sigma_2 \) is the state after executing line 5, where \( \tau_1 \) has introduced a new write to \( d_1 \). Now consider the state \( \sigma_3 \) (the state after execution of line 10), where \( \tau_1 \) introduces a new memory snapshot in \( M \) with annotation RX and modification view pointing to the new write on \( d_1 \). When \( \tau_2 \) continues execution, its transaction must be ordered after the latest memory snapshot, but this will not induce a release-acquire synchronisation. This means that \( \tau_2 \)'s view of \( d_2 \) will not be updated. However, since \( \tau_2 \)'s transaction occurs after \( \tau_1 \)'s transaction, \( \tau_2 \) is guaranteed to read 10 for \( d_2 \). Note that the transaction executed by \( \tau_2 \) is a read-only relaxed transaction, the view of \( \tau_2 \) of the client variable (\( d_1 \)) is unchanged. However, \( \tau_2 \)'s view of the transactional memory (not shown in the diagrams) will be updated to the new memory state \( \{ f \mapsto 1, d_2 \mapsto 10 \} \).

Finally, Fig. 5c represents part of an execution of Fig. 2c comprising the complete execution of \( \tau_1, \tau_2 \) then \( \tau_3 \) in order. State \( \sigma_2 \) represents the state after executing line 4, where the modification view of the newly installed memory is consistent with the view of the executing thread \( \tau_1 \). Then, in \( \sigma_4 \) (the state after execution of line 10), we have a new write on \( d_2 \) with value 10 and a further new snapshot that synchronises with the snapshot \( \{ f \mapsto 1 \}^R \) causing the thread view of \( \tau_2 \) and the modification view of the new snapshot to be updated to the last writes of \( d_1 \) and \( d_2 \). Next, in \( \sigma_5 \), when \( \tau_3 \) executes its transaction, this transaction is guaranteed to synchronise with \( \{ f \mapsto 2 \}^{RA} \)
causing r3’s view to be updated to the latest writes of d1 and d2, which is inherited from the modification view of \{ f \mapsto 2 \}^{RA}.

### 3.4 Modular operational semantics

To reason about clients that use abstract TMS2-RA transactions in a modular fashion, we use configurations that are triples \((lst, y, \beta)\), where \(lst : Reg \rightarrow Val\) denotes the local register state, \(y\) is the TMS2-RA state (which includes all transactional variables described in Fig. 4) and \(\beta\) is the C11 state of the client (see [Dalvandi et al. 2020a, 2022], §A).

The transition relation for transactional operations is given in Fig. 6. These follow the automata-style description given in Fig. 4, but make state components that are affect more precise. The most

\begin{align}
\text{TxBEGIN}(sflag, m, regSet) & \quad y.\text{status}_t = \text{NOTSTARTED} \quad y.\text{txn}_t = \bot \quad m \in \text{vmems}_t \\
\text{lst}, y, \beta \rightarrow_t \text{lst}, y \quad \begin{cases}
\text{beginIdx}_t := m, \text{seenIdxs}_t := \emptyset, \text{rdSet}_t := \emptyset, \\
\text{wrSet}_t := \emptyset, \text{syncType}_t := sflag, \text{regs}_t := \text{regSet}_t.
\end{cases} \\
\text{status}_t = \text{READY}, y.\text{txn}_t := t
\end{align}

\begin{align}
\text{TxWRITE}(l, v) & \quad y.\text{status}_t = \text{READY} \quad y.\text{txn}_t = t \\
\text{lst}, y, \beta \rightarrow_t \text{lst}, y \quad \text{wrSet}_t := y.\text{wrSet}_t \cup \{ l \mapsto v \}, \beta
\end{align}

\begin{align}
\text{TxREAD}(l, r) & \quad y.\text{status}_t = \text{READY} \quad y.\text{txn}_t = t \quad y.\text{wrSet}_t = \emptyset \\
\text{lst}, y, \beta \rightarrow_t \text{lst}[r := a], y \quad \begin{cases}
\text{rdSet}' := \emptyset \quad \text{tvview}' := \text{tvview} \\
\text{tvview}' := \text{tvview} \circ \text{view}(y.\text{seenIdxs}_t, y.\text{v}) \quad \text{else} \quad \beta.\text{tvview}
\end{cases}
\end{align}

\begin{align}
\text{TxENDRO} & \quad y.\text{status}_t = \text{READY} \quad y.\text{txn}_t = t \quad y.\text{wrSet}_t \neq \emptyset \\
\text{lst}, y, \beta \rightarrow_t \text{lst}[\text{tvview} := \text{max}(y.\text{seenIdxs}_t)], \beta[\text{tvview} := \text{tvview}]
\end{align}

\begin{align}
\text{TxENDWR} & \quad y.\text{status}_t = \text{READY} \quad y.\text{txn}_t = t \\
\text{lst}, y, \beta \rightarrow_t \text{lst}[y.\text{status}_t := \text{COMMITTED}, y.\text{M}_t := \text{mem}', y.\text{S}_t := y.\text{syncType}_t, y.\text{V}_t := \text{tvview'}] \\
\text{tvview} := \text{tvview} \circ \text{view}(y.\text{seenIdxs}_t, y.\text{v}) \quad \text{else} \quad \beta.\text{tvview}
\end{align}

\begin{align}
\text{TxABORT} & \quad y.\text{status}_t = \text{READY} \quad y.\text{txn}_t = t \\
\text{lst}, y, \beta \rightarrow_t \text{lst}[\text{status}_t := \text{ABORTED}], \beta
\end{align}

Fig. 6. Operational semantics for TMS2-RA
interesting aspect of these rules is the interaction between a releasing writing transaction and subsequent committing reading transaction.

Note that each releasing writing transaction sets \( S_i \) (where \( i \) is last index in \( M \) at the time of writing) to either \( R \) or \( RA \). Additionally, the view of the thread at the time of writing is recorded in \( V_i \). A later transaction with an acquiring annotation calculates a new view using the function \( \text{view} \) as defined in Fig. 4 and updates, among other components, the executing thread’s view in \( \beta \). This means that, as expected, if there is a release-acquire synchronisation through a transactional memory library, then the client’s view will be updated to match the synchronisation that occurs.

4 A C11 STM IMPLEMENTATION

In this section, we develop a release-acquire version of a transactional mutex lock, that we call TML-ra, based on an SC implementation by Dalessandro et al. [Dalessandro et al. 2010]. Our algorithm is provided in Fig. 7, where the highlights indicate the fragments of code that we have introduced or modified. The grey highlights represent code additional to Dalessandro et al.’s original implementation, and the blue highlights represent the necessary release-acquire synchronisation.

We first discuss the core features of TML (§4.1), then discuss the extensions introduced in TML-ra to optimise for C11 release-acquire synchronisation (§4.2). We present the benchmarking results for both algorithms in §4.3. In §6, we present a proof that TML-ra implements TMS2-ra, i.e., any observation a client program makes when it uses TML-ra is a possible observation when it uses TMS2-ra.

4.1 TML

TML is synchronised using a single global counter \( glb \), initialised to 0, where \( glb \) is even iff no writing transaction is currently executing.

A transaction begins by taking a snapshot of \( glb \) in local variable \( loc \) and only begins if the value read is even.

Fig. 7. TML-ra: A release-acquire transactional mutex lock. For simplicity, the thread id is omitted
A write operation checks that loc is even and if so, it attempts to increment glb using the \texttt{CAS} at line W2. If this \texttt{CAS} succeeds, it increments loc (line W5), then immediately updates the location x (line W6). If the \texttt{CAS} fails, the transaction aborts. Note that if loc is odd then the current transaction “owns” the lock, meaning that lines W2-W5 can be bypassed.

A read operation (ignoring lines R3-R7 for now) reads the given location into the given register r (line R2). At lines R9 and R10 it checks that glb is consistent with loc. If so, the read succeeds, otherwise, the transaction aborts.

A transaction ends by checking whether the current transaction is a writing transaction. This can be determined by checking whether loc is odd since a writing transaction must have incremented glb via the \texttt{CAS} at line W2 and loc via the write at line W5 making both their values odd. Therefore, a writing transaction must increment glb to make it even again.

### 4.2 TML-ra

We now describe the necessary modifications to TML and the synchronisation induced by TMS2-ra. We assume that transactions in TML-ra are all release-acquiring and hence we omit the transaction annotation in \texttt{TxBegin}.

We assume all accesses to shared variables are either relaxed (e.g., the read at line R9), releasing (e.g., the write at line E2), acquiring (e.g., the read at line B2) or release-acquiring (e.g., the \texttt{CAS} at line R4). Additionally, we introduce a new local variable hasRead, initially set to false and a code path R3-R7, which is followed if a transaction performs a read without having previously performed a read or a write. We explain the purpose of this code path in more detail below.

\textit{Transaction synchronisation.} Recall that TMS2-ra requires that transactions are consistent w.r.t. a single memory snapshot and that external reads of a transaction synchronise with some memory snapshot. This may not occur in a relaxed memory context without adequate synchronisation. In particular, a writing transaction must perform a releasing write to glb at line E2 so that if a later transaction reads from this write, it synchronises with all of the writes performed by the writing transaction. To ensure this, we require the read of glb at line B3 as well as the \texttt{CAS} operations at lines W2 and R4 to be acquiring. Note that this also guarantees release-acquire client synchronisation.

The second key synchronisation is between W6 performed by a writing transaction \texttt{t_w} and R2 performed by a (different) reading transaction \texttt{t_r}. Suppose that both \texttt{t_w} and \texttt{t_r} are live. If \texttt{t_r} happens to read the write written at W6, it must now abort because \texttt{t_r}'s snapshot of glb will be inconsistent with the latest value of glb installed by \texttt{t_w}. The release-acquire synchronisation between W6 and R1 ensures that this will happen, i.e., \texttt{t_r} will see the new glb written by \texttt{t_w}, causing the test at R10 to fail and \texttt{t_r} to abort.

\textit{Causal linearizability.} The design of TML-ra ensures that all transactions, including read-only transactions are causally linearizable [Doherty et al. 2018], which is a condition that additionally guarantees compositionality (or locality [Herlihy and Wing 1990; Sela et al. 2021]) of concurrent objects. This notion of compositionality is that of Herlihy and Wing [Herlihy and Wing 1990]. In particular, under SC memory, given a history comprising several concurrent objects, if the history restricted to each object is linearizable, then the history as a whole is linearizable. In a relaxed memory setting, Doherty et al [Doherty et al. 2018] have shown that linearizability alone is insufficient to guarantee compositionality, and it is necessary to induce a “happens-before” relation when a specification induces a particular linearization.

The happens-before required by causal linearizability is naturally achieved for writing transactions via the \texttt{CAS} at line W2. For a read-only transaction, we introduce the \texttt{CAS} at line R4, which installs a new write to glb without changing its value. All transactions that follow the \texttt{CAS} at line R4 will be causally ordered after the reading transaction. Such a \texttt{CAS} must only be performed once,
thus we introduce a local variable hasRead, which is set to true if the CAS succeeds so that later reads from the same transaction can avoid the code path from R3-R7.

Note that the conditions necessary to guarantee causal linearizability (and hence compositionality) could have been introduced at the level of TMS2-ra. However, there are questions about whether the notion of compositionality introduced by Herlihy and Wing [Herlihy and Wing 1990] are appropriate in a relaxed memory context [Raad et al. 2019a]. Therefore we leave out the causal linearizability conditions in TMS2-ra to avoid over-constraining the specification.

4.3 Benchmarking

We implemented two versions of the TML algorithm: TML-ra (see Fig. 7) and TML-sc (the SC counterpart [Dalessandro et al. 2010]) and benchmarked both using the STAMP benchmarking suite [Minh et al. 2008]. Each experiment was repeated 20 times to rule out external loads on the test machine and an average of these times was taken. The results of the six benchmarks that we ran with STAMP are presented in Fig. 8. TML-ra is equivalent to or outperforms TML-sc in almost all cases, with a maximum improvement of 20%. On average, TML-ra performs 8.2% better than TML-sc.

Unsurprisingly, since TML optimises read-heavy workloads, its performance degrades under high write contention, and this is consistent with prior results [Dalessandro et al. 2010]. However, it is interesting that the degradation of TML-ra is not as severe as TML-sc for the Intruder and SSCA2 benchmarks.

TML-ra theoretically allows more parallelism than TML-sc since a read-only transaction $t_r$ is not forced to abort if a writing transaction $t_w$ executes after $t_r$’s first read operation - $t_r$ must only aborts if it sees $t_w$’s glb update, or one of $t_w$’s writes. Both Intruder and SSCA2 have a large number of short transactions; SSCA2 additionally has small read/write sets [Minh et al. 2008]. Here, TML-ra may be able to exploit the theoretical parallelism. In the single-threaded case, TML-ra executes far fewer heavyweight CASs.

As with prior results, we see that for the read-heavy benchmark Genome, the performance of both TML-ra and TML-sc improves as the number of threads increases.

5 TARO: A LOGIC FOR RELEASE-ACQUIRE TM

The development of view-based operational semantics for various fragments of C11 [Dalvandi et al. 2020a; Kaiser et al. 2017; Kang et al. 2017] has provided foundations for several logics for reasoning about C11 programs. These include separation logics [Kaiser et al. 2017; Svendsen et al. 2018]...
and extensions to Owicki-Gries reasoning [Dalvandi et al. 2020a, 2022; Lahav and Vafeiadis 2015; Wright et al. 2021]. Our point of departure is the Owicki-Gries encoding for RC11 RAR [Dalvandi et al. 2020a], which is the fragment of C11 that we focus on in this paper.5

A key benefit of the logic in [Dalvandi et al. 2020a] is that it enables reuse of standard Owicki-Gries proof decomposition rules and straightforward mechanisation in Isabelle/HOL [Dalvandi et al. 2020b, 2022]. As we shall see, we maintain these benefits in the context of C11 with release-acquire transactions. Our reasoning framework, called TARO, like Dalvandi et al [Dalvandi et al. 2020a; Dalvandi and Dongol 2021] uses view-based assertions to abstractly describe the system state, allowing reasoning about the current view of a thread, and view transfer from one thread to another through release-acquire synchronisation. TARO introduces additional assertions to enable reasoning about transactional views.

5.1 View-based assertions

In this section, we discuss the assertions and proof rules of TARO abstractly. The proof rules can be used to reason syntactically about a program without having to understand the low-level operational semantics of the C11 model. Our operational semantics is an extension of prior works [Dalvandi et al. 2020a; Kaiser et al. 2017; Kang et al. 2017] that include an encoding of standard Owicki-Gries semantics of the C11 model. Our operational semantics is an extension of prior works [Dalvandi et al. 2020a; Kaiser et al. 2017; Kang et al. 2017] that include an encoding of

To motivate TARO, consider the proof outline in Fig. 9 for the transactional message passing program from Fig. 2a. We use ‘•’ to distinguish transactional locations in a proof. For the program in Fig. 9, we have a transactional location $\hat{f}$.

5.1.1 View assertions. The proof outline contains three assertions from [Dalvandi et al. 2020a] describing the views that each thread may have of the system state. Recall (§3.1), that we can define the set of values that a thread can see in each state using the function $OV$.

- A definite value assertion, denoted $[x = v]_\tau$, holds iff thread $\tau$ sees the last write to location $x$ and this write has value $v$. Thus, $[x = v]_\tau \Rightarrow OV_\tau(x) = \{v\}$.

5These frameworks are based on models that assume top-level parallelism only. Therefore, our framework similarly re assumes top-level parallelism. This model can be extended to support dynamic parallelism, but such extensions are uninteresting for the purposes of this paper.
The assertion language presented here is heavily inspired by the view-based assertion language presented in [Dalvandi et al. 2020a]. Consider the third state, i.e., \( \sigma_2 \) in Fig. 3. There, we have \([d = 5]_{\tau_1} \land [f = 1]_{\tau_1}\) as well as \([f \approx 0]_{\tau_2} \land [f \approx 1]_{\tau_2}\). Moreover, we have \( \langle f = 1 \rangle [d = 5]_{\tau_2} \).

We ask the interested reader to consult [Dalvandi et al. 2020a, 2022] for further details of these assertions.

### 5.1.2 Transactional assertions

As alluded to above, TARO introduces several new assertions to describe the transactional state. These assertions are, in general, local to the transaction being executed, and hence, stable under the execution of other threads. Fig. 9 contains the following transaction local assertions:

- **Rel.**, which holds iff \( \tau \) is executing a releasing or release-acquiring transaction.
- **Acq.**, which holds iff \( \tau \) is executing an acquiring or release-acquiring transaction.
- \((\hat{x}, v) \in WS_\tau \) (and \((\hat{x}, v) \in RS_\tau\)), which holds iff \( \tau \) is executing a transaction whose write set (resp. read set) contains a write to (resp. read of) \( \hat{x} \) with value \( v \).
- \([x \lessapprox v]_\tau\), which holds iff \( \tau \) is executing a transaction such that committing this transaction results in the definite value assertion \([x = v]_\tau\) (see above).

In addition, we include a number of assertions. This section provides the formal definition for the assertion language used in the verification of client programs that use TMS2-RA (See §5.1). The assertion language presented here is heavily inspired by the view-based assertion language presented in [Dalvandi et al. 2020a].

A memory \( i \) is visible to a transaction executed by a thread \( \tau \) iff \( i \) is greater than the transaction thread view of \( \tau \) (\( \text{txview}_\tau \)) and is less than the maximum index of the memory \(|M| - 1\). We define the set of visible memories \( OM_\tau \) to be:

\[
OM_\tau = \{ n \mid n \geq \text{txview}_\tau \land n \leq |M| - 1 \}
\]

- **A transactional definite observation assertion**, denoted \([\hat{x} = v]_\tau\), holds iff for all memory versions \( i \), where \( i \) is greater than or equal to \( \text{beginIdx}_\tau \), the value of \( M_i(x) \) is \( v \). Formally, for a transactional state \( \gamma \):

\[
[\hat{x} = v]_\tau(\gamma) \equiv \forall i \in \gamma.OM_\tau, \gamma.M_i(\hat{x}) = v
\]

These are lifted to client-object states \((\gamma, \beta)\) in the normal manner, e.g., \([\hat{x} = v]_\tau(\gamma, \beta) = [\hat{x} = v]_\tau(\gamma)\)

- **A transactional possible observation assertion**, denoted \([\hat{x} \approx v]_\tau\), holds iff there exists a memory version \( i \) that has value \( v \) for \( \hat{x} \). Formally:

\[
[\hat{x} \approx v]_\tau(\gamma) \equiv \exists i \in \gamma.OM_\tau, \gamma.M_i(\hat{x}) = v
\]

- **A transactional conditional observation assertion**, denoted \( \langle \hat{y} = u \rangle [x = v]_\tau \), holds iff an acquiring transactional read of \( y \) by \( \tau \) that returns a value \( u \) is guaranteed to induce a release-acquire synchronisation so that \([x \lessapprox v]_\tau \) holds in the client state after the reading transaction successfully commits. Formally:

\[
\langle \hat{y} = u \rangle [x = v]_\tau(\gamma, \beta) \equiv \forall i \in \gamma.OM_\tau, \gamma.M_i(\hat{y}) = u \Rightarrow \gamma.V_i(x) = \beta.last(x) \land \text{val}(\beta.last(x)) = v \land \gamma.S_i
\]
where \( \text{last}(x) \) is the last write to \( x \) in the modification order. It is important to note that this assertion is over two states: transaction state \( \gamma \) and client state \( \beta \), explaining transfer of information across two threads using the transactional memory. In particular, the transactional view \( V_i \) for the memory index \( i \) must see the last write to \( x \) in the client state \( \beta \). This means that the thread that committed the transaction writing the value \( u \) to \( \hat{y} \) did so when it saw the last write to \( x \).

### Example 3.

Returning to our transactional MP example (Fig. 9), the precondition of line 1 contains assertions \( \neg \{ \hat{f} \approx 1 \}_{r_2} \) and \( [d = 0]_{r_1} \), which ensure that, prior to executing line 1, thread \( r_2 \) cannot see the value 1 for \( \hat{f} \) and thread \( r_1 \) must see the value 0 for \( d \), respectively. In the postcondition of line 2, \( [d = 0]_{r_1} \) changes to \( [d = 5]_{r_1} \) since \( r_1 \) performs a write to \( d \) with value 5. The other view-based assertions in \( r_1 \) are similar. We explain the transactional assertions involving \( \text{Rel} \) and \( \text{WS} \) below.

Now consider the assertions in thread \( r_2 \). The precondition of line 6 (which is also the precondition of line 5) contains a conditional value assertion \( \langle \hat{f} = 1 \rangle [d = 5]_{r_2} \). This assertion ensures that, if \( r_2 \) reads the value 1 for \( \hat{f} \) via an acquiring (or release-acquiring) transaction, and this transaction successfully commits, then its view is guaranteed to be updated so that \( [d = 5]_{r_2} \) holds. In a transactional setting, we establish this fact in three steps.

1. After executing line 7, we use \( \langle \hat{f} = 1 \rangle [d = 5]_{r_2} \) to establish that \( r_1 = 1 \Rightarrow [d \approx 5]_{r_2} \) holds. Note that \( r_2 \) stores the value 1 returned by a transactional read of \( \hat{f} \). Thus, \( \langle \hat{f} = 1 \rangle [d = 5]_{r_2} \) is transformed into an implication after the execution of line 7. The assertion \( [d \approx 5]_{r_2} \) is a new assertion introduced in TARO, which states that if the transaction executed by \( r_2 \) commits, then \( [d = 5]_{r_2} \) holds in the post-state.

2. If the transaction successfully commits (line 8), we use \( r_1 = 1 \Rightarrow [d \approx 5]_{r_2} \) to establish \( r_1 = 1 \Rightarrow [d = 5]_{r_2} \) in the postcondition. Recall that all registers used by a transaction are set to \( \bot \) when a transaction aborts, so if \( r_2 \) reaches line 9 by aborting the transaction, then this assertion is trivially true.

3. We use \( r_1 = 1 \Rightarrow [d = 5]_{r_2} \) to establish \( [d = 5]_{r_2} \) after the do-until loop, using the guard \( r_1 = 1 \) at line 9.

Finally, we use \( [d = 5]_{r_2} \) in the precondition of line 10 to establish the postcondition \( r_2 = 5 \). This is because \( [d = 5]_{r_2} \) guarantees that the only value \( r_2 \) can read for \( d \) is 5.

### 5.2 TARO: Transactional Owicki-Gries Reasoning

Now that we have introduced the assertions used by TARO, we now review the Owicki-Gries proof obligations. As discussed above, the use of view-based assertions allows us to use the standard Owicki-Gries theory. Regardless, we review the theory in the context of our language, which supports (abstract) TM operations. Formally, we model programs as a labelled transition system, given by the syntax in Fig. 10.

A command (of type \( \text{ACom} \)) is either a local assignment \( r := \text{Exp} \), a store to a shared location \( x := [R] \text{Exp} \), a load from a shared location \( r \leftarrow [A] x \), a compare-and-swap \( r \leftarrow \text{CAS}^{[R][R][A]}(x, u, v) \), or a transactional operation. The annotations \( RX, R \) and \( A \) are optional, as indicated by the brackets ‘[’ and ‘]’. Thus, for example, both \( x := e \) and \( x :=^{B} e \) are valid load commands; the former is relaxed and the latter is releasing. A \( \text{CAS} \) may be annotated to be relaxed, or release and/or acquire. Note that a \( \text{CAS} \) returns a boolean to indicate whether or not the compare-and-swap has been successful. \( \text{TxBegin}(\text{RX}[R][A]) \), \( \text{TxRead}(x, r) \), \( \text{TxWrite}(x, v) \) and \( \text{TxEnd} \) are transactional operations, as defined by the TMS2-RA automata in Fig. 4.
We use a program counter variable \( pc : TId \to Label \) to model control flow, and model a program \( \Pi \) as a function mapping each pair \((\tau, i)\) of thread identifier and label to the \emph{labelled statement} (in \( LCom \)) to be executed. A labelled statement may be (i) a plain statement of the form \( \alpha \xrightarrow{\text{goto}} j \), comprising an atomic statement \( \alpha \) to be executed and the label \( j \) of the next statement; or (ii) a conditional statement of the form \( \text{if } B \xrightarrow{\text{goto}} j \text{ else } \xrightarrow{\text{go}} k \) to accommodate branching, which proceeds to label \( j \) if \( B \) holds and to \( k \), otherwise. We assume a designated label, \( i \in Label \), representing the \emph{initial label}; i.e., each thread begins execution with \( pc(\tau) = i \). Similarly, \( \zeta \in Label \) represents the \emph{final label}.

We let \emph{Assertion} be the set of \emph{assertions} that use view-based expressions. We model program annotations via an \emph{annotation function}, \( \text{ann} \in \text{Ann} = TId \times Label \to \text{Assertion} \), associating each program point \((\tau, i)\) with its associated assertion. A \emph{proof outline} is a tuple \((in, \text{ann}, \text{fin})\), where \( in, \text{fin} \in \text{Assertion} \) are the initial and final assertions.

\begin{definition}[Validity] A proof outline \((in, \text{ann}, \text{fin})\) is \emph{valid} for a program \( \Pi \) iff each of the following holds:

\begin{align*}
\text{Initialisation} & : \forall \tau \in TId, in \Rightarrow \text{ann}(\tau, i). \\
\text{Finalisation} & : \forall \tau \in TId. \text{ann}(\tau, \zeta) \Rightarrow \text{fin} \\
\text{Local correctness} & : \forall \tau \in TId \text{ and } i \in Label, \text{ either:} \\
& \bullet \Pi(\tau, i) = \alpha \xrightarrow{\text{goto}} j \text{ and } \{\text{ann}(\tau, i)\} \alpha \{\text{ann}(\tau, j)\}; \text{ or} \\
& \bullet \Pi(\tau, i) = \text{if } B \xrightarrow{\text{goto}} j \xrightarrow{\text{else } k} \text{ and both } \text{ann}(\tau, i) \land B \Rightarrow \text{ann}(\tau, j) \land \text{ann}(\tau, i) \land \lnot B \Rightarrow \text{ann}(\tau, k) \text{ hold.}
\end{align*}

\text{Stability} : \forall \tau_1, \tau_2 \in TId \text{ such that } \tau_1 \neq \tau_2 \text{ and } i_1, i_2 \in Label \text{ if } \Pi(\tau_1, i_1) = \alpha \xrightarrow{\text{goto}} j, \text{ then } \{\text{ann}(\tau_2, i_2) \land \text{ann}(\tau_1, i_1)\} \alpha \{\text{ann}(\tau_2, i_2)\}
\end{definition}

Intuitively, \emph{Initialisation} (resp. \emph{Finalisation}) ensures that the initial (resp. final) assertion of each thread holds at the beginning (resp. end); \emph{Local correctness} establishes validity for each thread; and \emph{Stability} ensures that each (local) thread annotation is \emph{interference-free} under the execution of other threads [Owicki and Gries 1976].

To support Owicki-Gries reasoning, we have proved a number of high-level rules, extending those of Dalvandi et al. [Dalvandi et al. 2020a; Dalvandi and Dongol 2021] to cope with transactional assertions from §5.1 and the transactional commands. For instance, the following rules are used in the proof of transactional message passing. A number of other rules are provided as part of our Isabelle/HOL development.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{language_syntax.png}
\caption{Language syntax}
\end{figure}
Lemma 1. Suppose $r_1 \neq r_2$. Then each of the following holds:

\[
\begin{align*}
\{true\} & \ \text{TWrite}(x, v) \ \{\langle x, v \rangle \in \text{WS}_r\} \\
\{(x, u) \in \text{WS}_{r_1} \land \text{Rel}_{r_1} \land \langle \hat{x} \neq u \rangle_{r_2} \land \langle y = v \rangle_{r_1}\} & \ \text{TEnd}_{r_2} \ \{\langle \hat{x} = u \rangle [y = v]_{r_2}\} \\
\{(x, \_) \notin \text{WS}_r \land \text{Acq}_r \land \langle \hat{x} = u \rangle [y = v]_r\} & \ \text{TRead}_r(x, r) \ \{\langle \hat{x}, r \rangle \in \text{RS}_r \land (r = u \Rightarrow [y \hat{=} v]_r\} \\
\{\langle \hat{x}, r \rangle \in \text{RS}_r \land (r = u \Rightarrow [y \hat{=} v]_r\} & \ \text{TEnd}_r \ \{r = u \Rightarrow [y = m]_r\}
\end{align*}
\]

The rules in Lemma 1 have been verified in Isabelle/HOL w.r.t. the operational semantics. Once proved, they can be used to show validity of proof outlines such as those in Fig. 9 without having to consult the operational semantics.

Theorem 1. The proof outline in Fig. 9 is valid.

This theorem has been verified in Isabelle/HOL, and it makes extensive use of generic proof rules such as the ones proved in Lemma 1. In particular, given such lemmas, like in previous works [Bila et al. 2022; Dalvandi et al. 2020a; Dalvandi and Dongol 2021; Dalvandi et al. 2022], Isabelle/HOL is automatically able to find and apply the appropriate proof rule using the built-in sledgehammer tool [Böhme and Nipkow 2010]. This automation has been key to scaling mechanised verification of proof outlines in view-based logics. For example, the proofs of TML-RA (see §6) requires verification of complex invariants and proof outlines, and these proofs make use of the proof rules developed in prior work [Dalvandi et al. 2020a]. Similarly, TARO can be applied to verify more complex programs that use transactions, for instance if one were to develop transactional data structures. Interestingly, because transactions provide isolation guarantees, many of the proofs are simplified since the stability checks for in-flight transactions become trivial.

The proof outlines for the programs in Figs. 2b and 2c are provided in Appendix E.

6 PROVING CORRECTNESS OF TML-RA

We now turn to the question of correctness of TML-RA with respect to the TMS2-RA specification.

6.1 Refinement and Simulation for Weak Memory

Since we have an operational semantics with an interleaving semantics over weak memory states, the development of our refinement theory closely follows the standard approach under SC [de Roever and Engelhardt 1998]. Suppose $P$ is a program with initialisation $\text{Init}$. An execution of $P$ is defined by a possibly infinite sequence $\Delta_0 \Delta_1 \Delta_2 \ldots$ such that

1. each $\Delta_i$ is a 4-tuple $(P_i, lS_i, y_i, \beta_i)$ comprising a program to be executed, local state, global library state and global client state, and
2. $(P_0, lS_0, y_0, \beta_0) = (P, lS_{\text{Init}}, y_{\text{Init}}, \beta_{\text{Init}})$, and
3. for each $i$, we have $\Delta_i \implies \Delta_{i+1}$, where $\implies$ is the transition relation of the program (as defined by the operational semantics).

Let $LVar_p$ be the set of local variables corresponding to a program $P$. If $P$ is a client, a client trace corresponding to an execution $\Delta_0 \Delta_1 \Delta_2 \ldots$ is a sequence $ct \in \Sigma_p$ such that $ct_i = (\pi_2(\Delta_i) \vert P, \pi_4(\Delta_i))$, where $\pi_n$ is a projection function that extracts the $n$th component of a given tuple and $lS_{\vert P}$ restricts the given local state $lS$ to the variables in $LVar_p$. Thus, each $ct_i$ is the global client state component of $\Delta_i$. After such a projection, the concrete implementation may contain (finite or infinite) stuttering [de Roever and Engelhardt 1998], i.e., consecutive states in which the client state is unchanged. We let $\text{rem}_\text{stut}(ct)$ be the function that removes all stuttering from the trace $ct$, i.e., each consecutively repeating state is replaced by a single instance of that state. We let $\text{Tr}_SF(P)$
denote the set of **stutter-free traces** of a program $P$, i.e., the **stutter-free traces** generated from the set of all executions of $P$.

Below we refer to the client that uses the abstract object as the **abstract client** and the client that uses the object’s implementation as the **concrete client**. The notion of contextual refinement that we develop ensures that a client is not able to distinguish the use of a concrete implementation in place of an abstract specification. In other words, each thread of the concrete client should only be able to observe the writes (and updates) in the client state (i.e., $\gamma$ component) that the thread could already observe in a corresponding of the client state of the abstract client. First we define trace refinement for weak memory states.

**Definition 2** (State and Trace Refinement). We say a concrete client state $(ls, \beta_C)$ is a **refinement** of an abstract client state $(als, \beta_A)$, denoted $(ls, \beta_C) \leq (als, \beta_A)$ iff $ls = als$ and for all threads $\tau$ and $x \in \mathit{GVar}$, we have $\beta_C.OW_\tau(x) \subseteq \beta_A.OW_\tau(x)$. We say a concrete client trace $ct$ is a **refinement** of an abstract client trace $at$, denoted $ct \leq at$, iff $ct_i \leq at_i$ for all $i$.

This now leads to a natural trace-based definition of contextual refinement.

**Definition 3** (Program Refinement). A concrete program $P_C$ is a **refinement** of an abstract program $P_A$, denoted $P_C \leq P_A$, iff for any (stutter-free) client trace $ct \in \mathit{Tr}_{SF}(P_C)$ there exists a (stutter-free) client trace $at \in \mathit{Tr}_{SF}(P_A)$ such that $ct \leq at$.

Finally, we obtain a notion of contextual refinement for abstract objects. We let $P[O]$ be the client program calling operations from object $O$. Note that $O$ may be an abstract object, in which case execution of each method call follows the abstract object semantics, or a concrete implementation.

**Definition 4** (Contextual refinement). We say a concrete object $CO$ is a **contextual refinement** of an abstract object $AO$ iff for any client program $P$, we have $P[CO] \leq P[AO]$.

Here, we use a **simulation-based** proof method, which is a standard technique from the literature that establishes refinement between TMS2-RA and TML-RA. The difference in a relaxed memory setting is that the refinement relation is between more complex configurations of the form $(ls, \gamma, \beta)$, where $ls$ describes the local state, $\gamma$ is the client state and $\beta$ is a state of the TM in question. In particular, a **simulation relation**, $R$, relates triples $\Gamma_A \doteq (als, \beta_A)$ of the abstract system with triples $\Gamma_C \doteq (ls, \gamma_C, \beta_C)$ of the concrete system.

The definition below assumes a reflexive relation $\gamma_C \mathrel{\mathit{tview}_\tau} \gamma'_C$ for each thread $\tau$ that arbitrarily advances the thread view of $\tau$ (for one or more locations).

**Definition 5** (Forward simulation). For an abstract object $AO$ and a concrete object $CO$, for a client program $P$, we say $R(\Gamma_A, \Gamma_C) \doteq R_V((als, \beta_A), (ls, \beta_C)) \land R_O((als_{AO}, \gamma_A), (ls_{CO}, \gamma'_C))$ is a forward simulation between $A$ and $C$ iff each of the following holds:

**Client observation.**

$$R_V((als, \beta_A), (ls, \beta_C)) = als_{IP} = ls_{IP} \quad (\forall \tau \in \mathit{TId}, x \in \mathit{Loc}. \ \beta_A.\mathit{tview}(t, x) \leq \beta_C.\mathit{tview}(t, x))$$

**Thread view stability.** For any thread $\tau$,

$$R_O((als_{AO}, \gamma_A), (ls_{CO}, \gamma'_C)) \Rightarrow R_O((als_{AO}, \gamma_A), (ls_{CO}, \gamma'_C))$$

**Initialisation.** For any concrete initial state $\Gamma^0_C$, there exists an abstract initial state $\Gamma^0_A$ such that $R(\Gamma^0_A, \Gamma^0_C)$.

**Preservation.** For any concrete states $\Gamma_C, \Gamma'_C$, such that $C$ can take an atomic transition from $\Gamma_C$ to $\Gamma'_C$, if $\Gamma_A$ is an abstract state such that $R(\Gamma_A, \Gamma_C)$, then either

- $R(\Gamma_A, \Gamma'_C)$, or (stuttering step)
- there exists a transition of $A$ from $\Gamma_A$ to some state $\Gamma'_A$ such that $R(\Gamma'_A, \Gamma'_C)$. (non-stuttering step)
Initialisation and preservation are standard components of a forward simulation. Client observation is necessary in a relaxed memory context to ensure that the client-side observations of the concrete system are possible observations of the abstract system. In particular, if an abstract object specifies a particular client-side synchronisation, then this synchronisation must also be present in the concrete implementation (see [Dalvandi and Dongol 2021]). Thread view stability guarantees that the $R_O$ component of the refinement relation is preserved when the thread view in the library is shifted forward, e.g., due to synchronisation within a client.

Note that Definition 5 only guarantees preservation of safety. To additionally preserve liveness, further progress guarantees are required in an implementation [Dongol and Groves 2016; Gotsman and Yang 2011]. We leave liveness preservation through refinement for future work since notions of fairness and progress of weak memory models is still at the early stages [Lahav et al. 2021].

Theorem 2. If $R$ is a forward simulation between AO and CO, then for any client $P$ we have $P[CO] \leq P[AO]$.

6.2 Forward Simulation for TML-RA

Perhaps the most technically challenging aspect of this paper is the proof of Theorem 3 below, which ensures the correctness of TML-RA w.r.t. TMS2-RA. Validity of the forward simulation itself has been verified using Isabelle/HOL. The refinement relation

$$R((als,y_A, \beta_A),(ls,y_C, \beta_C)) \equiv R_V((als, \beta_A), (ls, \beta_C)) \wedge (1) \wedge (2) \wedge (3) \wedge (4) \wedge (5) \wedge (6) \wedge (7) \wedge (8) \wedge (9)$$

The first conjunct (1) in the refinement relation $R$ states that the value of the last write to $\text{glb}$ divided by 2 ($\text{wc}(n) \equiv n \div 2$) is equal to the last version of history written to $M$.

$$\text{wc}(y_C.\text{lastval}(\text{glb})) = \lfloor y_A.M \rfloor$$  \hspace{1cm} (1)

The next conjunct, (2), states that the last value written to any location $l$ in $y_C$ is either the value of $l$ in the last abstract memory index or in the write set of the executing transaction

$$\forall l. l \neq \text{glb} \Rightarrow y_C.\text{lastval}(l) \in \{y_A.M_{[y_A.M]}(l), y_A.\text{wrSet}_t(l)\}$$  \hspace{1cm} (2)

where $\text{lastval}(x)$ is a function that returns the value of the last write written to a location $x$.

The next conjunct (3) is an on-the-fly simulation relation (i.e. the transaction has begun and is not committed or aborted) and states that for all threads $r$ if transaction $t$ ($y_A.\text{txn}_r = t$) is on-the-fly, the value of $\text{wc}(y_C.\text{loc}_r)$ will be greater than or equal to $\text{beginIdx}_t$ and the read set of $t$ will be consistent with memory version $\text{wc}(y_C.\text{loc}_r)$:

$$y_A.\text{beginIdx}_t \leq \text{wc}(ls.\text{loc}_t) \wedge y_A.\text{rdSet}_t \subseteq y_A.M_{\text{wc}(ls.\text{loc}_t)}$$  \hspace{1cm} (3)

Conjunct (4) states that if the value of $ls.\text{loc}_t$ is even then write set of $y_A$ must be empty:

$$\text{even}(ls.\text{loc}_t) \Rightarrow y_A.\text{wrSet}_t = \emptyset$$  \hspace{1cm} (4)

Also if a transaction $t$ that has already written to a location then the write set of $y_A$ is not empty:

$$ls.\text{hasWritten}_t \Rightarrow y_A.\text{wrSet}_t \neq \emptyset$$  \hspace{1cm} (5)

If a transaction has not read any location yet in the concrete state, then the read set of the abstract state should be empty:

$$\neg ls.\text{hasRead}_t \Rightarrow y_A.\text{rdSet}_t = \emptyset$$  \hspace{1cm} (6)
If there is a write in the write set of the abstract state, then the value should match the value of the last write written to that location by the concrete implementation:

$$\forall l \in \text{dom}(\gamma_A.\text{wrSet}_t). \quad \gamma_A.\text{wrSet}_t(l) = \gamma_C.\text{lastval}(l)$$  \hspace{1cm} (7)

The value of a visible write of thread $\tau$ to variable $glb$ divided by two is a visible memory by thread $\tau$ of the abstract state:

$$\forall w \in \gamma_C.\text{OW}_t(glb). \quad \text{wc}(\text{val}(w)) \in \gamma_A.\text{vmems}_t$$  \hspace{1cm} (8)

All seen memory indices by the abstract transaction $t$ are less the value of thread view of $glb$ for thread $\tau$ divided by 2:

$$\forall i \in \gamma_A.\text{seenIdxs}_t. \quad i \leq \text{wc}(\text{val}(\gamma_C.\text{tview}_t(glb)))$$  \hspace{1cm} (9)

**Theorem 3.** $R$ is a forward simulation between TMS2-ra and TML-ra.

**Proof.** This theorem has been verified in Isabelle/HOL. $\square$

### 7 Related Work

**Verifying C11 programs.** There are now several different approaches to program verification that support different aspects of the C11 relaxed memory model using pen-and-paper proofs (e.g., [Alglave and Cousot 2017; Doko and Vafeiadis 2017; Lahav and Vafeiadis 2015; Turon et al. 2014]), model checking (e.g., [Abdulla et al. 2019; Kokologiannakis et al. 2019]), specialised tools (e.g., [Krishna et al. 2020; Summers and Müller 2018; Svendsen et al. 2018; Tassarotti et al. 2015]), and generalist theorem provers (e.g., [Dalvandi et al. 2020a]). These cover a variety of (fragments of) memory models and proceed via exhaustive state space exploration, separation logics, or Hoare-style calculi. A related approach to TARO that uses a view-based semantics for persistent x86-TSO has been developed by Bila et al. [2022].

Another series of works has focussed on semantics that support the relaxed dependencies that are allowed by C11 [Jagadeesan et al. 2020; Kang et al. 2017; Lee et al. 2020; Paviotti et al. 2020]. These have been followed more recently by logics and verification over this semantics [Svendsen et al. 2018; Wright et al. 2021]. However, relaxed dependencies produce high levels of non-determinism, making verification significantly more complex. We consider a verification framework that supports relaxed dependencies and STMs to be a topic for future research.

More recent works include robustness of C11-style programs, which aims to show “adequate synchronisation” so that the relaxed memory executions reduce to executions under stronger memory models [Margalit and Lahav 2021]. Such reductions, although automatic, are limited to finite state systems, and a small number of threads. Furthermore, it is currently unclear how they would handle client-library synchronisation or relaxed (non-SC) specifications.

**Correctness conditions under relaxed memory.** Following the extensive literature on the semantics of relaxed memory architectures, a natural next question has been the development of library abstractions for relaxed memory. One aim has been to ensure observational refinement and compositionality of the implemented objects. A series of works have considered reforumulations of linearizability [Doherty et al. 2018; Dongol et al. 2018b; Raad et al. 2019a] by presenting suitable weakenings fine-tuned to the underlying memory model. This includes extensions of linearizability, e.g., so that it is defined in terms of axiomatic (aka declarative) relaxed memory models [Dongol et al. 2018b; Raad et al. 2019a] and those that are based on the more abstract concept of execution structures [Doherty et al. 2018]. Recent works have covered verification of relaxed memory concurrent data structures that have been developed to satisfy the conditions described above [Dalvandi and Dongol 2021; Krishna et al. 2020; Raad et al. 2019a], but none of these cover transactions.
Khyzha and Lahav [2022] have recently developed notions of abstraction for crash resilient libraries, providing correctness conditions (extending linearizability) that ensure contextual refinement for concurrent objects executed over the PSC (persistent sequential consistency) model. They do so by exposing the internal synchronisation mechanisms that are used to implement an object in the history (in addition to the invocations and responses). Our work differs since we consider transactional memory libraries as opposed to concurrent objects, use a different memory model and focus on verification of contextual refinement directly. Nevertheless, in future work, it would be interesting to see if their methods provide an alternative method for specifying concurrent object and transactional memory libraries in C11.

Several papers have revisited transaction semantics in the context of relaxed memory models [Chong et al. 2018; Dongol et al. 2018a, 2019; Raad et al. 2019b]. Raad et al have considered relaxed memory and snapshot isolation [Raad et al. 2018, 2019b], which is a weaker condition that serializability (and hence opacity and TMS2). The question of whether snapshot isolation can be fully exploited by implementations in a relaxed memory setting remains a topic of future research, with most transactional implementations aiming to support at least serializability [Zardoshti et al. 2019]. Dongol et al. [2018a] and Chong et al. [2018] have provided axiomatic transactional semantics integrated with relaxed memory models, focussing on hardware memory models and hardware transactions. Chong et al. [2018] additionally propose a model for C11 transactions, but these models are focussed on transactions within the compiler, as opposed to STMs. Finally, the axiomatic models proposed in these earlier works [Chong et al. 2018; Dongol et al. 2018a] are not suitable for operational verification, e.g., as supported by TARO, where we require an operational semantics as provided by TMS2-ra.

Another set of works has focussed on distributed (relaxed) transactions [Beillahi et al. 2021a,b; Xiong et al. 2020]. Although there are analogues between transactions in distributed systems and relaxed memory, constraints such as replication consistency and session order are not factors in shared memory, and hence the underlying issues are fundamentally different. Xiong et al. [2020] describe a taxonomy of distributed transactional models supported by an operational semantics. It would be interesting to investigate whether TARO can be adapted to cope with client-object systems in their models.

Relaxed memory TM implementations. There is a set of recent works on implementing TM algorithms in C11 [Spear et al. 2020; Zardoshti et al. 2019]. The focus here has been real-world implementability of STMs via compiler support. Since the focus is on benchmarks and real-world workflows, these works neither consider a formal semantics nor provide a verification framework. Our work can thus be seen as providing a formal basis to support to these efforts. In particular, we show how the serialisability specifications assumed by Spear et al. [2020]; Zardoshti et al. [2019] can be relaxed, without impacting correctness, while improving performance.

8 CONCLUSIONS

In this paper, we have presented a new approach to release-acquire transactions for RC11 RAR (a fragment of C11 that supports relaxed as well as release-acquire atomics). We have developed a new TM specification, TMS2-ra, that extends TMS2 to a relaxed memory context by describing the interactions between transactions and their clients. We implement TMS2-ra by TML-ra, which is an adaptation of an existing eager algorithm, TML. We show that TML-ra outperforms TML-sc using the STAMP benchmarks.

Our second set of contributions covers the verification of release-acquire TM implementations. We focus on proofs at two levels: (i) correctness of client programs that use TMS2-ra, and (ii) correctness of implementations of TMS2-ra. For (i), we have developed a logic, TARO, extending [Dalvandi
and Dongol 2021], and used this logic to prove that TMS2-RA does indeed guarantee the desired client-side synchronisation properties. For (ii), we have applied a simulation method, similar to [Dalvandi and Dongol 2021] and proved a forward simulation between TML-RA and TMS2-RA. All proofs for (i) and (ii) as well as all meta-level soundness results are fully mechanised in the Isabelle/HOL proof assistant, providing a high level of assurance to our results.

Our motivation for using TML as the main implementation case study was to start with a simple algorithm with an existing proof in SC [Derrick et al. 2018]. TML performs a global synchronisation through a CAS on a single location, which degrades performance on write-heavy workloads. For improved scalability, there are more sophisticated algorithms like TL2 [Dice et al. 2006] that offer per-location locking as well as hybrid TM implementations [Matveev and Shavit 2015] that combine hardware and software TM. TMS2 is known to be a sufficient abstraction for hybrid TMs in SC [Armstrong and Dongol 2017], so it is likely that TMS2-RA also provides a basis for developing and verifying relaxed and release-acquire versions of these more sophisticated algorithms. We leave such studies for future work.

ACKNOWLEDGMENTS

The authors would also like to thank the anonymous referees for their valuable comments and helpful suggestions. Dalvandi and Dongol are supported by EPSRC Grant EP/R032556/1. Dongol is additionally supported by EPSRC Grant EP/V038915/1, EPSRC Grant EP/R025134/2, ARC Grant DP190102142 and VeTSS.

REFERENCES

P. A. Abdulla, J. Arora, M. F. Atig, and S. N. Krishna. 2019. Verification of programs under the release-acquire semantics. In PLDI, K. S. McKinley and K. Fisher (Eds.). ACM, 1117–1132. https://doi.org/10.1145/3314221.3314649

J. Alglave and P. Cousot. 2017. Ogre and Pythia: an invariance proof method for weak consistency models. In POPL, G. Castagna and A. D. Gordon (Eds.). ACM, 3–18.

J. Alglave, L. Maranget, and M. Tautschnig. 2014. Herding Cats: Modelling, Simulation, Testing, and Data Mining for Weak Memory. ACM Trans. Program. Lang. Syst. 36, 2 (2014), 7:1–7:74.

A. Armstrong and B. Dongol. 2017. Modularising Opacity Verification for Hybrid Transactional Memory. In FORTE (LNCS, Vol. 10321), A. Bouajjani and A. Silva (Eds.). Springer, 33–49.

A. Armstrong, B. Dongol, and S. Doherty. 2017. Proving Opacity via Linearizability: A Sound and Complete Method. In FORTE (LNCS, Vol. 10321), A. Bouajjani and A. Silva (Eds.). Springer, 50–66.

G. Assa, H. Meir, G. Golan-Gueta, I. Keidar, and A. Spiegelman. 2020. Nesting and composition in transactional data structure libraries. In Ppop ’20, R. Gupta and X. Shen (Eds.). ACM, 405–406. https://doi.org/10.1145/3332466.3374514

G. Assa, H. Meir, G. Golan-Gueta, I. Keidar, and A. Spiegelman. 2021. Using Nesting to Push the Limits of Transactional Data Structure Libraries. In OPODIS (LIPIcs, Vol. 217), Q. Bramas, V. Gramoli, and A. Milani (Eds.). Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 30:1–30:17. https://doi.org/10.4230/LIPIcs.OPODIS.2021.30

H. Attiya, A. Gotsman, S. Hans, and N. Rinetzky. 2018. Characterizing Transactional Memory Consistency Conditions Using Observational Refinement. J. ACM 65, 1 (2018), 2:1–2:44.

M. Batty, A. F. Donaldson, and J. Wickerson. 2016. Overhauling SC atoms in C11 and OpenCL. In POPL, ACM, 634–648.

M. Batty, S. Owens, S. Sarkar, P. Sewell, and T. Weber. 2011. Mathematizing C++ concurrency. In POPL, T. Ball and M. Sagiv (Eds.). ACM, 55–66.

S. M. Beillahi, A. Bouajjani, and C. Enea. 2021a. Checking Robustness Between Weak Transactional Consistency Models. In ESOP (LNCS, Vol. 12648), N. Yoshida (Ed.). Springer, 87–117. https://doi.org/10.1007/978-3-030-72019-3_4

S. M. Beillahi, A. Bouajjani, and C. Enea. 2021b. Robustness Against Transactional Causal Consistency. Log. Methods Comput. Sci. 17, 1 (2021). https://lmcs.episciences.org/7149

E. Vafeiadi Bila, B. Dongol, O. Lahav, A. Raad, and J. Wickerson. 2022. View-Based Owckii-Gries Reasoning for Persistent x86-TSO. In ESOP (Lecture Notes in Computer Science, Vol. 13240), I. Sergey (Ed.). Springer, 234–261. https://doi.org/10.1007/978-3-030-99336-8_9

S. Böhme and T. Nipkow. 2010. Sledgehammer: Judgement Day. In IJCAR (LNCS, Vol. 6173). Springer, 107–121.

N. G. Bronson, J. Casper, H. Chaﬁ, and K. Olukotun. 2010. Transactional predication: high-performance concurrent sets and maps for STM. In PODC, A. W. Richa and R. Guerraoui (Eds.). ACM, 6–15. https://doi.org/10.1145/1835698.1835703

Proc. ACM Program. Lang., Vol. 1, No. OOPSLA, Article 1. Publication date: December 2022.
M. Spear, H. Boehm, V. Luchangco, M. L. Scott, and M. Wong. 2020. *Transactional Memory Lite Support in C++*. Technical Report. isocpp.

A. J. Summers and P. Müller. 2018. Automating Deductive Verification for Weak-Memory Programs. In *TACAS (LNCS, Vol. 10805)*, D. Beyer and M. Huisman (Eds.). Springer, 190–209.

K. Svendsen, J. Pichon-Pharabod, M. Doko, O. Lahav, and V. Vafeiadis. 2018. A Separation Logic for a Promising Semantics. In *ESOP (LNCS, Vol. 10801)*, A. Ahmed (Ed.). Springer, 357–384.

J. Tassarotti, D. Dreyer, and V. Vafeiadis. 2015. Verifying read-copy-update in a logic for weak memory. In *PLDI*, D. Grove and S. Blackburn (Eds.). ACM, 110–120. https://doi.org/10.1145/2737924.2737992

A. Turon, V. Vafeiadis, and D. Dreyer. 2014. GPS: navigating weak memory with ghosts, protocols, and separation. In *OOPSLA*, A. P. Black and T. D. Millstein (Eds.). ACM, 691–707.

V. Vafeiadis and C. Narayan. 2013. Relaxed separation logic: A program logic for C11 concurrency. In *OOPSLA*. 867–884.

D. Wright, M. Batty, and B. Dongol. 2021. Owicki-Gries Reasoning for C11 Programs with Relaxed Dependencies. 13047 (2021), 237–254. https://doi.org/10.1007/978-3-030-90870-6_13

S. Xiong, A. Cerone, A. Raad, and P. Gardner. 2020. Data Consistency in Transactional Storage Systems: A Centralised Semantics. In *ECOOP (LIPIcs, Vol. 166)*, R. Hirschfeld and T. Pape (Eds.). Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 21:1–21:31. https://doi.org/10.4230/LIPIcs.ECOOP.2020.21

P. Zardoshti, T. Zhou, P. Balaji, M. L. Scott, and M. F. Spear. 2019. Simplifying Transactional Memory Support in C++. *ACM Trans. Archit. Code Optim.* 16, 3 (2019), 25:1–25:24. https://doi.org/10.1145/3328796
\[
\begin{align*}
\text{READ} & \quad a \in \{rd(x, v), rdA(x, v)\} \quad w \in \gamma.OW(x) \quad \text{val}(w) = v \\
\text{tview}' &= \text{if } \gamma.\text{rel}(w) \land a = rdA(x, v) \text{ then } \gamma.\text{tview}_{\gamma} \otimes \gamma.\text{mview}_{\gamma} \text{ else } \gamma.\text{tview}_{\gamma}[x := w] \\
\begin{array}{c}
\gamma \xrightarrow{a} \gamma[	ext{tview}_{\gamma} := \text{tview}']
\end{array}
\end{align*}
\]

\[
\begin{align*}
\text{WRITE} & \quad a \in \{wr(x, v), wrR(x, v)\} \quad w \in \gamma.OW(x) \setminus \gamma.cvd \quad \text{fresh}_\gamma(x, q) \quad \text{tst}(w) < q \\
\text{writes}' &= \gamma.\text{writes} \cup \{(x, v, q)\} \quad \text{tview}' = \gamma.\text{tview}_{\gamma}[x := (x, v, q)] \quad b = (a = wrR(x, v)) \\
\gamma \xrightarrow{a} \gamma[	ext{tview}_{\gamma} := \text{tview}', \text{mview}_{\gamma(x, v, q)} := \text{tview}', \text{writes} := \text{writes}', \text{rel} := \gamma.\text{rel}[w := b]]
\end{align*}
\]

\[
\begin{align*}
\text{RMW-RA} & \quad a = rmwRA(x, v, q) \quad w \in \gamma.OW(x) \setminus \gamma.cvd \quad \text{val}(w) = u \quad \text{fresh}_\gamma(x, q) \quad \text{tst}(w) < q \\
\text{writes}' &= \gamma.\text{writes} \cup \{(x, v, q)\} \quad \text{cvd}' = \gamma.cvd \cup \{(x, v, q)\} \\
\text{tview}' &= \text{if } \gamma.\text{rel}(w) \text{ then } \gamma.\text{tview}_{\gamma}[x := (x, v, q)] \otimes \gamma.\text{mview}_{\gamma} \text{ else } \gamma.\text{tview}_{\gamma}[x := (x, v, q)] \\
\gamma \xrightarrow{a} \gamma[	ext{tview}_{\gamma} := \text{tview}', \text{mview}_{\gamma(x, v, q)} := \text{tview}', \text{writes} := \text{writes}', \text{cvd} := \text{cvd}', \text{rel} := \gamma.\text{rel}[w := (x, v, q) := \text{true}]]
\end{align*}
\]

Fig. 11. Memory semantics for reads, writes and updates, where \(\text{fresh}_\gamma(x, q)\) holds iff there is no write in \(\gamma.\text{writes}\) on \(x\) with timestamp \(q\), i.e., \((x, _, q) \notin \gamma.\text{writes}\)

A  RC11 RAR OPERATIONAL SEMANTICS

We now briefly review the C11 operational semantics (introduced by [Dalvandi et al. 2020a]) used in our framework.

Component State. Here we detail the C11 state as modelled by the operational semantics. The first state component is \(\text{writes}\) which is the set of all global writes to shared locations. Each global write is represented by a tuple \((x, v, q)\), where \(x\) is a shared location, \(q\) is a rational number used as a timestamp, and \(v\) is the value written by the global write. The writes to each variable are totally ordered by timestamps.

For any write \(w = (x, v, q)\), we have \(\text{var}(w) = x\), \(\text{tst}(w) = q\) and \(\text{val}(w) = v\). The state needs to record the writes that are observable by each thread. A function \(\text{tview}_t\) is included in the state to record the viewfront of thread \(t\) (i.e. the latest write that a thread has seen so far). All the writes with a timestamp greater than or equal to the timestamp of the viewfront of thread \(t\) are observable by the thread. Another component of the state is a function \(\text{mview}_w\) that records the viewfront of write \(w\), which is set to be the viewfront of the thread that executed \(w\) at the time of \(w\)’s execution. \(\text{mview}_w\) is used to compute a new value for \(\text{tview}_t\) if a thread \(t\) synchronizes with \(w\). The state also must record if a global write is releasing. This is recorded by a function \(\text{rel}_w\) which returns \(true\) if \(w\) is releasing or \(false\) otherwise. Finally, the state maintains a variable \(\text{cvd} \subseteq \text{writes}\). The semantics assumes that each update action occurs in the modification order immediately after the write that it reads from to preserve the atomicity of updates. To prevent any newer write to intervene between any update and the write that it reads from, we add all the writes read by an update operation to the the covered set \(\text{cvd}\) so newer writes should never interact with covered writes.
The initial state \( y^{\text{Init}} \) is defined as follows.
\[
y^{\text{Init}}.\text{writes} \doteq \{(x, 0, 0) \mid x \in \text{Loc}\}
\]
\[
y^{\text{Init}}.\text{cvd} \doteq \emptyset
\]
\[
y^{\text{Init}}.\text{rel} \doteq \lambda(x, 0, 0). \text{false}
\]
\[
y^{\text{Init}}.\text{tview}_e \doteq \lambda x \in \text{Loc}. (x, 0, 0)
\]
\[
y^{\text{Init}}.\text{mview}_w \doteq \lambda x \in \text{Loc}. (x, 0, 0)
\]

\textbf{Transition semantics.} The transition relation of our semantics for global reads and writes is given in Fig. 11 [Dalvandi et al. 2020a].

\textbf{Read transition by thread} \( r \). Assume that \( a \) is either a relaxed or acquiring read to variable \( x \), \( w \) is a write to \( x \) that \( t \) can observe (i.e., \( (w, q, v) \in y.\text{OW}_r(x) \)), and the value read by \( a \) is the value written by \( w \). Each read causes the viewfront of \( t \) to be updated. For an unsynchronised read, \( \text{tview}_t \) is simply updated to include the new write. A synchronised read causes the executing thread’s view of the executing component and context to be updated. In particular, for each variable \( x \), the new view of \( x \) will be the later (in timestamp order) of either \( \text{tview}_t(x) \) or \( \text{mview}_w(x) \).

\textbf{Write transition by thread} \( t \). A write transition must identify the write \( (w, v, q) \) after which \( a \) occurs. This \( w \) must be observable and must not be covered — the second condition preserves the atomicity of read-modify-write (RMW) updates. We must choose a fresh timestamp \( q' \in \mathbb{Q} \) for \( a \), which for a C11 state \( y \) is formalised by \( \text{fresh}_y(q, q') = q < q' \land \forall w' \in y.\text{writes}. q < \text{tst}(w') \Rightarrow q' < \text{tst}(w') \). That is, \( q' \) is a new timestamp for variable \( x \) and that \( (a, q', v') \) occurs immediately after \( (w, v, q) \). The new write is added to the set \( \text{writes} \).

We update \( y.\text{tview}_e \) to include the new write, which ensures that \( t \) can no longer observe any writes prior to \( (a, v', q') \). Moreover, we set the viewfront of \( (a, v', q') \) to be the new viewfront of \( t \) in \( y \) together with the thread viewfront of the environment state \( \beta \). If some other thread synchronises with this new write in some later transition, that thread’s view will become at least as recent as \( t \)’s view at this transition. Since \( \text{mview}_w \) keeps track of the executing thread’s view of both the component being executed and its context, any synchronisation through this new write will update views across components.

\textbf{Update (aka RMW) transition by thread} \( t \). These transitions are best understood as a combination of the read and write transitions. As with a write transition, we must choose a valid fresh timestamp \( q' \), and the state component \( \text{writes} \) is updated in the same way. State component \( \text{mview}_w \) includes information from the new view of the executing thread \( t \). As discussed earlier, in \text{UPDATE} transitions it is necessary to record that the write that the update interacts with is now covered, which is achieved by adding that write to \( \text{cvd} \). Finally, we must compute a new thread view, which is similar to a \text{READ} transition, except that the thread’s new view always includes the new write introduced by the update.

\section{TMS2-RA Operational Semantics}

This section presents further details of the operational semantics from §3.3 of TMS2-RA as formalised in our Isabelle/HOL development.

\textbf{Component State.} Here we present the transactional state of TMS2-RA which builds on the earlier semantics of TMS2 [Doherty et al. 2013]. The state space of TMS2-RA extends the state space of TMS2 and comprises several components. The first component is \( M \) which is a sequence that keeps track of memory snapshots (memory states). The status of each transaction \( t \) is stored in
status, which can have any of the following values: NOTSTARTED, READY, COMMITTED, ABORTED. Each transaction \( t \) also has a write set \( \text{wrSet}_t \) and a read set \( \text{rdSet}_t \) where the writes and reads performed by the transaction are stored. For each transaction \( t \) there is also a beginIdx\(_t \) variable which is set to the most recent memory version when the transaction begins. We extend the TMS2 state space with a number of new components. The seenIdx\(_t \) variable stores the memory version of all the reads performed by the transaction. \( V_i \) is the memory modification view of a stored memory \( i \) \((0 \leq i \leq |M| - 1)\). Memory modification view of memory \( i \) is an snapshot of the transaction’s client thread view at the time of committing that memory. \( S_i \) indicates that if the transaction that committed memory version \( i \) was releasing.

**Initialisation.** The initial state \( \gamma^{\text{Init}} \) is defined as follows:

\[
\begin{align*}
\gamma^{\text{Init}}.M & \triangleq (\lambda l \in \text{Loc. } 0) \\
\gamma^{\text{Init}}.V & \triangleq (\lambda l \in \text{Loc. } \beta^{\text{Init}}.t\text{view}_t(l)) \\
\gamma^{\text{Init}}.S & \triangleq (\text{false}) \\
\gamma^{\text{Init}}.\text{status}_t & \triangleq \text{NOTSTARTED} \\
\gamma^{\text{Init}}.\text{rdSet}_t & \triangleq 0 \\
\gamma^{\text{Init}}.\text{wrSet}_t & \triangleq 0 \\
\gamma^{\text{Init}}.\text{seenIdx}_t & \triangleq 0 \\
\gamma^{\text{Init}}.\text{beginIdx}_t & \triangleq 0
\end{align*}
\]

where \( \beta^{\text{Init}} \) is the initial state of the client program.

**Transition semantics of TMS2-RA.** The transition relation of our TMS2-RA semantics for various transactional operations is given in Fig. 6 and explained below.

**TxBegin operation by transaction** \( t \). A transaction starts with a TxBegin operation and should specify if it is a relaxed or releasing/acquiring transaction. The TxBegin operation takes \( a \) and \( r \) and sets the value of \( \text{syncType}_t \) accordingly. It also sets the value \( \text{beginIdx}_t \) to be the latest memory version at the time of beginning the transaction and changes the \( \text{status}_t \) to READY. Values of \( \text{seenIdx}_t, \text{rdSet}_t \) and \( \text{wrSet}_t \) are set to empty.

**TxWrite operation by transaction** \( t \). Assuming that \( l \) is a location and \( v \) is a value and \( \text{status}_t = \text{READY} \), TxWrite operation of transaction \( t \) adds the \( l \mapsto v \) pair to the write set of transaction \( t \) (i.e. \( \text{wrSet}_t \)). Other state components remain unchanged.

**TxRead operation by transaction** \( t \). The transactional read operation (TxRead) reads the value \( (v) \) of location \( l \) from the transaction \( t \)’s write set \( \text{wrSet}_t \) if the transaction \( t \) has previously wrote to the location \( l \) \((l \in \text{dom}(\text{wrSet}_t)) \). In this case the state will remain unchanged.

If \( t \) has not previously written to \( l \) \((l \notin \text{dom}(\text{wrSet}_t)) \) then the value of \( l \) will be read from a memory version \( i \) where \( i \) is greater than or equal to \( \text{beginIdx}_t \) and the \( \text{rdSet}_t \) is consistent with that memory version (i.e. \( \text{rdSet}_t \subseteq M_i \)). In this case version \( i \) will be added to \( \text{seenIdx}_t \) and the transaction’s read set \( \text{rdSet}_t \) is also updated to include the \( l \mapsto v \). seenIdx\(_t\) is particularly important for synchronisation if the transaction is acquiring.

**TxEndRO operation by transaction** \( t \). A read-only transaction is committed by TxEndRO. If a transaction is read-only \((\text{wrSet}_t = 0) \) then it updates \( \text{status}_t \) of the transaction state \( (\gamma) \) to be COMMITTED and will leave the rest of the state unchanged. If the transaction was set to be acquiring
by $\text{TxBEGIN (isACQ}_t = \text{True)}$ and the transaction’s read set is not empty ($\text{rdSet}_t \neq \emptyset$) then the client’s thread view ($\beta_t\text{tview}_t$) may also get synchronised as well.

**TXEndWR operation by transaction $t$.** A writer transaction is committed by TXEndWR. Similar to a read-only transaction, a writer transaction ($\text{wrSet}_t \neq \emptyset$) will set $\text{status}_t$ to COMMITTED.

A writer transaction also add a new memory version $i$ to $M$ where $i$ is equal to the size of $\gamma.M$ meaning that the new memory version is added to the end of $M$ sequence. The new memory version is obtained by overwriting the latest memory version in $\gamma.M$ with the transaction’s write set: $\text{mem}' = \text{last}(\gamma.M \oplus \text{wrSet}_t)$. The function $\text{last}$ is defined as $\text{last}(m) = m_{|m|-1}$. The memory modification view ($V_i$) of the new memory version $i$ and the updated thread view of the client state ($tview_t$) is going to be the same and determined by $tview'$. The value of $tview'$ is determined in the same way as explained for TXEndRO.

**TXAbort operation by transaction $t$.** If transaction $t$ aborts, TXAbort will set $\text{status}_t$ to ABORTED. At this point, other transaction operations (except TXBegin) cannot be executed. The client state $\beta$ will remain unchanged.

### C  FORWARD SIMULATION IMPLIES OBSERVATIONAL REFINEMENT

We have already shown that there exists a forward simulation between TMS2-RA and TML-RA. In this section, we show that if there exists a forward simulation between an abstract TM specification $AO$ and a concrete implementation $CO$ as defined in Definition 5, then for any client $P$, $P[CO]$ is a contextual refinement of $P[AO]$ ($P[CO] \leq P[AO]$).

**Theorem 2.** If $R$ is a forward simulation between $AO$ and $CO$, then for any client $P$ we have $P[CO] \leq P[AO]$.

**Proof.** Assume $ft$ is a full trace of $P[CO]$, where for each $i$, $ft_i$ is a triple of the form $(Is_i, Y_i, \beta_i)$. We show that there exists a full trace $aft$ of $P[AO]$ such that $\xi(ft) \leq \xi(aft)$ (see Definition 2), where $\xi(ft)$ projects the full trace to the client trace, i.e., for each $i$, $\xi(ft)_i = (Is_i[P], \beta_i)$ (and similarly $\xi(aft)$), and additionally removes any stuttering.

The proof is by induction over prefixes $ft'$ of $ft$.

For the base case, $ft' = ((Is_{Init}, Y_{Init}, \beta_{Init}))$ is a trace containing just the initial state of $C$. By “Initialisation” of Definition 5 there exists a $(als_{Init}, f_{Init}^{\text{Init}}, \beta_{Init}^{\text{Init}})$ such that

$$R((als_{Init}, f_{Init}^{\text{Init}}, \beta_{Init}^{\text{Init}}), (Is_{Init}, Y_{Init}, \beta_{Init}))$$

Moreover, by “Client observation” of Definition 5, we have $als_{Init}|P = Is_{Init}|P$ and for all threads $x$ and locations $x$, $\beta_{Init}.OW(\tau, x) \subseteq \beta_{Init}.OW(\tau, x)$. Thus, for $\xi(ft)$ there exists an $aft$ such that $\xi(ft) \leq \xi(aft)$.

For our inductive hypothesis, assume the result holds for $ft'$, i.e., there exists an abstract prefix $aft'$ of an abstract trace $aft$ of $P[AO]$ such that $\xi(ft') \leq \xi(aft')$. Moreover, we assume that $R(\text{last}(aft'), last(ft'))$. Suppose $ft'' = ft' \cdot (Is, Y_C, \beta_C)$ where $(Is, Y_C, \beta_C)$ is generated by a concrete step from $last(ft')$. There are three possibilities based on the step taken by the concrete program.

- **The first case is when the concrete program takes a library step and $ft''$ is the program trace after the execution of the library step, because we already proved $CO \leq AO$ then by preservation rule of Definition 5 we know that there exists an abstract trace $aft'' = aft' \cdot (als, Y_A, \beta_A)$ such that $R((als, Y_A, \beta_A), (Is, Y_C, \beta_C))$. Moreover, using “Client observation” of Definition 5, we have $\xi(ft'') \leq \xi(aft'')$.
- **The next case is when the concrete program takes a non-synchronising client step. Since the abstract and concrete takes the same non-synchronising step, the abstract and concrete...**
library states remain unchanged, thus \( R_O((als|AO, \gamma_A), (ls|CO, \gamma_C)) \). Moreover, the thread view and local state of both abstract and concrete programs will be updated in the same way, thus we also have \( R_V((als, \beta_A), (ls, \beta_C)) \). Finally, by the client observation property and the refinement relation \( R \) are preserved. Since we match the concrete step at the abstract level, we have \( \xi(ft') \leq \xi(aft') \).

- The last case is when the concrete program takes a synchronising client step. Like the unsynchronising case, the abstract and concrete client steps are identical and they both update the thread view and local state of the client in the same way, thus \( R_V((als, \beta_A), (ls, \beta_C)) \). Thus, we have \( \xi(ft'') \leq \xi(af''t) \). We must now show that the refinement relation holds in the post-state. As opposed to the previous case, the synchronising client step potentially updates the library state by advancing the library thread view for the executing thread, \( \tau \). However, this is equivalent to moving the library view forward using the “Thread view stability” property of Definition 5. Thus, we have \( R_O((als|AO, \gamma_A), (ls|CO, \gamma_C)) \).

\[ \square \]

D SELECTION OF TARO PROOF RULES

We present a selection of TARO proof rules that we use in our examples. The full development [Davandi and Dongol 2022] contains many other rules, but we do not present all of these, since they are less interesting. Note that \( z \) below is a client variable.

D.1 Assertions over \( TxBegin \)

1. \( \{\neg[\dot{x} \approx u], r\} \quad TxBegin(_, _) \{\neg[\dot{x} \approx u], r\} \)
2. \( \{(\dot{x} = u)[z = v], r\} \quad TxBegin(_, _) \{(\dot{x} = u)[z = v], r\} \)
3. \( \{[z = u], r\} \quad TxBegin(_, _) \{[z = u], r\} \)
4. \( \{true\} \quad TxBegin_r(R, _) \{Rel_r\} \)
5. \( \{true\} \quad TxBegin_r(A, _) \{Acq_r\} \)
6. \( \{(\dot{y}, v) \in WS_r \land \tau \neq \tau'\} \quad TxBegin_r(_, _) \{(\dot{y}, v) \in WS_r\} \)

D.2 Assertions over \( TxRead \)

1. \( \{\neg[\dot{x} \approx u], r\} \quad TxRead(_, _) \{\neg[\dot{x} \approx u], r\} \)
2. \( \{[\dot{x} = u], r\} \quad TxRead_r(_, _) \{status_r = READY \Rightarrow [\dot{x} = u], r\} \)
3. \( \{WS_r = \emptyset\} \quad TxRead_r(\dot{x}, r) \{(\dot{x}, r) \in RS_r\} \)
4. \( \{[\dot{x} \approx r, r] \notin WS_r\} \quad TxRead_r(\dot{x}, r) \{[\dot{x} \approx r], r\} \)
5. \( \{[\dot{x} = u], r \land \dot{x} \notin dom(WS_r)\} \quad TxRead_r(\dot{x}, r) \{r = u\} \)
6. \( \{(\dot{y}, v) \in WS_r\} \quad TxRead_r(_, _) \{(\dot{y}, v) \in WS_r\} \)
7. \( \{(\dot{y}, v) \in RS_r \land \tau \neq \tau'\} \quad TxRead_r(_, _) \{(\dot{y}, v) \in RS_r\} \)

D.3 Assertions over \( TxWrite \)

1. \( \{\neg[\dot{x} \approx u], r\} \quad TxWrite(_, _) \{\neg[\dot{x} \approx u], r\} \)
2. \( \{[z = u], r\} \quad TxWrite(_, _) \{[z = u], r\} \)
3. \( \{true\} \quad TxWrite_r(\dot{y}, v) \{(\dot{y}, v) \in WS_r\} \)
This section provides the full proof outline for two additional examples. The proof outline presented in Fig. 13 includes two new assertions that were not introduced previously:

\[ \langle \hat{x} = u \rangle [z = \hat{v}] \land w \neq u \} \]
\[ \operatorname{TxWrite}_r(\hat{y}, \omega) \{ \langle \hat{x} = u \rangle [z = \hat{v}] \} \]
\[ \{ \hat{x} \neq \hat{y} \land (\hat{y}, \hat{v}) \in WS_r \} \]
\[ \operatorname{TxWrite}_r(\hat{x}, \_ \} \{ (\hat{y}, \hat{v}) \in WS_r \} \]

D.4 Assertions over \( \text{TxEnd} \)

1. \( \{ \langle \hat{x} = u \rangle [z = \hat{v}] \land WS_r = \emptyset \} \)
\[ \operatorname{TxEnd}_r \{ \langle \hat{x} = u \rangle [z = \hat{v}] \} \]

2. \( \{ \hat{x}, u \in WS_r \land \neg \langle \hat{x} \approx u \rangle \land \}
\[ \{ \langle \hat{x} = u \rangle [z = \hat{v}] \} \]
\[ \operatorname{TxEnd}_r \{ \langle \hat{x} = u \rangle [z = \hat{v}] \} \]

D.5 Assertions over client actions

1. \( \{ \langle \hat{x} = u \rangle [z = \hat{v}] \} \}
\[ \operatorname{r} \leftarrow \{ \langle \hat{x} = u \rangle [z = \hat{v}] \} \]
\[ \{ \langle \hat{x} = u \rangle [z = \hat{v}] \} \]
\[ \operatorname{z} \leftarrow m \{ \langle \hat{x} = u \rangle [z = \hat{v}] \} \]

E ADDITIONAL EXAMPLES

This section provides the full proof outline for two additional examples. The proof outline presented in Fig. 13 includes two new assertions that were not introduced previously:

- **Memory-value assertion**: A memory-value assertion, denoted as \( M[\hat{x}, \hat{v}]_i \), holds iff the value of location \( x \) in memory version \( i \) is \( \hat{v} \).

\[ M[\hat{x}, \hat{v}]_i \triangleq i \in \operatorname{dom}(M) \land M_i(\hat{x}) = \hat{v} \]

- **Never-written assertion**: A never-written assertion, denoted as \( NW[\hat{x}, \hat{v}] \), holds iff none of the recorded memories in \( M \) has the value \( v \) for location \( x \).

\[ NW[\hat{x}, \hat{v}] \triangleq \forall i \in \operatorname{dom}(M). \neg M[\hat{x}, \hat{v}]_i \]

A selection of proof rules over memory-value and never-written predicates are given below.

1. \( \{ M[\hat{x}, u] \} \}
\[ \operatorname{TxBegin}_r(\_ \} \{ M[\hat{x}, u] \} \]

2. \( \{ M[\hat{x}, u] \} \}
\[ \operatorname{TxRead}_r(\_ \} \{ M[\hat{x}, u] \} \]

3. \( \{ M[\hat{x}, u] \} \}
\[ \operatorname{TxWrite}_r(\_ \} \{ M[\hat{x}, u] \} \]

4. \( \{ (\hat{x}, u) \in WS_r \land |M| = n \} \}
\[ \operatorname{TxEnd}_r \{ \text{status}_r = \text{COMMITTED} \Rightarrow M[\hat{x} = u]_n \} \]

5. \( \{ M[\hat{x} = \hat{v}]_i \} \}
\[ \operatorname{TxEnd}_r \{ M[\hat{x} = \hat{v}]_i \} \]

Proc. ACM Program. Lang., Vol. 1, No. OOPSLA, Article 1. Publication date: December 2022.
\[
\begin{align*}
&M[\hat{x} = u],_{i-1} \land M[\hat{x} = v],_{i} \land \\
&M[\hat{y} = l],_{i-1} \land M[\hat{y} = n],_{i} \land \\
&u \neq v \land l \neq n \land i = |M| - 1 \land \\
&\text{txn}_i = t \land \text{beginIndex}_i = i - 1 \land \\
&(\hat{x}, v) \in RS \land WS = \emptyset \\
\end{align*}
\]

\[
(\overline{\text{TxRead}_i}(\hat{y}, r) \land \{\text{status}_i = \text{READY} \Rightarrow r = n\})
\]

\[
\begin{align*}
&\{NW[\hat{x}, v]\} \land \text{TxBegin}_i(\_ , \_ ) \land \{\neg[\hat{x} \approx v],_r\} \\
&\{NW[\hat{x}, v]\} \land \text{TxBegin}_i(\_ , \_ ) \land \{NW[x, v]\} \\
&\{NW[\hat{x}, v]\} \land \text{TxRead}_i(\_ , \_ ) \land \{NW[x, v]\} \\
&\{NW[\hat{x}, v]\} \land (\hat{x}, v) \notin WS \land \text{TxEnd}_i \land \{NW[\hat{x}, v]\}
\end{align*}
\]

**Theorem 4.** The proof outlines in Fig. 12 and Fig. 13 are valid.

**Proof.** This theorem has been verified in Isabelle/HOL. \qed
\{\forall r \in \{r_1, r_2, r_3\}, [\hat{f} = 0]_r \land [d_1 = 0]_r \land [d_2 = 0]_r,\}

**Thread r1**

\[
\begin{align*}
1: & \quad d_1 := 5; \\
2: & \quad T_x B e g i n (R, \emptyset) \\
3: & \quad T_x W r i t e (f, 1); \\
4: & \quad \{T x E n d, f'_1 := true\}; \\
5: & \quad \{f = 1\}[d_1 = 5]_r \land tf_1
\end{align*}
\]

**Thread r2**

\[
\begin{align*}
6: & \quad T_x B e g i n (R_{A_1}, \{r_2\}) \\
7: & \quad T_x R e a d (f, r_2); \\
8: & \quad \text{if } r_2 = 1 \text{ then} \\
9: & \quad T_x W r i t e (f, 2) \\
10: & \quad T_x E n d
\end{align*}
\]

**Thread r3**

\[
\begin{align*}
11: & \quad T_x B e g i n (A, \{r_3\}) \\
12: & \quad T_x R e a d (f, r_3); \\
13: & \quad T_x E n d
\end{align*}
\]

Fig. 12. Proof outline for extended transactional MP, where \(P(k) \triangleq [d_2 = k]_{r_2} \land (f = 1)[d_1 = 42]_{r_2} \land [\hat{f} \neq 2]_{r_1} \land [\hat{f} \neq 2]_{r_3}\)
Thread \(r_1\)
\[
\{\begin{align*}
& \text{\(NW[f,1] \land NW[d_2,10]\)} \\
& \{\begin{align*}
& \text{\(d_1 = 0\)} \\
& \text{\(\land [M = 0]\)} \\
& \text{\(\land \) if } d_1 = 5; \\
& \text{\(\land [M = 0]\)} \\
& \text{\(\land \) if } d_1 = 5; \\
& \text{\(\land [M = 0]\)} \\
& \text{\(\land \) if } d_1 = 5; \\
& \text{\(\land [M = 0]\)} \\
\end{align*}\}
\end{align*}\}
\]
1: \(d_1 := 5\);
2: \(\text{TxWrite}(R_X,0);\)
3: \(\text{TxWrite}(d_2,10);\)
4: \(\text{TxWrite}(f,1);\)
5: \(\text{TxEnd};\)
6: \(\text{TxBegin}(r_1);\)
7: \(\text{TxRead}(f,1);\)
8: \(\text{if } r_1 = 1 \text{ then}\)
9: \(\text{TxRead}(d_2, r_2);\)
10: \(\text{TxEnd};\)
11: \(r_3 \leftarrow d_1;\)

Thread \(r_2\)
\[
\{\begin{align*}
& \text{\(M[f = 0]_0 \land M[d_2 = 0]\)} \\
& \{\begin{align*}
& \text{\(\land \) if } \[M[f = 0]_1 \land M[d_2 = 10]\)} \\
& \text{\(r_1 = 1 \land (f, 1) \in RS_{r_1}\)} \\
& \{\begin{align*}
& \text{\(\land \) if } \[M[f = 1]_1 \land M[d_2 = 10]\)} \\
& \text{\(\land \) if } \[M[f = 1]_1 \land M[d_2 = 10]\)} \\
& \text{\(\land \) if } \[M[f = 1]_1\)} \\
& \text{\(\land \) if } \[M[f = 1]_1\)} \\
\end{align*}\}
\end{align*}\}
\]
1: \(d_1 := 5;\)
2: \(\text{TxWrite}(R_X,0);\)
3: \(\text{TxWrite}(d_2,10);\)
4: \(\text{TxWrite}(f,1);\)
5: \(\text{TxEnd};\)
6: \(\text{TxBegin}(RX_{\{r_1, r_2\}});\)
7: \(\text{TxBegin}(r_1);\)
8: \(\text{if } r_1 = 1 \text{ then}\)
9: \(\text{TxRead}(d_2, r_2);\)
10: \(\text{TxEnd};\)
11: \(r_3 \leftarrow d_1;\)

\{\begin{align*}
\text{\(\land \) if } \[M[f = 1]_1 \land M[d_2 = 10]\)} \\
\text{\(r_1 = 1 \land (f, 1) \in RS_{r_1}\)} \\
\{\begin{align*}
\text{\(\land \) if } \[M[f = 1]_1 \land M[d_2 = 10]\)} \\
\text{\(\land \) if } \[M[f = 1]_1\)} \\
\end{align*}\}
\]

Fig. 13. Proof outline for relaxed transactions where \(C\) and \(R\) are shorthand for COMMITTED and READY, respectively.