Communicating Memory Transactions

Mohsen Lesani Jens Palsberg

UCLA Computer Science Department
University of California, Los Angeles, USA
{lesani, palsberg}@cs.ucla.edu

Abstract

Many concurrent programming models enable both transactional memory and message passing. For such models, researchers have built increasingly efficient implementations and defined reasonable correctness criteria, while it remains an open problem to obtain the best of both worlds. We present a programming model that is the first to have opaque transactions, safe asynchronous message passing, and an efficient implementation. Our semantics uses tentative message passing and keeps track of dependencies to enable undo of message passing in case a transaction aborts. We can program communication idioms such as barrier and rendezvous that do not deadlock when used in an atomic block. Our experiments show that our model adds little overhead to pure transactions, and that it is significantly more efficient than Transactional Events. We use a novel definition of safe message passing that may be of independent interest.

Categories and Subject Descriptors D.1 [**Programming Techniques**]: D1.3 Concurrent Programming – Parallel programming

General Terms Languages, Design, Algorithms

Keywords Transactional Memory, Actor

1. Introduction

1.1. Background

Multi-cores are becoming the mainstream of computer architecture, and they require parallel software to maximize performance. Therefore, researchers sense the need for effective concurrent programming models more than ever before. We expect a concurrent programming model to provide means for both isolation and communication: concurrent operations on shared memory should be executed in isolation to preserve consistency of data, while threads also need to communicate to coordinate cooperative tasks. The classical means of programming isolation and communication is locks and condition variables [16]. Locks protect memory by enforcing that the memory accesses of blocks of code are isolated from each other by mutual exclusion. Condition variables allow threads to communicate: a thread can wait for a condition on shared memory locations and the thread that satisfies the condition can notify waiting threads. However, development and maintenance of concurrent data structures by fine-grained locks is notoriously hard and error-prone, and lock-based abstractions do not lend themselves well to composition. We need a higher level of abstraction.

A promising isolation mechanism to replace locks is memory transactions because they are easy to program, reason about, and compose [12]. The idea is to mark blocks of code as atomic and let the runtime system guarantee that these blocks are executed in isolation from each other. Researchers have developed several implementations [5][13], semantics [1][24][15], and correctness criteria [10][24] for memory transactions. In particular, we prefer to work with memory transactions that satisfy a widely recognized correctness criterion called opacity [10]. To complement memory transactions, which communication mechanism should replace condition variables? We want the addition of a communication mechanism to preserve opacity while adding little implementation overhead to pure transactions. Let us review the strengths and weaknesses of several known mechanisms.

1.2. Synchronizers, retry, and punctuation

Luchango and Marathe were the first to consider the interaction of memory transactions and they introduced synchronizers. A synchronizer encapsulates shared data that can be accessed simultaneously by every transaction that synchronizes (i.e. requests access) to it. The transactions that synchronize on a synchronizer (that is either read from or write to it) all commit or abort together. Additional concurrency control mechanisms are needed to protect the shared data against race conditions [20]. The work is recently extended to transaction communicators [22].

To enable a transaction to wait for a condition, Harris and Fraser introduced guarded atomic blocks [11], and Haskell added the "retry" keyword [12]. On executing "retry", Haskell aborts and then retries the transaction. Later, Smaragdakis et al. [28] established the need for transactional communication. They showed that neither of the previous mechanisms supports programming of a composable barrier abstraction: if used in an atomic block, the barrier deadlocks. In contrast to Haskell's "retry", Smaragdakis et al. [28] and also Dudnik and Swift [7] advocated that the waiting transaction should be committed rather than aborted. They observed that if the transaction is aborted, all its writes are discarded, while if it is committed, its writes will be visible to other transactions, thereby enabling the transaction to leave information for other transactions before it starts waiting.

Dudnik and Swift used their observation as the basis for designing transactional condition variables [7]; their model allows no nesting of atomic blocks. Smaragdakis et al. [28] used their observation as the basis for designing TIC which enables programming of a barrier abstraction that won't deadlock even if it is used in an atomic block. TIC splits (“punctuates”) each transaction into two transactions; this may violate local invariants and therefore requires the programmer to provide code for reestablishing the local invariants. TIC executes that code at the point of the split, that is, after wait is called and before the first

PPoPP'11 February 12–16, 2011, San Antonio, Texas, USA.

half of the transaction is committed. As explained in [28], TIC breaks isolation and therefore doesn't satisfy opacity.

1.3. Message Passing

A dual approach to providing means for isolation and communication is to begin with a message passing model such as Actors [2] and Concurrent ML (CML) [26], and then add an isolation mechanism. Examples of such combinations include Stabilizers [30], Transactional Events (TE) [6], and Transactional Events for ML (TE for ML) [8].

In Stabilizers, threads can communicate by sending and receiving synchronous messages on channels. The programmer can mark locations of code as stable checkpoints. If a thread encounters a transient fault, it calls "stabilize", which causes the run-time system to revert back the current thread, and all threads with which it has transitively communicated, to their latest possible stable checkpoints. In summary, Stabilizers support program location recovery but not atomicity and isolation as explained in [30].

Inspired by CML and Haskell STM, TE provides the programmer with a sequencing combinator to combine two events such as synchronous sends and receives into one compound event. The combination is an all-or-nothing transaction in the sense that executing the resulting event performs either both or none of the two events. The sequencing combinator enables straightforward programming of: (1) a modular abstraction of guarded (conditional) receive (this is not possible in CML), (2) three-way-rendezvous (a generalization of barrier) (this is not possible with pure memory transactions [6]), and (3) memory transactions (by representing each location as a server thread). TE supports the completeness property, namely: if there exists an interleaving for a set of compound events such that their sends and receives are matched to each other, the interleaving is guaranteed to be found. While the completeness property can terminate some scheduler-dependent programs, scheduler-independence is the well known property expected from concurrent algorithms. More importantly, finding such an interleaving is NP-hard [6] and can be implemented with an exponential number of run-time search threads [6]. Our experiments show that the performance penalty can be excessive.

TE supports all-or-nothing compound events but it prevents any shared memory mutation inside compound events. In follow-up work on TE, the authors of TE in ML [8] explain that encoding memory as a ref server is inefficient. They extend TE to support mutation of shared memory in compound events. TE for ML logically divides a compound event into sections called chunks. Chunks are delimited by the sends and receives of the compound event. The semantics of TE for ML breaks the isolation of shared memory mutations of a compound event at the end of its chunks. At these points (i.e. before sends and receives), the shared memory mutations that are done in the chunk can be seen by chunks of other synchronizing events. Similar to the punctuation in TIC, chunking breaks isolation and thus doesn't satisfy opacity.

1.4. Our Approach

The above review shows that previous work has problems with either nesting of atomic blocks, opacity, or efficiency. Our goal is to do better. In this paper, we present Communicating Memory Transactions (CMT) that integrates memory transactions with a style of asynchronous communication known from the Actor model. CMT is the first model to have opaque transactions, safe asynchronous message passing, and an efficient implementation. We use a novel definition of safety for asynchronous message passing that generalizes previous work. Safe communication means that every committed transaction has received messages only from committed transactions. To satisfy communication safety, CMT keeps track of dependencies to enable undo of message passing in case a transaction aborts. We show how to program three fundamental communication abstractions in CMT, namely synchronous queue, barrier, and three-way rendezvous. In particular we show that our barrier and rendezvous abstractions do not deadlock when used in an atomic block. To enable an efficient implementation, CMT does not satisfy the completeness property [8] found in TE. Based on the transactional memory implementations TL2 [5] and DSTM2 [13], we present two efficient implementations of CMT. We will explain several subtle techniques that we use to implement the semantics. Our experiments show that our model adds little overhead to pure transactions, and that it is significantly more efficient than Transactional Events.

In Section 2 we discuss five CMT programs. In Section 3 we recall the optimistic semantics of memory transactions by Koskinen, Parkinson, and Herlihy [15], and in Section 4 we give a semantics of CMT as an extension of the semantics in Section 3. In Section 5 we explain our implementation of CMT, and in Section 6 we show our experimental results.

2. Examples

The goal of this section is to give examples of CMT programs and give an informal discussion of the semantics of CMT. In particular, we will illustrate the notions of communication safety, dependency and collective commit. We use the following syntax: to delimit parallel sections of the program, || is used. $ch\ send\ e$ sends the result of expression e to channel ch. $x \coloneqq ch\ receive$ receives a message from channel ch and assigns it to the thread local variable x. To provide means of programming abstractions, macro definitions are allowed: $let\ macroName(params)\ \ t$. The body term t of the macro is inlined with $params$ at the call sites.

Let us start with a simple example: a server thread that executes a transaction in response to request messages from a client thread.

```
{ // Client                 | { // Server
  atomic                    |   atomic
    ch send unit            |     x := ch receive
} ||                        | }
```

The server transaction receives the tentative message from the client transaction and mutates memory according to the message. If the client transaction aborts, the message that it has sent is invalid. Therefore, the server transaction should commit only if the client transaction is committed. In other words, the communication is safe under the condition that a receiving transaction is committed only if the sender transaction is committed. We say that the receiving transaction depends on the sender transaction. If the sender aborts the receiver should abort as well. The abortion is propagated to depending transactions. If a receive is executed on a channel that is empty or contains an invalid message (a message sent by an aborted transaction), the receive suspends until a message becomes available.

Consider the two-way rendezvous abstraction that can swap values between two threads. (Rendezvous is a generalization of barrier that swaps values in addition to time synchronization.)

```
let rendezvous(sc1,rc1,sc2,rc2)  | let swap(x,sc,rc,v)
  atomic                         |   sc send v;
    x1 := sc1 receive;           |   x := rc receive
    x2 := sc2 receive;           |
    rc1 send x2;                 |
    rc2 send x1                  |
```

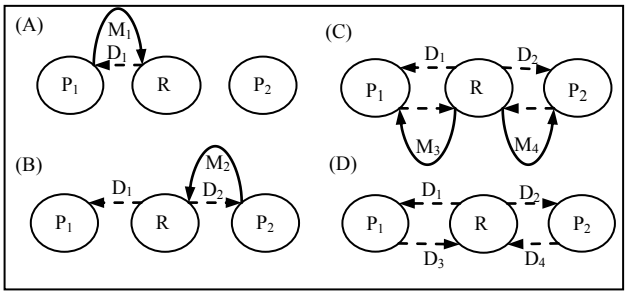

Figure 1. Interactions of 2-way Rendezvous

Consider the following program that employs the above abstractions. Each abstraction is inlined at its call sites and its parameters are substituted with passed arguments. Columns represent parallel parts of the program. (To discuss the interaction of transactions, the parties call *swap* inside atomic blocks.)

```
{ // Party1                 { // Rendezvous          { // Party2
  atomic                      rendezvous(             atomic
    // code before              ch1, ch2,               // code before
    swap(                      ch3, ch4)               swap(
      x, ch1, ch2, unit);    } ||                        x, ch3, ch4, unit);
    // code after                                       // code after
} ||                                                 }
```

Figure 1 shows the steps of execution of the above program. Solid arrows show messages and dashed arrows show dependencies. Party_1 sends a tentative Message_1 to Rendezvous. Rendezvous receives Message_1 and becomes dependent on Party_1 (Figure 1.A). The same happens for Party_2 (Figure 1.B). At this point, Rendezvous is dependent on both parties.

Assume that Party_2 aborts. The abortion is propagated to Rendezvous by Dependency_2. Rendezvous is also aborted and retried. On the retry, it receives Message_1 again. But as Message_2 is invalid, the second receive suspends. This means that Rendezvous repeats Figure 1.A again. It effectively ignores the aborted transaction of Party_2 and waits for another.

When Party_2 is retried, Figure 1.B is repeated. At this time, Rendezvous has received request messages from both parties. It tentatively sends swapped messages back to both Party_1 and Party_2. The parties are released from suspension and receive the messages. They get dependent on Rendezvous (Figure 1.C). At this time, parties and Rendezvous are interdependent (Figure 1.D).

Assume that Party_2 aborts in the code after *swap*. Dependencies propagate abortion to Rendezvous and then to Party_1. In other words, if one of the parties aborts, the Rendezvous and all the other parties are aborted and retried. This is the expected behavior: as Party_2 is aborted, the value that it has swapped with Party_1 is invalid. Therefore, Party_1 should be aborted as well. (This also matches the semantics expected from the barrier. As Party_2 aborts, it is retried. This means that it will reach the barrier again. By the semantics of the barrier, no party should pass the barrier when there is a party that has not reached the barrier. Thus, as Party_2 will reach the barrier, Party_1 should not have passed it. Therefore, Party_1 should be aborted as well.)

Finally, the transactions of Rendezvous, Party_1 and Party_2 reach the end of the atomic blocks. As they are interdependent, each of them can be committed only if the others are committed. If each of them obliviously waits until its dependencies are resolved, deadlock happens. As will be explained in the following sections, interdependent transactions are recognized as a cluster and transactions of a cluster are collectively committed.

In contrast to an implementation using Haskell retry, calling *swap* inside a nested atomic block does not lead to a deadlock. In addition, in contrast to TIC and TE for ML, opacity of transactions is satisfied.

Synchronous Queue
The abstractions:
```
let syncSend(
    sc, rc, v)
      sc send v;
      rc receive
let syncReceive(
    x, sc, rc)
  x := sc receive;
  rc send unit
```
The program:
```
{ // Sender
  syncSend(
    x, ch0, ch1)
} || { // Receiver
  syncReceive(
    x, ch0, ch1)
}
```

Barrier
The abstractions:
```
let barrier(
    bc1, pc1,
    bc2, pc2)
  atomic
    bc1 receive;
    bc2 receive;
    pc1 send unit;
    pc2 send unit
let await(bc, pc)
  bc send unit;
  pc receive
```
The program:
```
{ // Barrier
  barrier(
    ch1, ch2,
    ch3, ch4)
} || { // Party1
  await(ch1, ch2)
} || { // Party2
  await(ch3, ch4)
}
```

3-way Rendezvous
The abstractions:
```
let rendezvous(
    sc1, rc1,
    sc2, rc2,
    sc3, rc3)
  atomic
    x1 := sc1 receive;
    x2 := sc2 receive;
    x3 := sc3 receive;
    rc1 send ⟨x2, x3⟩;
    rc2 send ⟨x1, x3⟩;
    rc3 send ⟨x1, x2⟩;
let swap(x, sc, rc, v)
  sc send v;
  x := rc receive
```
The program:
```
{ // Rendezvous
  rendezvous(
    ch1, ch2,
    ch3, ch4,
    ch5, ch6)
} || { // Party1
  swap(
    x, ch1, ch2, unit)
} || { // Party2
  swap(
    x, ch3, ch4, unit
} || { // Party3
  swap(
    x, ch5, ch6, unit)
}
```

Figure 2: CMT Programs

Similar to Two-way Rendezvous, the abstractions for Synchronous queue, Barrier and Three-way rendezvous can be programmed in CMT as shown in Figure 2. Please note that it is assumed that these basic abstractions are used only once. For example, the basic barrier abstraction is not a cyclic barrier. For the three-way rendezvous, we assume that e can be pairs of the form $\langle e, e \rangle$. Implementations of Barrier with Haskell retry, TIC and TE for ML and an implementation of CMT can be seen in the technical report [17] section 15.1. Implementations of Synchronous Queue and Rendezvous can be seen in the technical report [17] sections 15.2 and 15.3.

3. Memory Transactions

We now recall the optimistic semantics of memory transactions by Koskinen, Parkinson, and Herlihy [15]. Their semantics is the starting point for our semantics of CMT in Section 4. TL2 is an implementation that realizes this semantics.

Note: we have fixed a few typos in the syntax, semantics and definition of moverness after personal communication with the authors of [15].

3.1. Syntax

A configuration is a triple of the form $\langle \mathcal{T} \cdot \sigma_{sh} \cdot \ell_{sh} \rangle$. (To simplify reading of long configurations, "·" is used to separate elements of configurations.) $\mathcal{T}$ represents the set of threads. σ_{sh} denotes the shared store that contains objects. ℓ_{sh} is a log of pairs $\langle \tau^{cmt}, \ell_\tau \rangle$: each committed transaction τ^{cmt} and the operations it has performed ℓ_τ. $\mathcal{T}$ is a set of elements of the form $\langle \tau, s, \sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau \rangle$. τ is

$$OCMD \quad \langle\langle \tau, c; s, \sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau\rangle, \mathcal{T} \cdot \sigma_{sh} \cdot \ell_{sh}\rangle \xrightarrow{\perp}_o \langle\langle \tau, s, [\![c]\!]\sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau\rangle, \mathcal{T} \cdot \sigma_{sh} \cdot \ell_{sh}\rangle \quad \tau \neq \perp$$

$$OBEG \quad \langle\langle \perp, \text{beg}; s, \sigma_\tau, \overleftarrow{\sigma_\tau}, []\rangle, \mathcal{T} \cdot \sigma_{sh} \cdot \ell_{sh}\rangle \xrightarrow{\langle \tau, \text{beg}\rangle}_o \langle\langle \text{fresh}(\tau), s, \text{snap}(\sigma_\tau, \sigma_{sh}), \sigma_\tau[\text{stmt} \mapsto \text{"beg; } s\text{"}], []\rangle, \mathcal{T} \cdot \sigma_{sh} \cdot \ell_{sh}\rangle$$

$$OAPP \quad \langle\langle \tau, x := o.m; s, \sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau\rangle, \mathcal{T} \cdot \sigma_{sh} \cdot \ell_{sh}\rangle \xrightarrow{\langle \tau, o.m\rangle}_o \langle\langle \tau, s, \sigma_\tau\big[o \mapsto ([\![o]\!]\sigma_\tau).m, x \mapsto rv\big(([\![o]\!]\sigma_\tau).m\big)\big], \overleftarrow{\sigma_\tau}, \ell_\tau :: (\text{"}o.m\text{"})\rangle, \mathcal{T} \cdot \sigma_{sh} \cdot \ell_{sh}\rangle \quad \tau \neq \perp$$

$$OCMT \quad \frac{\forall \langle \tau^{cmt}, \ell_{\tau'}\rangle \in \ell_{sh} : \tau^{cmt} > \tau \Rightarrow \ell_\tau \sqsupset \ell_{\tau'}}{\langle\langle \tau, end; s, \sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau\rangle, \mathcal{T} \cdot \sigma_{sh} \cdot \ell_{sh}\rangle \xrightarrow{\langle \tau, \text{cmt}\rangle}_o \langle\langle \perp, s, \text{zap}(\sigma_\tau), \text{zap}(\sigma_\tau), []\rangle, \mathcal{T} \cdot \text{merge}(\sigma_{sh}, \ell_\tau) \cdot \ell_{sh} :: \langle \text{fresh}(\tau^{cmt}), \ell_\tau\rangle\rangle} \quad \tau \neq \perp$$

$$OABT \quad \langle\langle \tau, s, \sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau\rangle, \mathcal{T} \cdot \sigma_{sh} \cdot \ell_{sh}\rangle \xrightarrow{\langle \tau, \text{abt}\rangle}_o \langle\langle \perp, [\![\text{stmt}]\!]\overleftarrow{\sigma_\tau}, \overleftarrow{\sigma_\tau}/\text{stmt}, \overleftarrow{\sigma_\tau}, []\rangle, \mathcal{T} \cdot \sigma_{sh} \cdot \ell_{sh}\rangle \quad \tau \neq \perp$$

$$\text{snap}(\sigma_\tau, \sigma_{sh}) = \sigma_\tau[o \mapsto [\![o]\!]\sigma_{sh}] \ \ \forall o \in \text{objects}(P) \qquad \text{merge}(\sigma_{sh}, [\ ]) = \sigma_{sh}$$

$$\text{zap}(\sigma_\tau) = \sigma_\tau[o \mapsto \perp] \ \ \forall o \in \text{objects}(P) \qquad \text{merge}(\sigma_{sh}, (\text{"}o.m\text{"}) :: \ell_\tau) = \text{merge}(\sigma_{sh}[\text{o} \mapsto ([\![o]\!]\sigma_{sh}]).m], \ell_\tau)$$

Figure 3: Optimistic Semantics of Memory Transactions

the transaction identifier (or $\perp$ that denotes that the code is executing outside transactions). Transaction identifiers are assumed to be ordered by the time that they are generated. s is the statement to be executed by the thread. Statements have the following syntax:

$s \rightarrow i; s \mid i$ *Statement*

$i \rightarrow beg \mid end \mid x := o.m \mid \text{c} \mid skip$ *Instruction*

beg and end denote the start and end of transactions. We use $atomic\ s$ as a syntactic sugar for $beg; s; end$. $o.m$ denotes calling method m on shared object o. Commands (reading and writing) that are applied to thread-local state are represented by c. σ_τ is the transaction-local store of objects. $\overleftarrow{\sigma_\tau}$ is the backup store that stores states of (thread-local) objects before the transaction is started. It is used to recover state when the transaction aborts. The statement before the transaction is started is also backed up in $\overleftarrow{\sigma_\tau}$. The pattern $\overleftarrow{\sigma_\tau}; stmt \mapsto s$ denotes a back up store that maps the backed up statement to s. ℓ_τ is the ordered log of operations that has been performed by the transaction. The initial configuration is of the form $Conf_0^o = \langle \mathcal{T}_0 \cdot \sigma_{sh_0} \cdot []\rangle$. $\mathcal{T}_0$ is $\mathcal{T}_0 = \{T_1, \ldots, T_n\}$ where $T_i = \langle \perp, P_i, \sigma_{sh_0}, \sigma_{sh_0}; stmt \mapsto \perp, []\rangle$. $\{P_{i=1..n}\}$ are the parallel segments of the program. σ_{sh_0} is the store where every object is mapped to its initial state i.e. $\sigma_{sh_0} = \{\forall o \in objects(P).o \mapsto init(o)\}$. $M[k \mapsto v]$ denotes assigning value v to key k in map M. $[\![k]\!]M$ represents value of key k in map M.

3.2. Operational Semantics

The semantics [15] is shown in Figure 3. The semantics is a labeled transition system. The syntax supports nested atomic blocks. We can transform a program with nested atomics into an equivalent program with only top-level atomics by simply removing all inner atomics. Hence, it is sufficient that the semantics supports only top-level atomics.

We will now explain the five rules in Figure 3. The $OCMD$ rule applies the statement to the local store. $[\![c]\!]\sigma_\tau$ denotes application of the command c to the local store σ_τ. The $OBEG$ rule starts a new transaction. A $fresh$ transaction identifier is generated. $fresh(\tau)$ generates unique and increasing transaction identifiers τ. The current store and also the current statement are stored in the backup store. A snapshot of the current state of objects is taken from the shared store to the local store. The $OAPP$ rule executes a method. The method is applied to the local store and is logged in the local log. rv represents the returned value. As defined by [15], read and write operations on memory locations are special cases of method call. The $OCMT$ rule checks that the methods of the current transaction are right movers with respect to the methods of the transactions that have been committed since the current transaction has started. Right moverness ensures that tentative execution of a transaction can be committed even though other transactions have committed after it started. Please refer to the appendix for a detailed definition of right moverness. If the methods of the transaction satisfy the moverness condition, the transaction is committed. The methods of the local log are applied to the shared store. The local log is also saved with a $fresh$ id in the shared log. This is used to check moverness while later transactions are committing. The $OABT$ reduction aborts the transaction. The store and the statement that were saved in the backup store when the transaction was starting are restored.

3.3. Properties

The semantics satisfies opacity which is a correctness condition for memory transactions [10]. We say that a sequence of labels $l_1, \ldots l_n$ is given by $\rightarrow_o$ started from $Conf_1^o$ if there are configurations $Conf_{i=2..n}^o$ such that for each $i \in \{1..n-1\}$: $Conf_{i=1}^o \xrightarrow{l_i}_o Conf_{i=n+1}^o$.

THEOREM 1 (Opacity). Every sequence of labels $\langle \tau, \text{beg}\rangle$, $\langle \tau, o.m\rangle$, $\langle \tau, \text{abt}\rangle$ and $\langle \tau, \text{cmt}\rangle$ given by $\rightarrow_o$ started from $Conf_0^o$ is opaque (Proposition 6.2 of [15]).

4. Communicating Memory Transactions

We now present the syntax and semantics of CMT. The semantics adds a core message passing mechanism to the semantics presented in the previous section.

4.1. Syntax

The syntax is extended as follows:

$s \rightarrow i; s \mid i$ *Statement*

$i \rightarrow beg \mid end \mid x := o.m \mid c \mid skip$ *Instruction*

$\mid ch\ send\ e \mid x := ch\ receive$

$ch\ send\ e$ sends the result of expression e to channel ch. $x := ch\ receive$ receives a message from channel ch and assigns it to the thread local variable x. We assume that messages are primitive values.

The configuration of the semantics in section 3 is augmented with the following elements: $\mathcal{M}$, $\mathcal{C}$ and $\mathcal{D}$. Therefore a configuration is a tuple of the form $\langle \mathcal{T} \cdot \sigma_{sh} \cdot \ell_{sh} \cdot \mathcal{M} \cdot \mathcal{C} \cdot \mathcal{D}\rangle$. $\mathcal{M}$

CMD

$$\langle\langle \tau, c; s, \sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau\rangle, \mathcal{T}\cdot\sigma_{sh}\cdot\ell_{sh}\cdot\mathcal{M}\cdot\mathcal{C}\cdot\mathcal{D}\rangle \xrightarrow{\perp} \langle\langle \tau, s, [\![c]\!]\sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau\rangle, \mathcal{T}\cdot\sigma_{sh}\cdot\ell_{sh}\cdot\mathcal{M}\cdot\mathcal{C}\cdot\mathcal{D}\rangle \qquad \tau \neq \perp$$

BEG

$$\frac{\mathcal{M}' = \mathcal{M} \cup \{\tau \mapsto \mathbb{r}\}}{\langle\langle \perp, \text{beg}; s, \sigma_\tau, \overleftarrow{\sigma_\tau}, []\rangle, \mathcal{T}\cdot\sigma_{sh}\cdot\ell_{sh}\cdot\mathcal{M}\cdot\mathcal{C}\cdot\mathcal{D}\rangle \xrightarrow{\langle\tau,\text{beg}\rangle} \langle\langle \text{fresh}(\tau), s, \text{snap}(\sigma_\tau, \sigma_{sh}), \sigma_\tau[\text{stmt} \mapsto \text{"beg; } s\text{"}], []\rangle, \mathcal{T}\cdot\sigma_{sh}\cdot\ell_{sh}\cdot\mathcal{M}'\cdot\mathcal{C}\cdot\mathcal{D}\rangle}$$

APP

$$\frac{\begin{array}{l}\langle\langle \tau, x \coloneqq o.m; s, \sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau\rangle, \mathcal{T}\cdot\sigma_{sh}\cdot\ell_{sh}\cdot\mathcal{M}\cdot\mathcal{C}\cdot\mathcal{D}\rangle \xrightarrow{\langle\tau,o.m\rangle} \\ \langle\langle \tau, s, \sigma_\tau[\text{o} \mapsto ([\![o]\!]\sigma_\tau).m, x \mapsto rv\big(([\![o]\!]\sigma_\tau).m\big)], \overleftarrow{\sigma_\tau}, \ell_\tau :: (\text{"}o.m\text{"})\rangle, \mathcal{T}\cdot\sigma_{sh}\cdot\ell_{sh}\cdot\mathcal{M}\cdot\mathcal{C}\cdot\mathcal{D}\rangle\end{array}}{\tau \neq \perp}$$

CMT

$$\frac{\begin{array}{c}\text{Cluster}(\{\tau_{i=1..n}\}, \mathcal{M}, \mathcal{D}) \\ \forall\tau_{i=1..n}\forall\langle\tau^{cmt}, \ell_{\tau'}\rangle \in \ell_{sh}.\tau^{cmt} > \tau_i \Rightarrow \ell_{\tau_i} \trianglerighteq \ell_{\tau'} \qquad \forall\tau_{i=1..n}\forall\tau_{j=1..i-1}.\ell_{\tau_i} \trianglerighteq \ell_{\tau_j} \\ \mathcal{M}' = \mathcal{M}[\tau_i \mapsto \mathbb{c}]_{i=1..n} \\ \hline \langle\tau_i, end; s_i, \sigma_{\tau_i}, \overleftarrow{\sigma_{\tau_i}}, \ell_{\tau_i}\rangle_{i=1..n}, \mathcal{T}\cdot\sigma_{sh}\cdot\ell_{sh}\cdot\mathcal{M}\cdot\mathcal{C}\cdot\mathcal{D}\rangle \xrightarrow{\langle\tau_1,\text{cmt}\rangle\ldots\langle\tau_n,\text{cmt}\rangle} \\ \langle\langle \perp, s_i, \text{zap}(\sigma_{\tau_i}), \text{zap}(\sigma_{\tau_i}), []\rangle_{i=1..n}, \mathcal{T}\cdot\text{merge}\big(\sigma_{sh}, \{\ell_{\tau_{i=1..n}}\}\big)\cdot\ell_{sh} :: \text{seq}\big(\langle\text{fresh}(\tau_i{}^{cmt}), \ell_{\tau_i}\rangle_{i=1..n}\big)\cdot\mathcal{M}'\cdot\mathcal{C}\cdot\mathcal{D}\rangle\end{array}}{\forall\tau_{i=1..n}.\tau_i \neq \perp}$$

ABT

$$\frac{\mathcal{M}' = \mathcal{M}[\tau \mapsto \mathbb{a}]}{\langle\langle \tau, s, \sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau\rangle, \mathcal{T}\cdot\sigma_{sh}\cdot\ell_{sh}\cdot\mathcal{M}\cdot\mathcal{C}\cdot\mathcal{D}\rangle \xrightarrow{\langle\tau,\text{abt}\rangle} \langle\langle \perp, [\![\text{stmt}]\!]\overleftarrow{\sigma_\tau}, \overleftarrow{\sigma_\tau}/\text{stmt}, \overleftarrow{\sigma_\tau}, []\rangle, \mathcal{T}\cdot\sigma_{sh}\cdot\ell_{sh}\cdot\mathcal{M}'\cdot\mathcal{C}\cdot\mathcal{D}\rangle} \qquad \tau \neq \perp$$

Send

$$\frac{\mathcal{C}' = \mathcal{C}[ch \mapsto \langle\tau, v\rangle]}{\langle\langle \tau, ch\ send\ v; s, \sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau\rangle, \mathcal{T}\cdot\sigma_{sh}\cdot\ell_{sh}\cdot\mathcal{M}\cdot\mathcal{C}\cdot\mathcal{D}\rangle \xrightarrow{\langle\tau,\text{ch send}\rangle} \langle\langle \tau, s, \sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau\rangle, \mathcal{T}\cdot\sigma_{sh}\cdot\ell_{sh}\cdot\mathcal{M}\cdot\mathcal{C}'\cdot\mathcal{D}\rangle} \qquad \tau \neq \perp$$

Receive

$$\frac{\mathcal{C}(ch) = \langle\tau', v\rangle \qquad \mathcal{D}' = \mathcal{D} \cup \{\tau \curvearrowright \tau'\}}{\langle\langle \tau, x \coloneqq ch\ receive; s, \sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau\rangle, \mathcal{T}\cdot\sigma_{sh}\cdot\ell_{sh}\cdot\mathcal{M}\cdot\mathcal{C}\cdot\mathcal{D}\rangle \xrightarrow{\langle\tau,\text{ch receive}\rangle} \langle\langle \tau, s, \sigma_\tau[x \mapsto v], \overleftarrow{\sigma_\tau}, \ell_\tau\rangle, \mathcal{T}\cdot\sigma_{sh}\cdot\ell_{sh}\cdot\mathcal{M}\cdot\mathcal{C}\cdot\mathcal{D}'\rangle} \qquad \tau \neq \perp$$

$$\begin{array}{lcl}\text{snap}(\sigma_\tau, \sigma_{sh}) & = & \sigma_\tau[o \mapsto [\![o]\!]\sigma_{sh}] \quad \forall o \in \text{objects}(P) \\ \text{zap}(\sigma_\tau) & = & \sigma_\tau[o \mapsto \perp] \quad \forall o \in \text{objects}(P)\end{array}$$

$$\text{Cluster}(\{\tau_{i=1..n}\}, \mathcal{M}, \mathcal{D}) = \forall i \in \{1 \ldots n\}: \begin{bmatrix} \forall\tau: ((\tau_i \curvearrowright \tau) \in \mathcal{D}) \Rightarrow \\ \begin{pmatrix}(\mathcal{M}(\tau) = \mathbb{c})\ or \\ (\exists j \in \{1 \ldots n\}: \tau = \tau_j)\end{pmatrix}\end{bmatrix}$$

$$\begin{array}{lcl}\text{merge}(\sigma_{sh}, [\ ]) & = & \sigma_{sh} \\ \text{merge}(\sigma_{sh}, (\text{"}o.m\text{"}) :: \ell_\tau) & = & \text{merge}(\sigma_{sh}[\text{o} \mapsto ([\![o]\!]\sigma_{sh}]).m], \ell_\tau) \\ \text{merge}(\sigma_{sh}, \{\}) & = & \sigma_{sh} \\ \text{merge}(\sigma_{sh}, \{\ell_{\tau_{i=1..n}}\}) & = & \text{merge}\big(\text{merge}\big(\sigma_{sh}, \{\ell_{\tau_{i=1..n-1}}\}\big), \ell_{\tau_n}\big) \\ \text{seq}(f(i)_{i=1..n}) & = & f(1) :: \cdots :: f(n)\end{array}$$

Figure 4: CMT Semantics

maps each transaction id to the state of the transaction. The state of a transaction can be either $\mathbb{r}$ (running), $\mathbb{c}$ (committed), or $\mathbb{a}$ (aborted). A committed transaction has finished successfully, while an aborted transaction has stopped execution and had its tentative effects discarded. $\mathcal{C}$ is a partial function that maps channels ch to pairs of the form $\langle\tau, v\rangle$ where τ is the sender transaction and v is the current value of the channel. To guarantee communication safety, we track dependencies between transactions. $\mathcal{D}$ is the transaction dependency relation that is a set of elements of the form $\tau \curvearrowright \tau'$. Transaction τ is dependent on transaction τ', i.e. $\tau \curvearrowright \tau'$, if τ receives a message that is sent by τ'. The dependency to τ' is said to be resolved, if τ' is committed. The initial configuration is $Conf_0 = \langle\mathcal{T}_0 \cdot \sigma_{sh_0} \cdot [] \cdot \emptyset \cdot \emptyset \cdot \emptyset\rangle$. $\mathcal{T}_0$ and σ_{sh_0} are defined as the prior semantics.

4.2. Operational Semantics

The rules *CMD*, *APP* are not changed other than the addition of $\mathcal{M}\cdot\mathcal{C}\cdot\mathcal{D}$ to both sides of the rules. The two rules *BEG* and *ABT* have a small change. They set the state of the transaction in $\mathcal{M}$ to running $\mathbb{r}$ and aborted $\mathbb{a}$, respectively.

The *Send* rule sends a message on a channel. The mapping $\mathcal{C}$ is updated to map the channel to the pair $\langle\tau, v\rangle$ where τ is the id of the current transaction and v is the sent value. The id of the sender transaction that is saved here is retrieved later when the message is received to record a dependency from the receiver to the sender. In CMT, each channel can hold a single value, while our implementation supports an arbitrary number of messages, as explained in section 5.

The *Receive* rule receives a message from a channel. If there exists a value in the channel, the value is received and the dependency of the current transaction to the sender transaction is added to $\mathcal{D}$. The condition that the sender transaction is not aborted can be added as an optimization.

The semantics in Figure 4 supports transactions that can send and receive. It is straightforward to extend the semantics to allow code executing outside transactions to send and receive.

The *CMT* rule encodes the collective commitment of a cluster. A set of transactions are committed if they satisfy the following two conditions.

To respect dependencies, the first condition is that only transactions of clusters are committed where Cluster is defined as follows. A set of transactions that have reached the end of their atomic blocks (called terminated) is a cluster iff any unresolved dependencies of them are to each other. The transactions that are considered in the *CMT* rule have already reached the end of their atomic blocks. It is checked that their dependencies are either to other transactions of the set or to committed transactions.

It is notable why the following simple commitment condition is not used instead: a transaction that has reached the end of its atomic block is committed only if all its dependencies are already resolved. It is straightforward that this condition directly translates to communication safety. But it can lead to deadlock. For example, if two transactions receive messages from each other,

they are interdependent. As mentioned for the example of Section 2, if each transaction in a dependency cycle obliviously waits until its dependencies are resolved, it may wait forever. In classical distributed transactions [18][3], all receives happen at the beginning of sub-transactions. Therefore, the dependencies form a tree and hierarchical commit and two phase commit protocol (2PC) can be employed. In CMT receives can happen in the middle of transactions; thus, the dependencies can in general form a cyclic graph. A commitment condition is needed that guarantees communication safety and also allows commitment of transactions with cyclic dependencies. It is also notable that in contrast to edges in DB read-write dependence graphs [9] that represent serialization precedence of source to the sink transaction, edges in the message dependence graphs represent commit dependence of source to the sink transaction. The former cannot be cyclic but the latter can.

The second condition is the moverness of transactions of the cluster with respect to each other. In the basic commit rule, the moverness condition was that methods of the committing transaction are right movers with respect to methods of the recently committed transactions. In addition to that, as we commit a set of transactions, we need to check that there is an order of them where methods of each transaction in the order are right movers with respect to method of earlier transactions in the order. (Note that this order is not necessarily the causal order of sends and receives.) If the conditions are met, the local logs of the transactions are applied to the shared store, the local logs are stored in the shared log with $fresh$ ids, and the state of the transactions are set to committed $\mathbb{c}$ in $\mathcal{M}$.

4.3. Properties

4.3.1. Opacity

The semantics of Figure 4 extends the semantics of Figure 3 with communication semantics while preserving the opacity of transactions. This enables programmers to reason locally about the consistency of data in each atomic block.

THEOREM 2 (Opacity). Every sequence of labels $\langle \tau, \mathrm{beg} \rangle$, $\langle \tau, o.m \rangle$, $\langle \tau, \mathrm{abt} \rangle$ and $\langle \tau, \mathrm{cmt} \rangle$ given by $\rightarrow$ started from $Conf_0$ is opaque.

High-level proof idea: Please refer to the technical report [17] section 10.1 for the formalization and the proof (29 pages). We reduce opacity for CMT to opacity for the semantics in Section 3. We show that for every sequence L of labels $\langle \tau, \mathrm{beg} \rangle$, $\langle \tau, o.m \rangle$, $\langle \tau, \mathrm{abt} \rangle$ and $\langle \tau, \mathrm{cmt} \rangle$ that can be obtained from transitions of $\rightarrow$, there is a sequence of transitions of $\rightarrow_o$ that yield a sequence of labels L' that is the same as L other than addition of calls to a definite new object. By THEOREM 1, L' is opaque. We show that removing all calls to an object from a sequence of labels preserves opaqueness of the sequence. Therefore, as L' is opaque, L is opaque. ■

4.3.2. Communication Safety

Assume that a transaction τ_r receives a message m that is tentatively sent by another transaction τ_s. Receiving m and using its value is a part of the computation of τ_r. Therefore, validity of the computation of τ_r relies on validity of m. If τ_s finally aborts, m becomes invalid and τ_r should be prevented from committing. This means that the receiving transaction τ_r should not commit before the sending transaction τ_s is committed. The notion is formalized as the following correctness condition:

DEFINITION 1 (Communication). The communication relation for an execution is the set of receiver and sender transaction pairs in the execution.

Suppose $Exec = Conf_0 \xrightarrow{l_0} Conf_1 \xrightarrow{l_1} \ldots \xrightarrow{l_{n-1}} Conf_n$. We define

$$Comm(Exec) = \{\, \tau_r \curvearrowright \tau_s \mid \exists i, j, ch: \quad 0 \le i < j < n, \\ l_i = (\tau_s, ch\ send), l_j = (\tau_r, ch\ receive) \\ \forall k: (i < k < j) \Rightarrow \big(\forall \tau: l_k \neq (\tau, ch\ send)\big) \}$$

Intuitively, τ_s is the last sender on ch before τ_r receives.

DEFINITION 2 (Unsafe execution) A configuration $Conf_0$ can execute to an unsafe configuration iff there is an execution

$Exec = Conf_0 \xrightarrow{l_0} Conf_1 \xrightarrow{l_1} \ldots \xrightarrow{l_{n-1}} Conf_n$, where
$Conf_n = \langle \mathcal{T}_n \cdot \sigma_{sh_n} \cdot \ell_{sh_n} \cdot \mathcal{M}_n \cdot \mathcal{C}_n \cdot \mathcal{D}_n \rangle$,
$\exists \tau_r, \tau_s:\ \mathcal{M}_n(\tau_r) = \mathbb{c}$
$\tau_r \curvearrowright \tau_s \in Comm(Exec)$
$\mathcal{M}_n(\tau_s) \neq \mathbb{c}$

THEOREM 3: Communication Safety: An initial configuration $Conf_0$ cannot execute to an unsafe configuration.

Please refer to the technical report [17] section 10.2 for the proof (16 pages).

High level proof idea: The first step is to prove $D_n = Comm(Exec)$ and thereby show that all members of $Comm(Exec)$ stem from the $Receive$ rule. Next we prove that when τ_r $receive$s a message from τ_s, τ_r is running, and we notice that the $Receive$ rule adds $\tau_r \curvearrowright \tau_s$ to $Comm(Exec)$. Later in the execution, τ_r may want to commit, and now the $\tau_r \curvearrowright \tau_s$ in $Comm(Exec)$ forces the CMT rule to ensure that τ_r only commits if either τ_s has already committed, or τ_r and τ_s commit together as members of the same cluster. ■

Our notion of communication safety generalizes a correctness criterion in [8]; let us explain why. Both TE and TE for ML support synchronous message passing. A high-level nondeterministic semantics "defines the set of correct transactions". In the high-level semantics, a set of starting transactions are stepped as follows: if there is a sequence of sub-steps that can match all the sends and receives of the transactions to each other, the transactions are committed together in single step. A low-level semantics is also defined that specifies stepping of the search threads that find the matching. It is proved that the low-level semantics complies with the high-level semantics. This essentially means that if a set of transactions are committed in the low-level semantics, each of them has communicated with transactions that are also committed at the same time. Our approach supports asynchronous messages. When a transaction sends a message, the message is enqueued in the recipient channel. Therefore, when a transaction is committing, there may not be matched receivers for the messages that it has sent but definite senders have sent the messages that it has received. Therefore, communication safety defines the condition that sender transactions are committed.

5. Implementation

We will now explain how we have implemented the calculus in Section 4 as the core functionality of a Scala [25] library called Transactors. Transactors integrate features of both memory transactions and actors. A transactor is an abstraction that consists of a thread and a channel that is called its mailbox. A mailbox is essentially a queue that can hold an arbitrary number of messages. Similar to the actor semantics [2], the messages in the mailbox are unordered. The thread of a transactor can perform the following operations both outside and inside transactions: reading from and

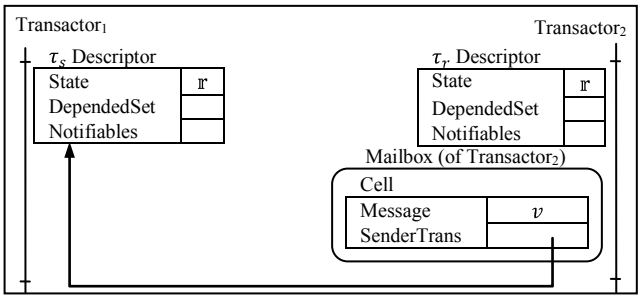

Figure 6. Sending

writing to shared memory and also sending messages to other transactors and receiving messages from its mailbox.

Recall that the starting point for Section 4 was Section 3 with its semantics of memory transactions. Similarly, the starting point for our implementation of the semantics in Section 4 is TL2, which implements Section 3's semantics of memory transactions. We explain how we have extended TL2 with an implementation of the new concepts in Section 4. In particular, we will explain about data structures that are built when messages are sent and received, the mechanism that notifies waiting transactions, cluster search and collective commit. (Our technique can work for other implementations of the semantics in Section 3 as well. In the technical report [17] section 13 we will explain how we have extended the implementation of DSTM2 in much the same way as we extended TL2. The pseudo codes of these two implementations can be found in the technical report [17] sections 12 and 14.)

In TL2, all memory locations are augmented with a lock that contains a version number. Transactions start by reading a global version-clock. Every read location is validated against this clock and added to the read-set. Written location-value pairs are added to the write-set. At commit, locks of locations in the write-set are acquired, the global version-clock is incremented and the read-set is validated. Then the memory locations are updated with the new global version-clock value and the locks are released.

In the implementation of transactors, the read and write procedures remain unchanged. As will be explained in subsection for the implementation of the CMT rule, we adapt the commit procedure to perform collective commitment of a cluster.

Each transaction has a descriptor that is a data structure that stores information regarding that transaction. This information includes the state of the transaction and a set that holds references to descriptors of depended transactions. Transactions change state as shown in Figure 7. Compared to the semantics in Section 4, the possible states of a transaction also include terminated. A transaction is terminated if it has reached the end of its atomic block and is not committed or aborted yet. The transaction descriptor also contains a set of notifiables and a message backup set that will be explained as we proceed.

In terms of $\mathcal{M}$ and $\mathcal{D}$ from the semantics, the descriptor of each transaction τ stores its state, $\mathcal{M}(\tau)$, and a set that holds references to descriptors of each τ' that $\tau \rightsquigarrow \tau' \in \mathcal{D}$. The mailboxes of transactors correspond to channels of $\mathcal{C}$. The semantics in Section 4 has seven rules. Two of those rules, CMD and APP, make no changes to the transaction map, channels, and dependencies. In the following five subsections we will explain how we implement the other five rules.

5.1. Starting a Transaction

We begin with the BEG rule. The rule changes M to $\mathcal{M}' = \mathcal{M} \cup \{\tau \mapsto \mathbb{r}\}$. When a transaction τ is started, a new transaction

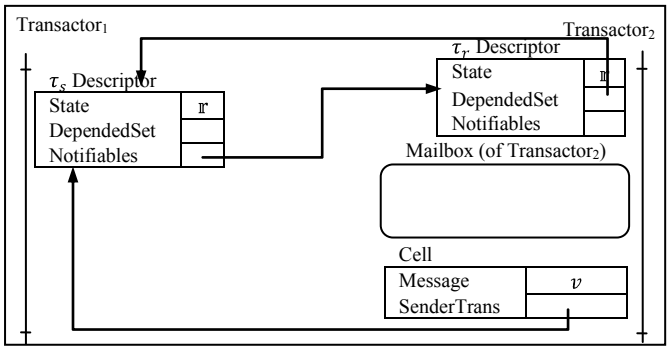

Figure 5. Receiving

descriptor with the running state $\mathbb{r}$ is created and stored in a thread local variable. (Later, to get the descriptor of the current transaction, this thread local variable is checked. If the variable has no value, the execution is outside atomic blocks and otherwise, the value is the descriptor of the current transaction.) The global version-clock is read and the body of the atomic block is started.

5.2. Sending and Receiving a Message

Next we consider the $Send$ rule. The rule changes $\mathcal{C}$ to $\mathcal{C}' = \mathcal{C}[ch \mapsto (\tau, v)]$. When a message v is being sent, a new cell containing the message is enqueued to the mailbox. As the $Send$ rule defines, besides the message, the sender transaction τ saves a reference to the descriptor of itself in the new cell. If the recipient transactor has been suspended inside a transaction to receive a message, it is resumed. If the send is being executed outside transactions, a reference to a dummy transaction descriptor that is always committed is saved as the sender transaction in the cell and if the recipient transactor has been suspended to receive a message (inside or outside a transaction), it is desuspended. Figure 6Figure 6 depicts relations of data structures while a message is being sent.

Next we consider the $Receive$ rule. The rule requires that $\mathcal{C}(ch) = (\tau_s, v)$ and changes $\mathcal{D}$ to $\mathcal{D}' = \mathcal{D} \cup \{\tau_r \rightsquigarrow \tau_s\}$. When a receive is being executed, cells of the mailbox are iterated. The reference to the descriptor of the sender transaction τ_s is obtained from each cell. The state of τ_s is read from its descriptor and the state of the message v of the cell is determined according to the state of τ_s. We use the terminology that (1) if the sender is committed, then the message is stable; and (2) if the sender is aborted, then the message is invalid. (3) if the sender is running or terminated, then the message is tentative. As any transaction that receives an invalid message should finally abort, invalid messages are dropped. This is the optimization that was mentioned for the $Receive$ rule. Thus, if the receive is being executed inside a transaction, a stable or tentative message is required to be taken from the mailbox. As executions that are outside transactions cannot be aborted, tentative messages can not be given to receives that are executed outside transactions. Therefore, a stable message is required for receives that are outside transactions. Cells are iterated and any invalid message is dropped until a required message is found. The thread suspends if a required message is not found until one becomes available. To track dependencies, if

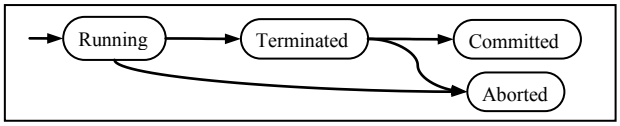

Figure 7. State transitions of a transaction

the found message is tentative, a reference to the descriptor of τ_s is added to the depended set of the descriptor of the current transaction τ_r. The depended sets of descriptors constitute a dependency graph. We say that τ_1 is adjacent to τ_2 if the descriptor of τ_2 is in the depended set of the descriptor of τ_1.

Figure 5 depicts data structures and their relations while a message is being received. Assume that a transaction τ_s has sent a message v that is received by another transaction τ_r. Assume that τ_s is running and τ_r is being terminated. As τ_r has an unresolved dependency, it cannot be committed yet. Therefore, the thread running τ_r goes to the waiting state until τ_s aborts or commits. Hence, when τ_s is aborted or committed, it should notify τ_r. Notification is done by notifiables. When τ_r is receiving the tentative message v, the reference to the descriptor of τ_s is obtained from the cell that contains v and a reference to the descriptor of τ_r is subscribed to it as a notifiable. On abortion or commitment of a transaction (τ_s), all its registered notifiables are notified.

When a transaction aborts, its effects should be rolled back. The messages that it has received from its mailbox should be put back. Therefore, to track messages that are received inside a transaction, when a message is being received, the cell that the message is obtained from is added to a backup set in the transaction descriptor (not shown in the figures). The set is iterated when the transaction is being aborted and any cell that is not invalid is put back to the mailbox.

5.3. Abortion

Next, we consider the ABT rule. The rule changes $\mathcal{M}$ to $\mathcal{M}' = \mathcal{M}[\tau \mapsto \text{a}]$. A transaction τ may deterministically abort as the result of resolution of a shared memory conflict. When τ is aborting, its state is set to aborted in its descriptor. Any cell of its backup set that is not invalid is put back to the mailbox. In addition, to wake up waiting transactions, τ propagates abortion to dependent transactions. Assume that $\{\tau_{r_{i=1..n}}\}$ is the set of transactions that are dependent on τ and $\{N_{i=1..n}\}$ is the set of notifiables that reference descriptors of $\{\tau_{r_{i=1..n}}\}$. τ notifies each N_i. The notification makes an abort event for τ_{r_i} if it is waiting. Finally, after notification, τ restarts its atomic block as a new transaction. On abortion of each τ_{r_i}, the same situation recurs, i.e. each of them notifies its own notifiables. Therefore, abortion of τ is propagated to transactions that are (transitively) dependent on τ. Note that by an implicit traversal of notifiable objects, abortion is propagated in the reverse direction of dependencies. The traversal avoids infinite loops by terminating at previously aborted transaction descriptors.

5.4. Termination and Commitment

Termination Every transaction that reaches the end of its atomic block sets the state of its descriptor to terminated. Then, the cluster search is started from the descriptor of the current transaction to check if it is possible to commit the transaction at this time. If the cluster search succeeds in finding a cluster, the transactions of the cluster are collectively committed and the atomic block returns successfully. Cluster search and collective commit are explained in the next subsection. If the cluster search cannot find a cluster at this time, the thread running the transaction goes to the waiting state. There are three different events that wake up a transaction from the waiting state:

- An Abortion event is raised when the transaction is notified of abortion of a depended transaction. On this event, the transaction starts abortion as explained above.
- A Dependency Resolution event: As will be explained in the collective commit procedure, a transaction that commits notifies all of the transactions that are dependent on it about the dependency resolution. On this event, as a dependency of the current transaction is known to be resolved, it may be able to commit; therefore, the cluster search is retried.
- A Commitment event is raised when the transaction is notified that it is committed by the cluster search and collective commit that is started from another transaction. On this event, the notifiables that are registered to the descriptor of transaction are notified of the dependency resolution. The atomic block returns successfully.

Commitment Next, we consider the CMT rule. The rule has the condition that the set of transactions should be a cluster $\text{Cluster}(\{\tau_{i=1..n}\}, \mathcal{M}, \mathcal{D})$ and also two moverness conditions $\forall\tau_{i=1..n}\forall\langle\tau^{cmt}, \ell_{\tau'}\rangle \in \ell_{sh}: \tau^{cmt} > \tau_i \Rightarrow \ell_{\tau_i} \overline{\triangleright} \ell_{\tau'}$ and $\forall\tau_{i=1..n}\forall\tau_{j=1..i-1}: \ell_{\tau_i} \overline{\triangleright} \ell_{\tau_j}$. If the rule is applied, it changes $\mathcal{M}$ to $\mathcal{M}' = \mathcal{M}[\tau_i \mapsto \text{c}]_{i=1..n}$. According to the first condition, to commit a transaction, the dependency graph should be searched for a cluster containing the transaction. If the cluster search succeeds in finding a cluster, the collective commit algorithm is executed on the found cluster to check moverness conditions.

Cluster Search: A cluster is a set of terminated transactions whose dependencies are all to members of that same cluster or to committed transactions. A cluster search inputs a terminated transaction τ, and outputs either the smallest cluster that contains τ, or reports that no such cluster exists, or reports that τ must abort. We are looking for the smallest cluster because in a later phase we will have to order them, which is a time-consuming task. The smallest cluster is necessarily a strongly connected component (SCC) so we do cluster search with Tarjan's algorithm [29] for identifying SSCs. The idea is to gradually expand a candidate set of transactions containing τ until the candiate set is a cluster or the algorithm reports that no such clusters exists or that τ must abort. Specifically, if we have a candidate set and a dependency $\tau_r \curvearrowright \tau_s$, where τ_r is a member of the candidate set, then the cluster search does a case analysis of τ_s. If τ_s is:

- Terminated: we add τ_s to the candidate set.
- Committed: we do nothing, since the dependency is resolved.
- Running: we report that no such cluster exists.
- Aborted: we report that τ must abort.

If the Tarjan algorithm finds only one SCC, a cluster containing τ is found. On the other hand, if more than one SCC is found, the last SCC (that contains τ) is dependent on other SCCs. It is not a cluster before the other SCCs commit. Therefore, we report that no such cluster exists. (If more than one SCC is found, it is still possible to commit them. They can be committed in the order that they are found by Tarjan algorithm. This is because, the first SCC that is found is a cluster and also any SCC in the found sequence will be a cluster if the SCCs before it in the sequence are committed. But for simplicity, the current transaction waits for other SCCs to finalize.)

After the cluster search, we take one of three actions depending on the output. (1) if a cluster containing τ is found, then we commit all the transactions in the cluster; (2) if the result is that no such cluster exists, then we cache that information to avoid needlessly doing the search again before the graph changes: the thread running τ goes to the waiting state; and (3) if the result is that τ must abort, then we abort τ.

Although a transaction may wait after termination to be notified by other transactions, the implementation satisfies finalization, the progress property that we define as follows. We define that a transaction is finalized iff it is aborted or committed.

We define that a transaction is settled iff it is terminated and it is not transitively dependent on a running transaction. The finalization property is that every settled transaction is eventually finalized.

Collective Commit: To commit a set of transactions, it should be checked that there exists an order of commitment of the transactions where earlier transactions in the order do not invalidate later transactions in the order. This check corresponds to the condition $\forall\tau_{i=1..n}\forall\tau_{j=1..i-1}: \ell_{\tau_i} \overline{\triangleright} \ell_{\tau_j}$ that requires an order of transactions where operations of later transactions in the order are right movers in respect to operations of earlier transactions. In TL2, a write to a location invalidates a read from the same location. Therefore, an order is required where for each location, the reading transaction comes before the writing transaction. This condition is implemented as follows. A graph of transactions is made where a transaction τ_r has an edge to transaction τ_w if the read set of τ_r has an intersection with the write set of τ_w. If there is a cycle in the graph, a desired order does not exist. In this case, the current transaction starts abortion. Otherwise, it is possible to commit the transactions of the cluster together. Note that a pure write (writing to a location without reading it) does not conflict with another pure write and any order of commitment is valid for them. The lock for each location in the write sets of all the transactions is acquired. The global counter is incremented and is read as the write version. The read set of each transaction in the cluster is validated. This validation corresponds to the condition $\forall\tau_{i=1..n}\forall\langle\tau^{cmt}, \ell_{\tau'}\rangle \in \ell_{sh}: \tau^{cmt} > \tau_i \Rightarrow \ell_{\tau_i} \overline{\triangleright} \ell_{\tau'}$. If one of the locks cannot be acquired or a read set is not validated, the acquired locks are released and the current transaction is aborted. Otherwise, collective commit can be done. The write sets of the transactions are written to memory with the write version. The acquired locks are released. The state of the descriptor of each transaction is set to committed. Each transaction other than τ_s is notified of commitment. This notification makes a Commitment event. Each transaction that is committed sends dependency resolution notification to all notifiables $\{N_{i=1..n}\}$ that are registered to its descriptor. Each N_i references a receiving transaction τ_{r_i}. The notification makes a Dependency Resolution event for τ_{r_i}, if it is waiting. When a transaction is committed, the messages that it has sent become stable. Therefore, they can be received by receives that are executed outside transactions. Each transaction that is committed desuspends the transactors that it has sent a message to and are suspended on receives that are executed out of transactions.

6. Experimental Results

6.1. Benchmarks and Platform

We experiment with three benchmarks: A server benchmark and two benchmarks from STAMP [23]. We adopt the Server benchmark that is independently explained by [20] as the Vacation Reservation, by [14] as the Server Loop programming idiom and by [21] as the Job Handling system. A server thread handles requests from client threads. Each request should appear to be handled atomically i.e. the handling code of the server is a transaction. In addition, the request of the client thread may be sent inside a transaction. The transaction of a client may request the service multiple times. We experiment with two instances of this benchmark.

The service can simply be provision of unique ids [14]. A generic function (`serverLoop`) is offered in [14] to create servers. Employing Transactors, we provide a generic class (`Server`) that can be extended to create servers. The pseudo code of `Server` can be found in the technical report [17] section 15.4. We compare the message passing performance of our two implementations of Transactors with the implementation of TE for ML on a Server instance that generates unique ids. To the best of our knowledge, TE for ML is the closest semantics with similar goals. (We programmed and tried to conduct comparisons on other cases such as barrier, but the implementation of TE for ML took a very long time or deadlocked on these cases.)

As a tangible application of this programming idiom, consider a web application with two tiers: the application logic tier and the database tier. The system may be organized such that separate threads run the two tiers. The case study in [4] showed that to speed up handling future requests, the application logic tier may cache some of the data that it sends to the database tier. The application tier updates the cached data in the data structures and the database tier updates the data in the database. Although the updates are performed by different threads, they should be done atomically; either both or none should be seen by other threads.

We adopt the method suggested by [4] to unify memory and database transactions. The approach benefits form handlers that are registered to be run at different points of the transaction lifecycle. We extended our library to support registration of handlers for both of the implementations. We experiment with the authorship database scheme from [4]. We consider inserting a new paper info including its authors. Using our library, we define application logic transactor and database server transactor. The application logic transactor starts a transaction, sends an update request to the database server transactor, performs updates to the data structures and finishes the transaction after receiving an acknowledge message from the database server transactor. Upon receipt of a request, the database server transactor, executes a transaction comprised of queries to update data in the database and sends back an acknowledge message. The two transactions are interdependent and are collectively committed. (Note that if writing to the database is only to maintain a log for later accesses, the application logic transactor does not need to wait for the acknowledge message. In this case, only the database transaction is dependent on the application logic transaction and therefore, the application logic transaction can commit before the database transaction is done.) We study the overhead of cluster search and collective commit on this case.

To study the overhead of transactions supported by Transactors over pure transactions, we have adopted Kmeans clustering and Genome sequencing benchmarks from the Stanford transactional benchmark suite [23] and have programmed them in Scala using our Transaction and Transactors libraries.

The experiments are done on Intel(R) Core(TM)2 Duo CPU T7250 @2.00GHz and Linux 2.6.31-21-generic #59-Ubuntu. Scala version is 2.7.7.final (Oracle Java HotSpot(TM) Server VM, Java 1.6.0_17). TE for ML patch is on OCaml 3.08.1. Oracle MySQL version is 14.14 distribution 5.1.41. The database connector is MySQL Connector/J v.5.1.13. All the reported numbers are after warmup and are averages of results from repeated experiments.

6.2. Measurements

Message Passing Performance The first experiment compares the performance of the unique id generator server in Transactors and in TE for ML over different number of repetitions of the client transaction. The same thread repeats the client transaction. (New threads are not launched for each repetition.) In this experiment, the number of requests of the client transaction is constant (equal to 2). Performance ratio represents the performance of Transactors divided by the performance of TE for

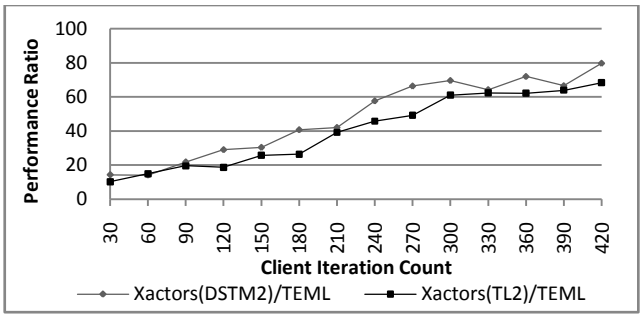

Figure 8. Server – Performance over Client Iteration Count

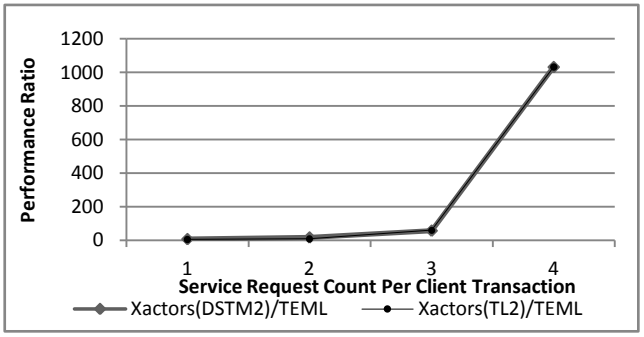

Figure 9. Server – Performance over Service Request Count

ML. The two lines in Figure 8 show the performance ratio of the two implementations of Transactors over the implementation of TE for ML. The performance ratio increases with the number of client iterations.

The second experiment compares the performance of the server case over different number of requests of the client transaction. In this experiment, the number of repetitions of the client transaction is constant (equal to 40). Figure 9 shows the performance ratio of each of the implementations of Transactors over the implementation of TE for ML. As the number of requests increase, the performance ratio grows fast. (The two curves overlap at this scale.)

Overhead of Cluster Search and Collective Commit In this experiment, the application logic transactor maintains the set of papers and the map of each author to her set of papers. Upon addition of a new paper, the application logic transactor updates the papers set and the author-to-papers map. The database transactor inserts a row to the Paper table, gets the unique id assigned to the paper and for each author, inserts a row to the PaperAuthor table. We measure the time of the application logic transaction for insertion of a paper with four authors. Table 1 shows the percent of time that is spent in the cluster search and collective commit procedures.

Overhead over Pure Transactions Atomic blocks of Transactors provide opacity just like atomic blocks of basic memory transactions. Therefore, Transactors can be used wherever basic transactions are used. But as Transactors support communication, there is an overhead. We study this overhead on

Table 1. Percent of Total Time Spent in Cluster Search and Collective Commit

	Cluster Search	Collective Commit
Xactors (DSTM2)	2.5	8.6
Xactors (TL2)	3.6	19.3

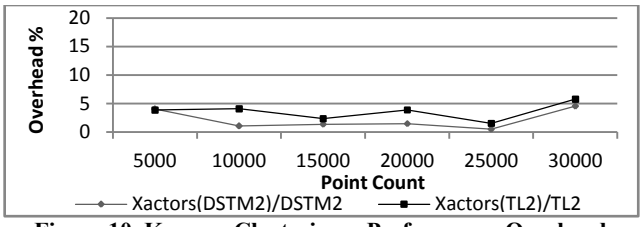

Figure 10. Kmeans Clustering – Performance Overhead

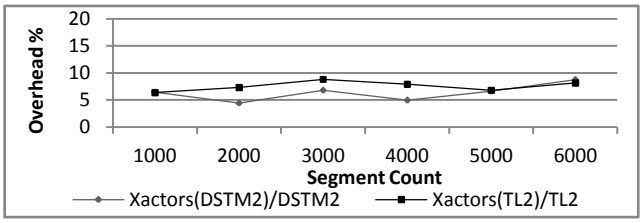

Figure 11. Genome Sequencing – Performance Overhead

Kmeans clustering and Genome sequencing benchmarks. Each of our implementations of Transactors is based on an implementation of memory transactions. We compare the performance of each implementation of Transactors over the implementation of the memory transactions that it is based on. The performance overhead for the Kmeans and Genome cases over different input sizes is shown respectively in Figure 10 and Figure 11. The experiments show that the overhead is below ten percent.

6.3. Assessment

Message Passing Performance In the first experiment, the performance ratio increases with the number of client iterations. This is because Transactors use a constant number of threads. On the other hand in TE for ML, to support the completeness property, when a thread receives on a channel, every message that has been sent to the channel should be tried by a search thread. As the messages that are sent to a channel increase, the number of search threads for a receive statement increases and affects performance.

In the second experiment, in the executions with more requests in the client transaction, more messages are sent to the server channel. As mentioned for the first experiment, in TE for ML, increase in the number of messages that are sent to a channel affects performance of receive statements on the channel. Furthermore, for clients that send more requests, more `chooseEvt` statements are executed at the server thread. The number of search threads that reach a `chooseEvt` statement are doubled to try each branch. In effect, the exponential number of search threads aggravates the performance of TE for ML.

As mentioned before, TE for ML is inherently inefficient as its semantics requires finding the successful matching which is NP-hard. The measurements indicate that Transactors provide up to a thousand times faster communication than TE for ML.

Overhead of Cluster Search and Collective Commit The overhead in the implementation based on DSTM2 is relatively low. The overhead of the collective commit procedure in the implementation based on TL2 is relatively high due to the time consuming procedure of checking existence of an order of commitment that respects moverness. This procedure is the hot spot to be optimized.

Overhead over Pure Transactions In our implementations, special care is devoted to optimization of the paths that are passed by transactions that do not send or receive messages. The

measurements suggest that Transactors add less than ten percent overhead to non-communicating transactions.

7. Conclusion

This paper presents CMT that defines the semantics of transactional communication. The usefulness of CMT is shown by expressing three fundamental communication idioms. It is proved that the semantics satisfies opacity and communication safety. The semantics is implemented on top of two implementations of memory transactions. The experiments show that the implementations provide considerably efficient communication and add low overhead to non-communicating transactions.

8. References

[1] Abadi, M., Birrell, A., Harris, T., and Isard, M. 2008. Semantics of transactional memory and automatic mutual exclusion. SIGPLAN Not. 43, 1 (Jan. 2008), 63-74.

[2] Agha, Gul A. ACTORS: A Model of Concurrent Computation in Distributed Systems. MIT Press, Cambridge, Massachusetts, 1986.

[3] Aguilera, M. K., Merchant, A., Shah, M., Veitch, A., and Karamanolis, C. 2007. Sinfonia: a new paradigm for building scalable distributed systems. In Proc. of SOSP '07. 159-174.

[4] Dias, R. J. and Lourenco, J. M.. 2009. Unifying Memory and Database Transactions. In Proc. of Euro-Par '09

[5] Dice, D., Shalev O., and Shavit N. Transactional locking II. In DISC'06, volume 4167 of Lecture Notes in Computer Science. Springer, 2006.

[6] Donnelly, K. and Fluet, M. 2008. Transactional events. J. Functional Programming. 18, 5-6 (Sep. 2008), 649-706.

[7] Dudnik P. and Swift, M. M. Condition Variables and Transactional Memory: Problem or Opportunity? In Proc. of TRANSACT'09.

[8] Effinger-Dean, L., Kehrt, M., and Grossman, D. 2008. Transactional events for ML. In Proc. of ICFP '08. 103-114.

[9] Gray J. Reuter A. 1992. Transaction Processing: Concepts and Techniques (1st ed.). Morgan Kaufmann Publishers Inc., San Francisco, CA, USA.

[10] Guerraoui, R. and Kapalka, M. 2008. On the correctness of transactional memory. In Proc. of PPoPP '08. 175-184.

[11] Harris, T. and Fraser, K. 2003. Language support for lightweight transactions. SIGPLAN Not. 38, 11 (Nov. 2003), 388-402.

[12] Harris, T., Marlow, S., Peyton-Jones, S., and Herlihy, M. 2005. Composable memory transactions. In Proc. of PPoPP '05. 48-60.

[13] Herlihy, M., Luchangco, V., and Moir, M. 2006. A flexible framework for implementing software transactional memory. In Proc. of OOPSLA '06. 253-262.

[14] Kehrt, M., Effinger-Dean L., Schmitz M., Grossman D. Programming Idioms for Transactional Events. PLACES 2009.

[15] Koskinen, E., Parkinson, M., and Herlihy, M. 2010. Coarse-grained transactions. In Proc. of POPL '10. 19-30.

[16] Lampson, B. W. and Redell, D. D. 1980. Experience with processes and monitors in Mesa. Commun. ACM 23, 2 (Feb. 1980), 105-117.

[17] Lesani, M. and Palsberg J. Communicating Memory Transactions. Technical report, 2010. http://www.cs.ucla.edu/~lesani/papers/CommMemTrans.pdf

[18] Lipton, R. J. 1975. Reduction: a method of proving properties of parallel programs. Commun. ACM 18, 12 (Dec. 1975), 717-721.

[19] Liskov, B. 1988. Distributed programming in Argus. Commun. ACM 31, 3 (Mar. 1988), 300-312.

[20] Luchangco, V. and Marathe, V. J. Transaction Synchronizers. In Proc. of SCOOL'05.

[21] Luchangco, V. and Marathe, V. J. You are not alone: breaking transaction isolation. In Proc. of IWMSE '10. 50-53.

[22] Luchangco, V. and Marathe, V. J. Transaction Communicators: Enabling Cooperation Among Concurrent Transactions. In Proc. of PPoPP'11.

[23] Minh, C. C., Chung, J., Kozyrakis, C., Olukotun K. STAMP: Stanford Transactional Applications for Multi-Processing. In Proc. of IISWC '08.

[24] Moore, K. F. and Grossman, D. 2008. High-level small-step operational semantics for transactions. In Proc. of POPL '08. 51-62.

[25] Odersky, M. The Scala Language Specification. 2010. Programming Methods Laboratory. EPFL.

[26] Reppy, J. H. 1999 Concurrent Programming in ML. Cambridge University Press.

[27] Scott, M. L. Sequential specification of transactional memory semantics. In Proc. of TRANSACT'06.

[28] Smaragdakis, Y., Kay, A., Behrends, R., and Young, M. 2007. Transactions with isolation and cooperation. In Proc. of OOPSLA '07. 191-210.

[29] Tarjan, Robert, 1971. Depth-first search and linear graph algorithms. In Proc. of the 12th Annual Symposium on Switching and Automata Theory (13-15 Oct. 1971).,114-121.

[30] Ziarek, L., Schatz, P., and Jagannathan, S. 2006. Stabilizers: a modular checkpointing abstraction for concurrent functional programs. In Proc. of ICFP '06. 136-147.

9. Appendix

The semantics uses a notion of right moverness [18] that we define here. Let Σ denote all the possible states of the store σ_{sh}. Let R denote the set of registers. For each $r \in R$, let $M_r = \{read, write\}$ denote the set of methods of r. For $r \in R$, $\sigma_1, \sigma_2 \in \Sigma$ and $m \in M_r$, let $\sigma_1 \xrightarrow{v \leftarrow r.m} \sigma_2$ denote the state transition from σ_1 to σ_2 by calling m on r that returns value v. Right moverness is defined as follows:

$\forall r_1, r_2 \in O, m_1 \in M_{r_1}, m_2 \in M_{r_2}$:

$r_1.m_1 \rhd r_2.m_2 \equiv \forall \sigma_1, \sigma_2, \sigma_3, \sigma_4 \in \Sigma$:

$$\left(\left(\sigma_1 \xrightarrow{v_1 \leftarrow r_1.m_1} \sigma_2 \; and \; \sigma_1 \xrightarrow{v_2 \leftarrow r_2.m_2} \sigma_3 \xrightarrow{v_1' \leftarrow r_1.m_1} \sigma_4\right) \Rightarrow (v_1 = v_1')\right)$$

According to the above definition, the right moverness relations are:

$\forall r_1, r_2 \in R, m_1, m_2 \in M_R: (r_1 \neq r_2) \Rightarrow (r_1.m_1 \rhd r_2.m_2)$

$r.read \rhd r.read$

$r.write \rhd r.read$

$r.write \rhd r.write$

Note that $r.read \rhd r.write$ is not correct.

Now we define right moverness for sequences of method calls. Let l denote a sequence of method calls on registers R (that is $l = v_1 \leftarrow r_1.m_1, \dots, v_n \leftarrow r_n.m_n$). Let $l_1 :: l_2$ denote the concatenation of the two sequences l_1 and l_2. Let $l[i]$ denote the ith method call in the sequence l. Let $l[1..i]$ denote the sequence of the first i method calls in the sequence l. Let $\sigma_1 \xrightarrow{l} \sigma_2$ denote multiple step transitions by l. That is if $l = v_1 \leftarrow r_1.m_1, \dots, v_n \leftarrow r_n.m_n$ then $\sigma_1 \xrightarrow{l} \sigma_n \Leftrightarrow \sigma_1 \xrightarrow{v_1 \leftarrow r_1.m_1} \sigma_2 \dots \sigma_{n-1} \xrightarrow{v_n \leftarrow r_n.m_n} \sigma_n$. Lifted right moverness is defined as follows: If $l_1 = v_1 \leftarrow r_1.m_1, \dots, v_n \leftarrow r_n.m_n$ and l_2 are two sequences of methods then

$l_1 \overline{\rhd} l_2 \equiv \forall i = 1..n: \forall \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5 \in \Sigma$:

$$\left(\left(\sigma_1 \xrightarrow{l_1[1..i-1]} \sigma_2 \xrightarrow{v_i \leftarrow r_i.m_i} \sigma_3 \; and \; \sigma_1 \xrightarrow{l_2 :: l_1[1..i-1]} \sigma_4 \xrightarrow{v_i' \leftarrow r_i.m_i} \sigma_5\right) \Rightarrow (v_i = v_i')\right)$$

Note that although $r.read \rhd r.write$ is not correct, $r.write, r.read \; \overline{\rhd} \; r.write$ is correct.

Technical Report

10. Properties

10.1. Opacity

10.1.1. Definitions

DEFINITION 3: $Trace$ of a sequence of reductions by $\rightarrow_o$:
Intuitively, $Trace$ of a sequence of reductions by $\rightarrow_o$ is the sequence of labels of the reductions.
$Trace(Conf_1^o) = \cdot$
$Trace\left(Conf_1^o \xrightarrow{l}_o Conf_2^o\right) = Label\left(Conf_1^o \xrightarrow{l}_o Conf_2^o\right)$
$Trace\left(Conf_1^o \xrightarrow{l_1}_o Conf_2^o \xrightarrow{l_2}_o \dots \xrightarrow{l_{n-1}}_o Conf_n^o\right) =$
$\quad Trace\left(Conf_1^o \xrightarrow{l_1}_o Conf_2^o \xrightarrow{l_2}_o \dots \xrightarrow{l_{i-1}}_o Conf_i^o\right), Trace\left(Conf_i^o \xrightarrow{l_i}_o Conf_{i+1}^o \xrightarrow{l_{i+1}}_o \dots \xrightarrow{l_{n-1}}_o Conf_n^o\right)$
$Label\left(Conf_1^o \xrightarrow{\perp}_o Conf_2^o\right) = \cdot$
$Label\left(Conf_1^o \xrightarrow{\langle\tau,\text{beg}\rangle}_o Conf_2^o\right) = \langle\tau, \text{beg}\rangle$
$Label\left(Conf_1^o \xrightarrow{\langle\tau,o.m\rangle}_o Conf_2^o\right) = \langle\tau, o.m\rangle$
$Label\left(Conf_1^o \xrightarrow{\langle\tau,\text{cmt}\rangle}_o Conf_2^o\right) = \langle\tau, \text{cmt}\rangle$
$Label\left(Conf_1^o \xrightarrow{\langle\tau,\text{abt}\rangle}_o Conf_2^o\right) = \langle\tau, \text{abt}\rangle$

DEFINITION 4: $Trace_{MT}$ of a sequence of reductions by $\rightarrow$:
Intuitively, $Trace_{MT}$ of a sequence of reductions by $\rightarrow$ is the sequence of labels of the reductions except send and receive labels.
$Trace_{MT}(Conf_1) = \cdot$
$Trace_{MT}\left(Conf_1 \xrightarrow{l} Conf_2\right) = Label_{MT}\left(Conf_1 \xrightarrow{l} Conf_2\right)$
$Trace_{MT}\left(Conf_1 \xrightarrow{l_1} Conf_2 \xrightarrow{l_2} \dots \xrightarrow{l_{n-1}} Conf_n\right) =$
$\quad Trace_{MT}\left(Conf_1 \xrightarrow{l_1} Conf_2 \xrightarrow{l_2} \dots \xrightarrow{l_{i-1}} Conf_i\right), Trace_{MT}\left(Conf_i \xrightarrow{l_i} Conf_{i+1} \xrightarrow{l_{i+1}} \dots \xrightarrow{l_{n-1}} Conf_n\right)$
$Label_{MT}\left(Conf_1 \xrightarrow{\perp} Conf_2\right) = \cdot$
$Label_{MT}\left(Conf_1 \xrightarrow{\langle\tau,\text{beg}\rangle} Conf_2\right) = \langle\tau, \text{beg}\rangle$
$Label_{MT}\left(Conf_1 \xrightarrow{\langle\tau,o.m\rangle} Conf_2\right) = \langle\tau, o.m\rangle$
$Label_{MT}\left(Conf_1 \xrightarrow{\langle\tau_1,\text{cmt}\rangle\dots\langle\tau_n,\text{cmt}\rangle} Conf_2\right) = \langle\tau_1, \text{cmt}\rangle, \dots, \langle\tau_n, \text{cmt}\rangle$
$Label_{MT}\left(Conf_1 \xrightarrow{\langle\tau,\text{abt}\rangle} Conf_2\right) = \langle\tau, \text{abt}\rangle$
$Label_{MT}\left(Conf_1 \xrightarrow{\langle\tau,\text{ch send}\rangle} Conf_2\right) = \cdot$
$Label_{MT}\left(Conf_1 \xrightarrow{\langle\tau_1,\text{ch receive}\rangle} Conf_2\right) = \cdot$

DEFINITION 5: Object $rand$ is a stateless random value generator[1] with a single method $gen()$.
The method $gen()$ is semantically right mover to methods of any object and methods of any object are right mover to it.
$\forall o, m: rand.gen \triangleright o.m$
$\forall o, m: o.m \triangleright rand.gen$

DEFINITION 6:
We define that two sets (or sequence of) methods are equivalent ($\equiv$) iff the difference of the two is only calls to method gen of $rand$ object.
Formally:
$\ell_1 \equiv \ell_2 \Leftrightarrow [(\ell_1/\ell_2) \cup (\ell_2/\ell_1) \subseteq \{rand.gen\}]$

[1] A stateless random value generator can generate different values according for example to the time that it is called and state of other objects in the memory.

The definition can also be lifted to commit sequences.
$\langle \tau^{cmt}, \ell_1 \rangle \equiv \langle \tau^{cmt}, \ell_2 \rangle \Leftrightarrow \ell_1 \equiv \ell_2$
$\ell_{sh_1} :: \langle \tau^{cmt}, \ell_1 \rangle \equiv \ell_{sh_2} :: \langle \tau^{cmt}, \ell_2 \rangle \Leftrightarrow \left[\left(\ell_{sh_1} \equiv \ell_{sh_2} \right) and \ (\ell_1 \equiv \ell_2) \right]$

LEMMA 1:
$\ell_1 \equiv \ell_2 \Leftrightarrow [\forall \ell_3 : \ell_3 \sqsupset \ell_2 \Rightarrow \ell_3 \sqsupset \ell_1 \ and \ \forall \ell_3 : \ell_2 \sqsupset \ell_3 \Rightarrow \ell_1 \sqsupset \ell_3]$
PROOF:
Direct from DEFINITION 5 (that $rand$ is statelesss) and DEFINITION 6.

LEMMA 2:
$\ell_1 \equiv \ell_2 \Leftrightarrow [\mathrm{merge}(\sigma, \ell_1) = \mathrm{merge}(\sigma, \ell_2)]$
PROOF:
Direct from DEFINITION 6 and that DEFINITION 5 (that $rand$ is stateless).

DEFINITION 7: We define the transformation function F on statements as follows:
$F(i; s) \triangleq F(i); F(s)$
$F(\mathrm{beg}) \triangleq \mathrm{beg}$
$F(x \coloneqq o.m) \triangleq x \coloneqq o.m$
$F(\mathrm{end}) \triangleq end$
$F(c) \triangleq c$
$F(x \coloneqq ch\ receive) \triangleq x \coloneqq rand.gen()$
$F(ch\ send\ e) \triangleq x \coloneqq x$
$F(\bot) = \bot$

DEFINITION 8:
Transactions:
"Every transaction has a unique identifier from a set, $Trans = \{T_1, T_2, \ldots\}$. Every transaction is initially live and may eventually become either committed or aborted" PPoPP'08

DEFINITION 9:
Transaction History:
"History is the sequence of all invocation and response events that were issued and received by transactions in a given execution." PPoPP'08
"$H \mid T_i$ denotes the longest subsequence of history H that contains only events executed by transaction T_i." PPoPP'08
$H \mid o$ denotes the longest subsequence of history H that contains only operations on object o.
$H \,/\, o$ denotes the longest subsequence of history H that does not contains operations on object o.
"$H \cdot H'$ denotes the concatenation of histories H and H'." PPoPP'08
"We say that a transaction T_i is in history H, and write $T_i \in H$, if $H \mid T_i$ is a non-empty sequence." PPoPP'08
A history is well-formed if for each transaction T_i, no event follows commit or abort event in $H \mid T_i$.

DEFINITION 10:
Equivalence of Histories:
"We say the histories H and H' are equivalent and write $H \equiv H'$, if, for every transaction $T_i \in Trans$, $H \mid T_i = H' \mid T_i$." PPoPP'08

DEFINITION 11:
Happen-before Relation:
"For every history H, relation $\prec_H$ is the partial order on the transactions in H, such that, for any two transactions $T_i, T_j \in H$, if T_i is completed and the first event of T_j follows the last event of T_i in H, then $T_i \prec_H T_j$." PPoPP'08
Concurrent Transactions:
"We say that transactions $T_i, T_j \in H$ are concurrent in history H if they are not ordered by the happen-before relation $\prec_H$, i.e., if $T_i \not\prec_H T_j$ and $T_j \not\prec_H T_i$." PPoPP'08
Preservation of Real-time Order:
"We say that a history H' preserves the real-time order of a history H, if $\prec_H \subseteq \prec_{H'}$. That is, if $T_i \prec_H T_j$, then $T_i \prec_{H'} T_j$, for any two transactions T_i and T_j in H." PPoPP'08

DEFINITION 12:
Sequential History:
"A (well-formed) history H is sequential if no two transactions in H are concurrent." PPoPP'08
(That is for each pair of transactions $T_i, T_j \in H$, either $T_i \prec_H T_j$ or $T_j \prec_H T_i$.)

DEFINITION 13:
Complete Transaction:
"We say that a history H is complete if H does not contain any live transaction." PPoPP'08
Complete histories set:
A history H' is in $Complete(H)$ if H' is well-formed and every transaction that is live in H is aborted in H'.

DEFINITION 14:
All-committed sequential history:
A sequential history S is all-committed, if all the transactions of S except possibly the last one are committed.
Filtered history:
Filtered history for transaction T_i in a sequential history S is the largest subsequence S' of S such that for every transaction $T_j \in S'$, either (1) $j = i$ or (2) T_j is committed in S and $T_j \prec_S T_i$. A filtered history is an all-committed history.

DEFINITION 15:
Legal histories and transactions:
An all-committed sequential history S is legal if for each o, $S \mid o \in Seq(o)$. (where $Seq(o)$ denotes sequential specification of o)

DEFINITION 16:
A transaction in a sequential history S is legal if the filtered history for T_i in S is legal.

DEFINITION 17:
Opacity:
"A history H is opaque if there exists a sequential history S equivalent to some history in $Complete(H)$, such that
(1) S preserves the real-time order of H, and (2) every transaction $T_i \in S$ is legal in S." PPoPP'08

10.1.2. Property Statement

THEOREM 2 (Opacity). Every sequence of labels $\langle \tau, \text{beg} \rangle$, $\langle \tau, o.m \rangle$, $\langle \tau, \text{abt} \rangle$ and $\langle \tau, \text{cmt} \rangle$ given by $\rightarrow$ started from $Conf_0$ is opaque.
Formally:
If
$Exec = Conf_0 \rightarrow \cdots \rightarrow Conf_n$ $(Eq.1)$
$Trace_{MT}(Exec) = L$ $(Eq.2)$
then
L is opaque.

Proof:
By LEMMA 3 on
$Eq.1$
$Eq.2$
it is concluded that
$\exists Exec'$
$Exec' = Conf_0^o \rightarrow_o \ldots \rightarrow_o Conf_m^o$ $(Eq.3)$
$Trace(Exec') \,/\, rand = L$ $(Eq.4)$

We define
$L' = Trace(Exec')$ $(Eq.5)$

From
$Eq.4$
$Eq.5$
it is concluded that
$L = L' \,/\, rand$ $(Eq.6)$

By THEOREM 1 on
$Eq.3$
$Eq.5$
it is concluded that
L' is opaque. $(Eq.7)$

By LEMMA 6 on
$Eq.7$

$Eq.6$
it is concluded that
L is opaque.

10.1.3. Helper lemmas

THEOREM 1 (Opacity). Every sequence of labels $\langle \tau, \text{beg} \rangle$, $\langle \tau, o.m \rangle$, $\langle \tau, \text{abt} \rangle$ and $\langle \tau, \text{cmt} \rangle$ given by $\rightarrow_o$ started from $Conf_0^o$ is opaque
Formally:
If
$Exec = Conf_0^o \rightarrow_o Conf_1^o \rightarrow_o \dots \rightarrow_o Conf_n^o$
$Trace(Exec) = L$
then
L is opaque.
Proposition 6.2 of [15]

LEMMA 3:
If
$Exec = Conf_0 \rightarrow \cdots \rightarrow Conf_n \quad (Eq:1)$
$Trace_{MT}(Exec) = L \quad (Eq:2)$
then
$\exists Exec'$
$Exec' = Conf_0^o \rightarrow_o \dots \rightarrow_o Conf_m^o$
$Trace(Exec') \,/\, rand = L$

PROOF:
By definition
$Conf_0 = \langle \mathcal{T}_0 \cdot \sigma_{sh_0} \cdot [] \cdot \emptyset \cdot \emptyset \cdot \emptyset \rangle \quad (Eq:3)$
$\mathcal{T}_0 = \langle \bot, P_i, \sigma_{sh_0}, \sigma_{sh_0}; stmt \mapsto \bot, [] \rangle_{i=1..k} \quad (Eq:4)$

We define
$Conf_0^o = \langle \mathcal{T}_0^o \cdot \sigma_{sh_0} \cdot [] \rangle \quad (Eq:5)$
$\mathcal{T}_0^o = \langle \bot, F(P_i), \sigma_{sh_0}, \sigma_{sh_0}; stmt \mapsto \bot, [] \rangle_{i=1..k} \quad (Eq:6)$
$Conf_n = \langle \mathcal{T}_n \cdot \sigma_{sh_n} \cdot \ell_{sh_n} \cdot \mathcal{M}_n \cdot \mathcal{C}_n \cdot \mathcal{D}_n \rangle \quad (Eq:7)$

It is trivial that
$[] \equiv [] \quad (Eq:8)$

From
$Eq:4$
$Eq:6$
$Eq:8$
$F(\bot) = \bot$
it is concluded that
$\forall i$:
$\langle \tau', s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_i \in \mathcal{T}_0 \Rightarrow$
$[\langle \tau', F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_i \in \mathcal{T}_0^o \; and \; \ell'_\tau \equiv \ell_\tau \; and \; (\tau' = \bot \Rightarrow \ell'_\tau = [\quad])] \quad (Eq:9)$

By LEMMA 4 on
$Eq:1$
$Eq:2$
$Eq:3$
$Eq:7$
$Eq:5$
$Eq:9$
$Eq:8$
it is concluded that
$\exists Conf_m^o$:
$Conf_m^o = \langle \mathcal{T}_m^o \cdot \sigma_{sh_n} \cdot \ell_{sh_m}{}^o \rangle \quad (Eq:10)$
$Exec' = Conf_0^o \rightarrow_o \dots \rightarrow_o Conf_m^o \quad (Eq:11)$

$Trace(Exec') \,/\, rand = L$ $(Eq: 12)$

$\forall i$:

$\langle \tau', s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_i \in \mathcal{T}_n \Rightarrow$

$[\langle \tau', F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_i \in \mathcal{T}_m^o \; and \; \ell'_\tau \equiv \ell_\tau \; and \; (\tau' = \bot \Rightarrow \ell'_\tau = [\quad])]$ $(Eq: 13)$

$\ell_{sh_m}^{\;o} \equiv \ell_{sh_n}$ $(Eq: 14)$

The conclusion is:

$Eq: 11$

$Eq: 12$

LEMMA 4:

If

$Exec = Conf_1 \rightarrow \cdots \rightarrow Conf_n$ $(Eq: 1)$

$Trace_{MT}(Exec) = L$ $(Eq: 2)$

$Conf_1 = \langle \mathcal{T}_1 \cdot \sigma_{sh_1} \cdot \ell_{sh_1} \cdot \mathcal{M}_1 \cdot \mathcal{C}_1 \cdot \mathcal{D}_1 \rangle$ $(Eq: 3)$

$Conf_n = \langle \mathcal{T}_n \cdot \sigma_{sh_n} \cdot \ell_{sh_n} \cdot \mathcal{M}_n \cdot \mathcal{C}_n \cdot \mathcal{D}_n \rangle$ $(Eq: 4)$

$Conf_1^o = \langle \mathcal{T}_1^o \cdot \sigma_{sh_1} \cdot \ell_{sh_1}^{\;o} \rangle$ $(Eq: 5)$

$\forall i$:

$\langle \tau', s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_i \in \mathcal{T}_1 \Rightarrow$

$[\langle \tau', F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_i \in \mathcal{T}_1^o \; and \; \ell'_\tau \equiv \ell_\tau \; and \; (\tau' = \bot \Rightarrow \ell'_\tau = [\quad])]$ $(Eq: 6)$

$\ell_{sh_1}^{\;o} \equiv \ell_{sh_1}$ $(Eq: 7)$

then

$\exists Conf_m^o$:

$Conf_m^o = \langle \mathcal{T}_m^o \cdot \sigma_{sh_n} \cdot \ell_{sh_m}^{\;o} \rangle$

$Exec' = Conf_1^o \rightarrow_o \ldots \rightarrow_o Conf_m^o$

$Trace(Exec') \,/\, rand = L$

$\forall i$:

$\langle \tau', s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_i \in \mathcal{T}_n \Rightarrow$

$[\langle \tau', F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_i \in \mathcal{T}_m^o \; and \; \ell'_\tau \equiv \ell_\tau \; and \; (\tau' = \bot \Rightarrow \ell'_\tau = [\quad])]$

$\ell_{sh_m}^{\;o} \equiv \ell_{sh_n}$

PROOF:

Induction on the length of $Exec$

1. Base case:

Length of $Exec$ is zero.

$Exec = Conf_1$ $(Eq: C1.1)$

$Conf_1 = Conf_n$ $(Eq: C1.2)$

From

$Eq: 3$

$Eq: 4$

$Eq: C1.2$

it is concluded that

$\mathcal{T}_1 = \mathcal{T}_n$ $(Eq: C1.3)$

$\sigma_{sh_1} = \sigma_{sh_n}$ $(Eq: C1.4)$

$\ell_{sh_1} = \ell_{sh_n}$ $(Eq: C1.5)$

By DEFINITION 4 on $Eq: C1.1$

$Trace_{MT}(Exec) = \cdot$ $(Eq: C1.6)$

From

$Eq: 2$

$Eq: C1.6$

it is concluded that

$L = \cdot$ $(Eq: C1.7)$

We define

$Conf_m^o = \langle \mathcal{T}_m^o \cdot \sigma_{sh_m}^{\;o} \cdot \ell_{sh_m}^{\;o} \rangle$ $(Eq: C1.8)$

$Conf_m^o = Conf_1^o$ $(Eq: C1.9)$

From
$Eq: C1.9$
$Eq: 5$
$Eq: C1.8$
it is concluded that
$\mathcal{T}_1^o = \mathcal{T}_m^o$ $(Eq: C1.10)$
$\sigma_{sh_1} = \sigma_{sh_m}^o$ $(Eq: C1.11)$
$\ell_{sh_1}^o = \ell_{sh_m}^o$ $(Eq: C1.12)$

From
$Eq: C1.11$
$Eq: C1.4$
it is concluded that
$\sigma_{sh_m}^o = \sigma_{sh_n}$ $(Eq: C1.13)$

From
$Eq: 7$
$Eq: C1.12$
$Eq: C1.5$
it is concluded that
$\ell_{sh_m}^o \equiv \ell_{sh_n}$ $(Eq: C1.14)$

From
$Eq: C1.8$
$Eq: C1.13$
it is concluded that
$Conf_m^o = \langle \mathcal{T}_m^o \cdot \sigma_{sh_n} \cdot \ell_{sh_m}^o \rangle$ $(Eq: C1.15)$

We define
$Exec' = Conf_1^o$ (that is equal to $Conf_m^o$) $(Eq: C1.16)$

By DEFINITION 3 and $Eq. C1.16$:
$Trace(Exec') = \cdot$ $(Eq: C1.17)$

From
$Eq: C1.7$
$Eq: C1.17$
it is concluded that
$Trace(Exec') \; / \; rand = \; L$ $(Eq: C1.18)$

From
$Eq: 6$
$Eq: C1.3$
$Eq: C1.10$
it is concluded that
$\forall i$:
$\langle \tau', s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_i \in \mathcal{T}_n \Rightarrow$
$[\langle \tau', F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_i \in \mathcal{T}_m^o \; and \; \ell'_\tau \equiv \ell_\tau \; and \; (\tau' = \perp \Rightarrow \ell'_\tau = [\quad])]$ $(Eq: C1.19)$

The conclusion of this case is
$Eq: C1.15$
$Eq: C1.16$
$Eq: C1.18$
$Eq: C1.19$
$Eq: C1.14$

2. Inductive case:
Induction hypothesis:

If

$Exec = Conf_1 \to \cdots \to Conf_{n-1}$ $(Eq: 1)$

$Trace_{MT}(Exec) = L$ $(Eq: 2)$

$Conf_1 = \langle \mathcal{T}_1 \cdot \sigma_{sh_1} \cdot \ell_{sh_1} \cdot \mathcal{M}_1 \cdot \mathcal{C}_1 \cdot \mathcal{D}_1 \rangle$ $(Eq: 3)$

$Conf_{n-1} = \langle \mathcal{T}_{n-1} \cdot \sigma_{sh_{n-1}} \cdot \ell_{sh_{n-1}} \cdot \mathcal{M}_{n-1} \cdot \mathcal{C}_{n-1} \cdot \mathcal{D}_{n-1} \rangle$ $(Eq: 4)$

$Conf_1^o = \langle \mathcal{T}_1^o \cdot \sigma_{sh_1} \cdot \ell_{sh_1}^o \rangle$ $(Eq: 5)$

$\forall i$:

$\langle \tau', s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_i \in \mathcal{T}_1 \Rightarrow$

$[\langle \tau', F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_i \in \mathcal{T}_1^o \; and \; \ell'_\tau \equiv \ell_\tau \; and \; (\tau' = \perp \Rightarrow \ell'_\tau = [\quad])]$ $(Eq: 6)$

$\ell_{sh_1}^o \equiv \ell_{sh_1}$ $(Eq: 7)$

then

$\exists Conf_r^o$:

$Conf_r^o = \langle \mathcal{T}_r^o \cdot \sigma_{sh_{n-1}} \cdot \ell_{sh_r}^o \rangle$

$Exec' = Conf_1^o \to_o \ldots \to_o Conf_r^o$

$Trace(Exec') \; / \; rand = L$

$\forall i$:

$\langle \tau', s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_i \in \mathcal{T}_{n-1} \Rightarrow$

$[\langle \tau', F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_i \in \mathcal{T}_r^o \; and \; \ell'_\tau \equiv \ell_\tau \; and \; (\tau' = \perp \Rightarrow \ell'_\tau = [\quad])]$

$\ell_{sh_r}^o \equiv \ell_{sh_{n-1}}$

From

$Eq: 1$

it is concluded that

$Exec' = Conf_1 \to \cdots \to Conf_{n-1}$ $(Eq: C2.1)$

We define

$Conf_{n-1} = \langle \mathcal{T}_{n-1} \cdot \sigma_{sh_{n-1}} \cdot \ell_{sh_{n-1}} \cdot \mathcal{M}_{n-1} \cdot \mathcal{C}_{n-1} \cdot \mathcal{D}_{n-1} \rangle$ $(Eq: C2.2)$

$L_1 = Trace_{MT}(Exec')$ $(Eq: C2.3)$

$L_2 = Trace_{MT}(Conf_{n-1} \to Conf_n)$ $(Eq: C2.4)$

From DEFINITION 4 on

$Eq: C2.3$

$Eq: C2.4$

$Eq: 1$

$Eq: 2$

it is concluded that

$L = L_1, L_2$ $(Eq: C2.5)$

By induction hypothesis on

$Eq: C2.1$

$Eq: C2.3$

$Eq: 3$

$Eq: C2.2$

$Eq: 5$

$Eq: 6$

$Eq: 7$

it is concluded that

$\exists Conf_r^o$:

$Conf_r^o = \langle \mathcal{T}_r^o \cdot \sigma_{sh_{n-1}} \cdot \ell_{sh_r}^o \rangle$ $(Eq: C2.6)$

$Exec'' = Conf_1^o \to_o \ldots \to_o Conf_r^o$ $(Eq: C2.7)$

$Trace(Exec'') \; / \; rand = L_1$ $(Eq: C2.8)$

$\forall i$:

$\langle \tau', s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_i \in \mathcal{T}_{n-1} \Rightarrow$

$[\langle \tau', F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_i \in \mathcal{T}_r^o \; and \; \ell'_\tau \equiv \ell_\tau \; and \; (\tau' = \perp \Rightarrow \ell'_\tau = [\quad])]$ $(Eq: C2.9)$

$\ell_{sh_r}^o \equiv \ell_{sh_{n-1}}$ $(Eq: C2.10)$

By LEMMA 5 on

$Eq: C2.4$

$Eq: C2.2$

$Eq: 4$

$Eq: C2.6$
$Eq: C2.9$
$Eq: C2.10$

it is concluded that

$\exists Conf_m^o$:

$Conf_m^o = \langle \mathcal{T}_m^o \cdot \sigma_{sh_n} \cdot \ell_{sh_m}^{\ o} \rangle$ $(Eq: C2.11)$

$Exec''' = Conf_r^o \rightarrow_o \ldots \rightarrow_o Conf_m^o$ $(Eq: C2.12)$

$Trace(Exec''') \,/\, rand = L_2$ $(Eq: C2.13)$

$\forall i$:

$\langle \tau', s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_i \in \mathcal{T}_n \Rightarrow$

$[\langle \tau', F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_i \in \mathcal{T}_m^o \; and \; \ell'_\tau \equiv \ell_\tau \; and \; (\tau' = \perp \Rightarrow \ell'_\tau = [\quad])]$ $(Eq: C2.14)$

$\ell_{sh_m}^{\ o} \equiv \ell_{sh_n}$ $(Eq: C2.15)$

We define

$Exec'''' = Exec'', Exec'''$ $(Eq: C2.16)$

From

$Eq: C2.7$
$Eq: C2.12$
$Eq: C2.16$

it is concluded that

$Exec'''' = Conf_1^o \rightarrow_o \ldots \rightarrow_o Conf_r^o \rightarrow_o \ldots \rightarrow_o Conf_m^o$ $(Eq: C2.17)$

From

DEFINITION 3
$Eq: C2.16$
$Eq: C2.8$
$Eq: C2.13$

it is concluded that

$Trace(Exec'''') \,/\, rand = L_1, L_2$ $(Eq: C2.18)$

From

$Eq: C2.5$
$Eq: C2.18$

it is concluded that

$Trace_{MT}(Exec'''') \,/\, rand = L$ $(Eq: C2.19)$

The conclusion for this case is:

$Eq: C2.11$
$Eq: C2.17$
$Eq: C2.19$
$Eq: C2.14$
$Eq: C2.15$

LEMMA 5:

If

$Label_{MT}(Conf_1 \rightarrow Conf_2) = L$ $(Eq: 1)$

$Conf_1 = \langle \mathcal{T}_1 \cdot \sigma_{sh_1} \cdot \ell_{sh_1} \cdot \mathcal{M}_1 \cdot \mathcal{C}_1 \cdot \mathcal{D}_1 \rangle$ $(Eq: 2)$

$Conf_2 = \langle \mathcal{T}_2 \cdot \sigma_{sh_2} \cdot \ell_{sh_2} \cdot \mathcal{M}_2 \cdot \mathcal{C}_2 \cdot \mathcal{D}_2 \rangle$ $(Eq: 3)$

$Conf_1^o = \langle \mathcal{T}_1^o \cdot \sigma_{sh_1} \cdot \ell_{sh_1}{}' \rangle$ $(Eq: 4)$

$\forall i$:

$\langle \tau', s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_i \in \mathcal{T}_1 \Rightarrow$

$[\langle \tau', F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_i \in \mathcal{T}_1^o \; and \; \ell'_\tau \equiv \ell_\tau \; and \; (\tau' = \perp \Rightarrow \ell'_\tau = [\quad])]$ $(Eq: 5)$

$\ell_{sh_1}{}' \equiv \ell_{sh_1}$ $(Eq: 6)$

then

$\exists Conf_2^o$:

$Conf_2^o = \langle \mathcal{T}_2^o \cdot \sigma_{sh_2} \cdot \ell_{sh_2}{}' \rangle$

$Exec = Conf_1^o \rightarrow_o \ldots \rightarrow_o Conf_2^o$

$Trace(Exec)\ /\ rand = L$
$\forall i$:
$\langle \tau', s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_i \in \mathcal{T}_2 \Rightarrow$
$[\langle \tau', F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell_\tau' \rangle_i \in \mathcal{T}_2^o \ and \ \ell_\tau{}' \equiv \ell_\tau \ and \ (\tau' = \perp \Rightarrow \ell_\tau' = [\quad])]$
$\ell_{sh_2}{}' \equiv \ell_{sh_2}$

PROOF:
Case Analysis on $Conf_1 \rightarrow Conf_2$:

1. Case CMD:

We define j to be number of the thread that reduction is done in.

$\mathcal{T}_1 = \langle \tau, c; s, \sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau \rangle_j, \mathcal{T}$ $(Eq: C1.1)$
$\sigma_{sh_1} = \sigma_{sh}$ $(Eq: C1.2)$
$\ell_{sh_1} = \ell_{sh}$ $(Eq: C1.3)$
$\mathcal{T}_2 = \langle \tau, s, [\![c]\!]\sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau \rangle_j, \mathcal{T}$ $(Eq: C1.4)$
$\sigma_{sh_2} = \sigma_{sh}$ $(Eq: C1.5)$
$\ell_{sh_2} = \ell_{sh}$ $(Eq: C1.6)$

From DEFINITION 4
$Label_{MT}\left(Conf_1 \xrightarrow{\perp} Conf_2\right) = \cdot$ $(Eq: C1.7)$

From
$Eq: C1.1$
it is concluded that
$\langle \tau, c; s, \sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau \rangle_j \in \mathcal{T}_1$ $(Eq: C1.8)$

We define st to be the statement that $stmt$ is mapped to in $\overleftarrow{\sigma_\tau}$. Therefore, we have
$\overleftarrow{\sigma_\tau} = \overleftarrow{\sigma_\tau}'; stmt \mapsto st$ $(Eq: C1.9)$

From
$Eq: C1.8$
$Eq: C1.9$
it is concluded that
$\langle \tau, c; s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_j \in \mathcal{T}_1$ $(Eq: C1.10)$

From
$Eq: C1.10$
$Eq: 5$
it is concluded that
$\langle \tau, F(c; s'), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell_\tau' \rangle_j \in \mathcal{T}_1^o$ $(Eq: C1.11)$
$\ell_\tau' \equiv \ell_\tau \ and \ (\tau = \perp \Rightarrow \ell_\tau' = [\quad])$ $(Eq: C1.12)$

From DEFINITION 7, it is concluded that
$F(c; s') = c; F(s')$ $(Eq: C1.13)$

From
$Eq: C1.11$
$Eq: C1.13$
it is concluded that
$\langle \tau, c; F(s'), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell_\tau' \rangle_j \in \mathcal{T}_1^o$ $(Eq: C1.14)$

From
$Eq: C1.14$
it is concluded that $\mathcal{T}_1^o$ is of the form (there exists a $\mathcal{T}^o$ such that)
$\mathcal{T}_1^o = \langle \tau, c; F(s'), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell_\tau' \rangle_j, \mathcal{T}^o$ $(Eq: C1.15)$

From the rule $OCMD$, it is concluded that
$\langle \langle \tau, c; F(s'), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell_\tau' \rangle_j, \mathcal{T}^o \cdot \sigma_{sh} \cdot \ell_{sh_1}{}' \rangle \xrightarrow{\perp}_o$
$\langle \langle \tau, F(s'), [\![c]\!]\sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell_\tau' \rangle_j, \mathcal{T}^o \cdot \sigma_{sh} \cdot \ell_{sh_1}{}' \rangle$ $(Eq: C1.16)$

We define
$\mathcal{T}_2^o = \langle \tau, F(s'), [\![c]\!]\sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell_\tau' \rangle_j, \mathcal{T}^o$ $(Eq: C1.17)$
${\ell_{sh_2}}' = {\ell_{sh_1}}'$ $(Eq: C1.18)$
$Conf_2^o = \langle \mathcal{T}_2^o \cdot \sigma_{sh_2} \cdot {\ell_{sh_2}}' \rangle$ $(Eq: C1.19)$

From
$Eq: C1.16$
$Eq: C1.15$
$Eq: C1.2$
$Eq: C1.17$
$Eq: C1.5$
$Eq: C1.18$
it is concluded that
$\langle \mathcal{T}_1^o \cdot \sigma_{sh_1} \cdot {\ell_{sh_1}}' \rangle \overset{\perp}{\rightarrow}_o \langle \mathcal{T}_2^o \cdot \sigma_{sh_2} \cdot {\ell_{sh_2}}' \rangle$ $(Eq: C1.20)$

From
$Eq: C1.20$
$Eq: 4$
$Eq: C1.19$
it is concluded that
$Conf_1^o \overset{\perp}{\rightarrow}_o Conf_2^o$
We define
$Exec = Conf_1^o \overset{\perp}{\rightarrow}_o Conf_2^o$ $(Eq: C1.21)$

By DEFINITION 3 on $Eq: C1.21$
$Trace(Exec) = \cdot$ $(Eq: C1.22)$

From
$Eq: C1.7$
$Eq: 1$
it is concluded that
$L = \cdot$ $(Eq: C1.23)$

From
$Eq: C1.22$
$Eq: C1.23$
it is concluded that
$Trace(Exec) \,/\, rand = L$ $(Eq: C1.24)$

From
$Eq: C1.1$
$Eq: C1.15$
$Eq: 5$
it is concluded that
$\forall i \neq j$:
$\langle \tau', s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_i \in \mathcal{T} \Rightarrow$
$[\langle \tau', F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell_\tau' \rangle_i \in \mathcal{T}^o \; and \; \ell_\tau' \equiv \ell_\tau \; and \; (\tau' = \perp \Rightarrow \ell_\tau' = [\quad])]$ $(Eq: C1.25)$

From
$Eq: C1.4$
$Eq: C1.9$
it is concluded that
$\mathcal{T}_2 = \langle \tau, s, [\![c]\!]\sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_j, \mathcal{T}$ $(Eq: C1.26)$

From
$Eq: C1.26$
$Eq: C1.17$
$Eq: C1.25$

$Eq: C1.12$

it is concluded that

$\forall i$:

$\langle \tau', s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_i \in \mathcal{T}_2 \Rightarrow$

$[\langle \tau', F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_i \in \mathcal{T}_2^o \; and \; \ell_\tau{}' \equiv \ell_\tau \; and \; (\tau' = \bot \Rightarrow \ell'_\tau = [\quad])] \quad (Eq: C1.27)$

From

$Eq: C1.3$

$Eq: C1.6$

it is concluded that

$\ell_{sh_1} = \ell_{sh_2} \quad (Eq: C1.28)$

From

$Eq: C1.18$

$Eq: C1.28$

$Eq: 6$

it is concluded that

$\ell_{sh_2}{}' \equiv \ell_{sh_2} \quad (Eq: C1.29)$

The conclusion of this case is

$Eq: C1.19$

$Eq: C1.21$

$Eq: C1.24$

$Eq: C1.27$

$Eq: C1.29$

2. Case BEG:

We define j to be number of the thread that reduction is done in.

$\mathcal{T}_1 = \langle \bot, \text{beg}; s, \sigma_\tau, \overleftarrow{\sigma_\tau}, [\quad] \rangle_j, \mathcal{T} \quad (Eq: C2.1)$

$\sigma_{sh_1} = \sigma_{sh} \quad (Eq: C2.2)$

$\ell_{sh_1} = \ell_{sh} \quad (Eq: C2.3)$

$\mathcal{T}_2 = \langle fresh(\tau), s, \text{snap}(\sigma_\tau, \sigma_{sh}), \sigma_\tau[\text{stmt} \mapsto \text{"beg; } s\text{"}], [\quad] \rangle_j, \mathcal{T} \quad (Eq: C2.4)$

$\sigma_{sh_2} = \sigma_{sh} \quad (Eq: C2.5)$

$\ell_{sh_2} = \ell_{sh} \quad (Eq: C2.6)$

From DEFINITION 4

$Label_{MT}\left(Conf_1 \xrightarrow{\langle \tau, \text{beg} \rangle} Conf_2\right) = \langle \tau, \text{beg} \rangle \quad (Eq: C2.7)$

From

$Eq: C2.1$

it is concluded that

$\langle \bot, \text{beg}; s, \sigma_\tau, \overleftarrow{\sigma_\tau}, [\quad] \rangle_j \in \mathcal{T}_1 \quad (Eq: C2.8)$

We define st to be the statement that $stmt$ is mapped to in $\overleftarrow{\sigma_\tau}$. Therefore, we have

$\overleftarrow{\sigma_\tau} = \overleftarrow{\sigma_\tau}'; stmt \mapsto st \quad (Eq: C2.9)$

From

$Eq: C2.8$

$Eq: C2.9$

it is concluded that

$\langle \bot, \text{beg}; s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, [\quad] \rangle_j \in \mathcal{T}_1 \quad (Eq: C2.10)$

From

$Eq: C2.10$ (Note that $\tau' = \bot$)

$Eq: 5$

it is concluded that

$\langle \bot, F(\text{beg}; s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), [\quad] \rangle_j \in \mathcal{T}_1^o \quad (Eq: C2.11)$

From DEFINITION 7, it is concluded that

$F(\text{beg}; s) = beg; F(s)$ $(Eq: C2.12)$

From
$Eq: C2.11$
$Eq: C2.12$
it is concluded that
$\langle \bot, beg; F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), [\quad]\rangle_j \in \mathcal{T}_1^o$ $(Eq: C2.13)$

From
$Eq: C2.13$
it is concluded that $\mathcal{T}_1^o$ is of the form (there exists a $\mathcal{T}^o$ such that)
$\mathcal{T}_1^o = \langle \bot, beg; F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), [\quad]\rangle_j, \mathcal{T}^o$ $(Eq: C2.14)$

From the rule $OBEG$, it is concluded that
$\langle \langle \bot, beg; F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), [\quad]\rangle_j, \mathcal{T}^o \cdot \sigma_{sh} \cdot \ell_{sh_1}{}'\rangle \xrightarrow{\langle \tau, \text{beg}\rangle}_o$
$\langle \langle \text{fresh}(\tau), F(s), \text{snap}(\sigma_\tau, \sigma_{sh}), \sigma_\tau[\text{stmt} \mapsto \text{beg;F(s)}], [\quad]\rangle_j, \mathcal{T}^o \cdot \sigma_{sh} \cdot \ell_{sh_1}{}'\rangle$ $(Eq: C2.15)$

We define
$\mathcal{T}_2^o = \langle \text{fresh}(\tau), F(s), \text{snap}(\sigma_\tau, \sigma_{sh}), \sigma_\tau[\text{stmt} \mapsto \text{beg;F(s)}], [\quad]\rangle_j, \mathcal{T}^o$ $(Eq: C2.16)$
$\ell_{sh_2}{}' = \ell_{sh_1}{}'$ $(Eq: C2.17)$
$Conf_2^o = \langle \mathcal{T}_2^o \cdot \sigma_{sh_2} \cdot \ell_{sh_2}{}'\rangle$ $(Eq: C2.18)$

From
$Eq: C2.15$
$Eq: C2.14$
$Eq: C2.2$
$Eq: C2.16$
$Eq: C2.5$
$Eq: C2.17$
it is concluded that
$\langle \mathcal{T}_1^o \cdot \sigma_{sh_1} \cdot \ell_{sh_1}{}'\rangle \xrightarrow{\langle \tau, \text{beg}\rangle}_o \langle \mathcal{T}_2^o \cdot \sigma_{sh_2} \cdot \ell_{sh_2}{}'\rangle$ $(Eq: C2.19)$

From
$Eq: C2.19$
$Eq: 4$
$Eq: C2.18$
it is concluded that
$Conf_1^o \xrightarrow{\langle \tau, \text{beg}\rangle}_o Conf_2^o$
Therefore, there exists $Exec'$ such that
$Exec = Conf_1^o \xrightarrow{\langle \tau, \text{beg}\rangle}_o Conf_2^o$ $(Eq: C2.20)$

By DEFINITION 3 on $Eq: C2.20$
$Trace(Exec) = \langle \tau, \text{beg}\rangle$ $(Eq: C2.21)$

From
$Eq: C2.7$
$Eq: 1$
it is concluded that
$L = \langle \tau, \text{beg}\rangle$ $(Eq: C2.22)$

From
$Eq: C2.21$
$Eq: C2.22$
it is concluded that
$Trace(Exec) \;/\; rand = \; L$ $(Eq: C2.23)$

From
$Eq: C2.1$

$Eq: C2.14$
$Eq: 5$
it is concluded that
$\forall i \neq j$:
$\langle \tau', s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_i \in \mathcal{T} \Rightarrow$
$[\langle \tau', F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell_\tau' \rangle_i \in \mathcal{T}^o \; and \; \ell_\tau{}' \equiv \ell_\tau \; and \; (\tau' = \perp \Rightarrow \ell_\tau' = [\quad])]$ $(Eq: C2.24)$

From
$Eq: C2.24$
$Eq: C2.4$
$Eq: C2.16$
it is concluded that
$\forall i$:
$\langle \tau', s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_i \in \mathcal{T}_2 \Rightarrow$
$[\langle \tau', F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell_\tau' \rangle_i \in \mathcal{T}_2^o \; and \; \ell_\tau{}' \equiv \ell_\tau \; and \; (\tau' = \perp \Rightarrow \ell_\tau' = [\quad])]$ $(Eq: C2.25)$

From
$Eq: C2.3$
$Eq: C2.6$
it is concluded that
$\ell_{sh_1} = \ell_{sh_2}$ $(Eq: C2.26)$

From
$Eq: C2.17$
$Eq: C2.26$
$Eq: 6$
it is concluded that
$\ell_{sh_2}{}' \equiv \ell_{sh_2}$ $(Eq: C2.27)$

The conclusion of this case is
$Eq: C2.18$
$Eq: C2.20$
$Eq: C2.23$
$Eq: C2.25$
$Eq: C2.27$

3. Case APP:
We define j to be number of the thread that reduction is done in.
$\mathcal{T}_1 = \langle \tau, x \coloneqq o.m; s, \sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau \rangle_j, \mathcal{T}$ $(Eq: C3.1)$
$\sigma_{sh_1} = \sigma_{sh}$ $(Eq: C3.2)$
$\ell_{sh_1} = \ell_{sh}$ $(Eq: C3.3)$
$\mathcal{T}_2 = \langle \tau, s, \sigma_\tau[\mathrm{o} \mapsto (\llbracket o \rrbracket \sigma_\tau).m, x \mapsto rv((\llbracket o \rrbracket \sigma_\tau).m)], \overleftarrow{\sigma_\tau}, \ell_\tau :: (\mathrm{o.m}) \rangle_j, \mathcal{T}$ $(Eq: C3.4)$
$\sigma_{sh_2} = \sigma_{sh}$ $(Eq: C3.5)$
$\ell_{sh_2} = \ell_{sh}$ $(Eq: C3.6)$

From DEFINITION 4
$Label_{MT}\left(Conf_1 \xrightarrow{\langle \tau, o.m \rangle} Conf_2\right) = \langle \tau, o.m \rangle$ $(Eq: C3.7)$

From
$Eq: C3.1$
it is concluded that
$\langle \tau, x \coloneqq o.m; s, \sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau \rangle_j \in \mathcal{T}_1$ $(Eq: C3.8)$

We define st to be the statement that $stmt$ is mapped to in $\overleftarrow{\sigma_\tau}$. Therefore, we have
$\overleftarrow{\sigma_\tau} = \overleftarrow{\sigma_\tau}'; stmt \mapsto st$ $(Eq: C3.9)$

From
$Eq: C3.8$
$Eq: C3.9$

it is concluded that

$\langle \tau, x \coloneqq o.m; s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_j \in \mathcal{T}_1$ $(Eq: C3.10)$

From

$Eq: C3.10$

$Eq: 5$

it is concluded that

$\langle \tau, F(x \coloneqq o.m; s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_j \in \mathcal{T}_1^o$ $(Eq: C3.11)$

$\ell_\tau{}' \equiv \ell_\tau \; and \; (\tau = \perp \Rightarrow \ell'_\tau = [\quad])$ $(Eq: C3.12)$

From DEFINITION 7, it is concluded that

$F(x \coloneqq o.m; s) = x \coloneqq o.m; F(s)$ $(Eq: C3.13)$

From

$Eq: C3.11$

$Eq: C3.13$

it is concluded that

$\langle \tau, x \coloneqq o.m; F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_j \in \mathcal{T}_1^o$ $(Eq: C3.14)$

From

$Eq: C3.14$

it is concluded that $\mathcal{T}_1^o$ is of the form (there exists a $\mathcal{T}^o$ such that)

$\mathcal{T}_1^o = \langle \tau, x \coloneqq o.m; F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_j, \mathcal{T}^o$ $(Eq: C3.15)$

From the rule $OAPP$, it is concluded that

$\langle \langle \tau, x \coloneqq o.m; F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_j, \mathcal{T}^o \cdot \sigma_{sh} \cdot \ell_{sh_1}{}' \rangle \xrightarrow{\langle \tau, o.m \rangle}_o$

$\langle \langle \tau, F(s), \sigma_\tau[\mathrm{o} \mapsto (\llbracket o \rrbracket \sigma_\tau).m, x \mapsto rv((\llbracket o \rrbracket \sigma_\tau).m)], \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau :: (\mathrm{o.m}) \rangle_j, \mathcal{T}^o \cdot \sigma_{sh} \cdot \ell_{sh_1}{}' \rangle$ $(Eq: C3.16)$

We define

$\mathcal{T}_2^o = \langle \tau, F(s), \sigma_\tau[\mathrm{o} \mapsto (\llbracket o \rrbracket \sigma_\tau).m, x \mapsto rv((\llbracket o \rrbracket \sigma_\tau).m)], \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau :: (\mathrm{o.m}) \rangle_j, \mathcal{T}^o$ $(Eq: C3.17)$

$\ell_{sh_2}{}' = \ell_{sh_1}{}'$ $(Eq: C3.18)$

$Conf_2^o = \langle \mathcal{T}_2^o \cdot \sigma_{sh_2} \cdot \ell_{sh_2}{}' \rangle$ $(Eq: C3.19)$

From

$Eq: C3.16$

$Eq: C3.15$

$Eq: C3.2$

$Eq: C3.17$

$Eq: C3.5$

$Eq: C3.18$

it is concluded that

$\langle \mathcal{T}_1^o \cdot \sigma_{sh_1} \cdot \ell_{sh_1}{}' \rangle \xrightarrow{\langle \tau, o.m \rangle}_o \langle \mathcal{T}_2^o \cdot \sigma_{sh_2} \cdot \ell_{sh_2}{}' \rangle$ $(Eq: C3.20)$

From

$Eq: C3.20$

$Eq: 4$

$Eq: C3.19$

it is concluded that

$Conf_1^o \xrightarrow{\langle \tau, o.m \rangle}_o Conf_2^o$

therefore, there exists $Exec$ such that

$Exec = Conf_1^o \xrightarrow{\langle \tau, o.m \rangle}_o Conf_2^o$ $(Eq: C3.21)$

By DEFINITION 3 on $Eq: C3.21$

$Trace(Exec) = \langle \tau, o.m \rangle$ $(Eq: C3.22)$

From

$Eq: C3.7$

$Eq: 1$

it is concluded that

$L = \langle \tau, o.m \rangle$ $(Eq: C3.23)$

From

$Eq: C3.22$

$Eq: C3.23$

it is concluded that

$Trace(Exec)\ /\ rand = L$ $(Eq: C3.24)$

From

$Eq: C3.1$

$Eq: C3.15$

$Eq: 5$

it is concluded that

$\forall i \neq j$:

$\langle \tau', s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_i \in \mathcal{T} \Rightarrow$

$[\langle \tau', F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell_\tau' \rangle_i \in \mathcal{T}^o \ and \ \ell_\tau{}' \equiv \ell_\tau \ and \ (\tau' = \perp \Rightarrow \ell_\tau' = [\quad])]$ $(Eq: C3.25)$

From

DEFINITION 6

$Eq: C3.12$

it is concluded that

$\ell_\tau{}' :: ("o.m") \equiv \ell_\tau :: ("o.m")$ $(Eq: C3.26)$

From

$Eq: C3.4$

$Eq: C3.9$

it is concluded that

$\mathcal{T}_2 = \langle \tau, s, \sigma_\tau[\mathrm{o} \mapsto ([\![o]\!]\sigma_{sh}).m, x \mapsto rv(([\![o]\!]\sigma_{sh}).m)], \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau :: (\mathrm{o.m}) \rangle_j, \mathcal{T}$ $(Eq: C3.27)$

From

$Eq: C3.25$

$Eq: C3.27$

$Eq: C3.17$

$Eq: C3.26$

it is concluded that

$\forall i$:

$\langle \tau', s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_i \in \mathcal{T}_2 \Rightarrow$

$[\langle \tau', F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell_\tau' \rangle_i \in \mathcal{T}_2^o \ and \ \ell_\tau{}' \equiv \ell_\tau \ and \ (\tau' = \perp \Rightarrow \ell_\tau' = [\quad])]$ $(Eq: C3.28)$

From

$Eq: C3.3$

$Eq: C3.6$

it is concluded that

$\ell_{sh_1} = \ell_{sh_2}$ $(Eq: C3.29)$

From

$Eq: C3.18$

$Eq: C3.29$

$Eq: 6$

it is concluded that

$\ell_{sh_2}{}' \equiv \ell_{sh_2}$ $(Eq: C3.30)$

The conclusion of this case is

$Eq: C3.19$

$Eq: C3.21$

$Eq: C3.24$

$Eq: C3.28$

$Eq: C3.30$

4. Case CMT:

$\mathcal{T}_1 = \langle \tau_i, end; s_i, \sigma_{\tau_i}, \overleftarrow{\sigma_{\tau_i}}, \ell_{\tau_i} \rangle_{i=1..c}, \mathcal{T}$ $(Eq: C4.1)$

$\sigma_{sh_1} = \sigma_{sh}$ $(Eq: C4.2)$

$\ell_{sh_1} = \ell_{sh}$ $(Eq: C4.3)$

$\mathcal{T}_2 = \langle \bot, s_i, \text{zap}(\sigma_{\tau_i}), \text{zap}(\sigma_{\tau_i}), [] \rangle_{i=1..c}, \mathcal{T}$ $(Eq: C4.4)$

$\sigma_{sh_2} = \text{merge}(\sigma_{sh}, \{\ell_{\tau_{i=1..c}}\})$ $(Eq: C4.5)$

$\ell_{sh_2} = \ell_{sh} :: \text{seq}(\langle \tau_i{}^{cmt}, \ell_{\tau_i} \rangle_{i=1..c})$ $(Eq: C4.6)$

From DEFINITION 4

$Label_{MT}\left(Conf_1 \xrightarrow{\langle \tau_1, \text{cmt} \rangle ... \langle \tau_c, \text{cmt} \rangle} Conf_2\right) = \langle \tau_1, \text{cmt} \rangle \ ... \langle \tau_c, \text{cmt} \rangle$ $(Eq: C4.7)$

$\forall \tau_{i=1..c} \forall \langle \tau^{cmt}, \ell_{\tau'} \rangle \in \ell_{sh}: \tau^{cmt} > \tau_i \Rightarrow \ell_{\tau_i} \sqsubset \ell_{\tau'}$ $(Eq: C4.8)$

$\forall \tau_{i=1..c} \forall \tau_{j=1..i-1}: \ell_{\tau_i} \sqsubset \ell_{\tau_j}$ $(Eq: C4.9)$

We define st_i to be the statement that $stmt$ is mapped to in $\overleftarrow{\sigma_{\tau_i}}$. Therefore, we have

$\overleftarrow{\sigma_{\tau_i}} = \overleftarrow{\sigma_{\tau_i}}'; stmt \mapsto st_i$ $(Eq: C4.10)$

From

$Eq: C4.1$

it is concluded that

$\forall \tau_{i=1..c}: \langle \tau_i, end; s_i, \sigma_{\tau_i}, \overleftarrow{\sigma_{\tau_i}}, \ell_{\tau_i} \rangle \in \mathcal{T}_1$

Thus from

$Eq: C4.10$

it is concluded that

$\forall \tau_{i=1..c}: \langle \tau_i, end; s_i, \sigma_{\tau_i}, \overleftarrow{\sigma_{\tau_i}}'; stmt \mapsto st_i, \ell_{\tau_i} \rangle \in \mathcal{T}_1$ $(Eq: C4.11)$

From

$Eq: C4.11$

$Eq: 5$

it is concluded that

$\forall i = 1..c: \langle \tau_i, F(end; s_i), \sigma_{\tau_i}, \overleftarrow{\sigma_{\tau_i}}'; stmt \mapsto F(st_i), \ell'_{\tau_i} \rangle_i \in \mathcal{T}_1^o$ $(Eq: C4.12)$

$\forall i = 1..c: \ell_{\tau_i}{}' \equiv \ell_{\tau_i} \ and \ \left(\tau_i = \bot \Rightarrow \ell_{\tau_i}{}' = [\quad]\right)$ $(Eq: C4.13)$

From DEFINITION 7, it is concluded that

$F(end; s_i) = end; F(s_i)$ $(Eq: C4.14)$

From

$Eq: C4.12$

$Eq: C4.14$

it is concluded that

$\forall i = 1..c: \langle \tau_i, end; F(s_i), \sigma_{\tau_i}, \overleftarrow{\sigma_{\tau_i}}'; stmt \mapsto F(st_i), \ell'_{\tau_i} \rangle_i \in \mathcal{T}_1^o$ $(Eq: C4.15)$

From

$Eq: C4.15$

it is concluded that $\mathcal{T}_1^o$ is of the form (there exists a $\mathcal{T}^o$ such that)

$\mathcal{T}_1^o = \langle \tau_i, end; F(s_i), \sigma_{\tau_i}, \overleftarrow{\sigma_{\tau_i}}'; stmt \mapsto F(st_i), \ell_{\tau_i}{}' \rangle_{i=1..c}, \mathcal{T}^o$ $(Eq: C4.16)$

We define

$\mathcal{T}^H_{j=1..c+1} = \langle \tau_i, end; F(s_i), \sigma_{\tau_i}, \overleftarrow{\sigma_{\tau_i}}'; stmt \mapsto F(st_i), \ell_{\tau_i}{}' \rangle_{i=j..c}, \langle \bot, F(s_i), \text{zap}(\sigma_{\tau_i}), \text{zap}(\sigma_{\tau_i}), [] \rangle_{i=1..j-1}, \mathcal{T}^o$ $(Eq: C4.17)$

$\sigma_{sh}{}^H_{j=1..c+1} = \text{merge}(\sigma_{sh}, \{(\ell_{\tau_i}{}')_{i=1..j-1}\})$ $(Eq: C4.18)$

$\ell_{sh}{}^H_{j=1..c+1} = \ell_{sh_1}{}' :: \text{seq}(\langle \tau_i{}^{cmt}, \ell_{\tau_i}{}' \rangle_{i=1..j-1})$ $(Eq: C4.19)$

(H is for helper.)

From

$Eq: C4.17$

$Eq: C4.16$

it is concluded that

$\mathcal{T}_1^o = \mathcal{T}_1^H$ $(Eq: C4.20)$

From
$Eq: C4.18$
$Eq: C4.2$
it is concluded that
$\sigma_{sh_1} = \sigma_{sh_1}^{H}$ $(Eq: C4.21)$

From
$Eq: C4.19$
it is concluded that
$\ell_{sh_1}{}' = \ell_{sh_1}^{H}$ $(Eq: C4.22)$

We define
$\mathcal{T}_2^o = \langle \perp, F(s_i), \text{zap}(\sigma_{\tau_i}), \text{zap}(\sigma_{\tau_i}), [] \rangle_{i=1..c}, \mathcal{T}^o$ $(Eq: C4.23)$

From
$Eq: C4.17$
$Eq: C4.23$
it is concluded that
$\mathcal{T}_2^o = \mathcal{T}_{c+1}^H$ $(Eq: C4.25)$

We define
$\sigma_{sh_2}^o = \text{merge}(\sigma_{sh}, \{(\ell_{\tau_i}{}')_{i=1..c}\})$ $(Eq: C4.26)$

From
$Eq: C4.26$
$Eq: C4.18$
it is concluded that
$\sigma_{sh_2}^o = \sigma_{sh_{c+1}}^H$ $(Eq: C4.27)$

From
$Eq: C4.26$
$Eq: C4.5$
$Eq: C4.13$
LEMMA 2
it is concluded that
$\sigma_{sh_2}^o = \sigma_{sh_2}$ $(Eq: C4.28)$

We define
$\ell_{sh_2}{}' = \ell_{sh_1}{}' :: \text{seq}(\langle \tau_i{}^{cmt}, \ell_{\tau_i}{}' \rangle_{i=1..c})$ $(Eq: C4.29)$

From
$Eq: C4.29$
$Eq: C4.19$
it is concluded that
$\ell_{sh_2}{}' = \ell_{sh_{C+1}}^H$ $(Eq: C4.30)$

From
$Eq: C4.29$
$Eq: C4.6$
$Eq: 6$
$Eq: C4.13$
DEFINITION 6
it is concluded that
$\ell_{sh_2}{}' \equiv \ell_{sh_2}$ $(Eq: C4.31)$

From
$Eq: C4.8$
$Eq: C4.13$
LEMMA 1

it is concluded that
$\forall \tau_{i=1..c} \forall \langle \tau^{cmt}, \ell_{\tau'} \rangle \in \ell_{sh} : \tau^{cmt} > \tau_i \Rightarrow \ell_{\tau_i}{}' \sqsupset \ell_{\tau'}$ $(Eq: C4.32)$

From
$Eq: C4.9$
$Eq: C4.13$
LEMMA 1
it is concluded that
$\forall \tau_{i=1..c} \forall \tau_{j=1..i-1} : \ell_{\tau_i}{}' \sqsupset \ell_{\tau_j}{}'$ $(Eq: C4.33)$

We show that:
$\forall j = 1..c : \langle \mathcal{T}_j^H \cdot \sigma_{sh_j}{}^H \cdot \ell_{sh_j}{}^H \rangle \xrightarrow{\langle \tau_j, \text{cmt} \rangle}_o \langle \mathcal{T}_{j+1}^H \cdot \sigma_{sh_{j+1}}{}^H \cdot \ell_{sh_{j+1}}{}^H \rangle$ $(Eq: C4.34)$

First, we show that the condition of the reduction:
$\forall \langle \tau^{cmt}, \ell_{\tau'} \rangle \in \ell_{sh_j}{}^H : \tau^{cmt} > \tau_j \Rightarrow \ell_{\tau_j}{}' \sqsupset \ell_{\tau'}$ $(Eq: C4.35)$
is valid.

From
$Eq: C4.32$
it is concluded that
$\forall \langle \tau^{cmt}, \ell_{\tau'} \rangle \in \ell_{sh} : \tau^{cmt} > \tau_j \Rightarrow \ell_{\tau_j}{}' \sqsupset \ell_{\tau'}$ $(Eq: C4.35.1)$

From
$Eq: C4.33$
it is concluded that
$\forall \tau_{i=1..j-1} : \ell_{\tau_j}{}' \sqsupset \ell_{\tau_i}{}'$ $(Eq: C4.35.2)$

From
$Eq: C4.35.1$
$Eq: C4.35.2$
it is concluded that
$\forall \langle \tau^{cmt}, \ell_{\tau'} \rangle \in \ell_{sh} \cup \{ \langle \tau_i{}^{cmt}, \ell_{\tau_i}{}' \rangle_{i=1..j-1} \} : \tau^{cmt} > \tau_j \Rightarrow \ell_{\tau_j}{}' \sqsupset \ell_{\tau'}$ $(Eq: C4.35.3)$
that is equivalent to
$\forall \langle \tau^{cmt}, \ell_{\tau'} \rangle \in \ell_{sh} :: \text{seq}\big(\langle \tau_i{}^{cmt}, \ell_{\tau_i}{}' \rangle_{i=1..j-1} \big) : \tau^{cmt} > \tau_j \Rightarrow \ell_{\tau_j}{}' \sqsupset \ell_{\tau'}$ $(Eq: C4.35.4)$

From
$Eq: C4.35.4$
$Eq: C4.19$
it is concluded that
$\forall \langle \tau^{cmt}, \ell_{\tau'} \rangle \in \ell_{sh_j}{}^H : \tau^{cmt} > \tau_j \Rightarrow \ell_{\tau_j}{}' \sqsupset \ell_{\tau'}$ $(Eq: C4.35.5)$
that is the conclusion $(Eq: C4.35)$.

Second, we show that the result of the reduction is $\langle \mathcal{T}_{j+1}^H \cdot \sigma_{sh_{j+1}}{}^H \cdot \ell_{sh_{j+1}}{}^H \rangle$:
$\langle \mathcal{T}_j^H \cdot \sigma_{sh_j}{}^H \cdot \ell_{sh_j}{}^H \rangle \xrightarrow{\langle \tau_j, \text{cmt} \rangle}_o \langle \mathcal{T}_{j+1}^H \cdot \sigma_{sh_{j+1}}{}^H \cdot \ell_{sh_{j+1}}{}^H \rangle$ $(Eq: C4.36)$

From
$Eq: C4.17$
$Eq: C4.18$
$Eq: C4.19$
it is concluded that
$\langle \mathcal{T}_j^H \cdot \sigma_{sh_j}{}^H \cdot \ell_{sh_j}{}^H \rangle =$
$$\begin{pmatrix} \langle \tau_i, end; F(s_i), \sigma_{\tau_i}, \overline{\sigma_{\tau_i}}'; stmt \mapsto F(st_i), \ell_{\tau_i}{}' \rangle_{i=j..c}, \langle \bot, F(s_i), \text{zap}\big(\sigma_{\tau_i}\big), \text{zap}\big(\sigma_{\tau_i}\big), [] \rangle_{i=1..j-1}, \mathcal{T}^o \cdot \\ \text{merge}\big(\sigma_{sh}, \{ (\ell_{\tau_i}{}')_{i=1..j-1} \}\big) \cdot \\ \ell_{sh_1}{}' :: \text{seq}\big(\langle \tau_i{}^{cmt}, \ell_{\tau_i}{}' \rangle_{i=1..j-1} \big) \end{pmatrix} \quad (Eq: C4.36.1)$$

By the rule CMT:

$$\begin{pmatrix}\langle \tau_i, end; F(s_i), \sigma_{\tau_i}, \overleftarrow{\sigma_{\tau_i}}'; stmt \mapsto F(st_i), \ell_{\tau_i}' \rangle_{i=j..c}, \langle \bot, F(s_i), \text{zap}(\sigma_{\tau_i}), \text{zap}(\sigma_{\tau_i}), [] \rangle_{i=1..j-1}, \mathcal{T}^o \cdot \\ \text{merge}(\sigma_{sh}, \{(\ell_{\tau_i}')_{i=1..j-1}\}) \cdot \\ \ell_{sh_1}' :: \text{seq}(\langle {\tau_i}^{cmt}, \ell_{\tau_i}' \rangle_{i=1..j-1}) \end{pmatrix} \xrightarrow{\langle \tau_j, \text{cmt} \rangle}_o$$

$$\begin{pmatrix}\langle \bot, F(s_j), \text{zap}\left(\sigma_{\tau_j}\right), \text{zap}\left(\sigma_{\tau_j}\right), [\quad] \rangle \langle \tau_i, end; F(s_i), \sigma_{\tau_i}, \overleftarrow{\sigma_{\tau_i}}'; stmt \mapsto F(st_i), \ell_{\tau_i}' \rangle_{i=j+1..c}, \langle \bot, s_i, \text{zap}(\sigma_{\tau_i}), \text{zap}(\sigma_{\tau_i}), [\quad] \rangle_{i=1..j-1}, \mathcal{T}^o \cdot \\ \text{merge}\left(\text{merge}(\sigma_{sh}, \{(\ell_{\tau_i}')_{i=1..j-1}\}), \ell_{\tau_j}'\right) \cdot \\ \ell_{sh_1}' :: \text{seq}(\langle {\tau_i}^{cmt}, \ell_{\tau_i}' \rangle_{i=1..j-1}) :: \langle \text{fresh}({\tau_j}^{cmt}), \ell_{\tau_j}' \rangle \end{pmatrix}$$

$(Eq: C4.36.2)$

$\langle \bot, F(s_j), \text{zap}\left(\sigma_{\tau_j}\right), \text{zap}\left(\sigma_{\tau_j}\right), [\quad] \rangle \langle \tau_i, end; F(s_i), \sigma_{\tau_i}, \overleftarrow{\sigma_{\tau_i}}'; stmt \mapsto F(st_i), \ell_{\tau_i}' \rangle_{i=j+1..c}, \langle \bot, s_i, \text{zap}(\sigma_{\tau_i}), \text{zap}(\sigma_{\tau_i}), [\quad] \rangle_{i=1..j-1}, \mathcal{T}^o$

can be rewritten as $(Eq: C4.36.3)$

$\langle \tau_i, end; F(s_i), \sigma_{\tau_i}, \overleftarrow{\sigma_{\tau_i}}'; stmt \mapsto F(st_i), \ell'_{\tau_i} \rangle_{i=j+1..c}, \langle \bot, F(s_i), \text{zap}(\sigma_{\tau_i}), \text{zap}(\sigma_{\tau_i}), [\quad] \rangle_{i=1..j}, \mathcal{T}^o$

From definition of merge

$$\text{merge}\left(\text{merge}(\sigma_{sh}, \{(\ell_{\tau_i}')_{i=1..j-1}\}), \ell_{\tau_j}'\right) = \text{merge}(\sigma_{sh}, \{(\ell_{\tau_i}')_{i=1..j}\}) \quad (Eq: C4.36.4)$$

From definition of seq

$$\ell_{sh_1}' :: \text{seq}(\langle {\tau_i}^{cmt}, \ell_{\tau_i}' \rangle_{i=1..j-1}) :: \langle \text{fresh}({\tau_j}^{cmt}), \ell_{\tau_j}' \rangle = \ell_{sh_1}' :: \text{seq}(\langle {\tau_i}^{cmt}, \ell_{\tau_i}' \rangle_{i=1..j}) \quad (Eq: C4.36.5)$$

From

$Eq: C4.36.2$
$Eq: C4.36.3$
$Eq: C4.36.4$
$Eq: C4.36.5$

it is concluded that

$$\begin{pmatrix}\langle \tau_i, end; F(s_i), \sigma_{\tau_i}, \overleftarrow{\sigma_{\tau_i}}'; stmt \mapsto F(st_i), \ell_{\tau_i}' \rangle_{i=j..c}, \langle \bot, F(s_i), \text{zap}(\sigma_{\tau_i}), \text{zap}(\sigma_{\tau_i}), [] \rangle_{i=1..j-1}, \mathcal{T}^o \cdot \\ \text{merge}(\sigma_{sh}, \{(\ell_{\tau_i}')_{i=1..j-1}\}) \cdot \\ \ell_{sh_1}' :: \text{seq}(\langle {\tau_i}^{cmt}, \ell_{\tau_i}' \rangle_{i=1..j-1}) \end{pmatrix} \xrightarrow{\langle \tau_j, \text{cmt} \rangle}_o$$

$$\begin{pmatrix}\langle \tau_i, end; F(s_i), \sigma_{\tau_i}, \overleftarrow{\sigma_{\tau_i}}'; stmt \mapsto F(st_i), \ell'_{\tau_i} \rangle_{i=j+1..c}, \langle \bot, F(s_i), \text{zap}(\sigma_{\tau_i}), \text{zap}(\sigma_{\tau_i}), [\quad] \rangle_{i=1..j}, \mathcal{T}^o \cdot \\ \text{merge}(\sigma_{sh}, \{(\ell_{\tau_i}')_{i=1..j}\}) \cdot \\ \ell_{sh_1}' :: \text{seq}(\langle {\tau_i}^{cmt}, \ell_{\tau_i}' \rangle_{i=1..j}) \end{pmatrix} \quad (Eq: C4.36.6)$$

From

$Eq: C4.17$

it is concluded that

$$\mathcal{T}_{j+1}^H = \langle \tau_i, end; F(s_i), \sigma_{\tau_i}, \overleftarrow{\sigma_{\tau_i}}'; stmt \mapsto F(st_i), \ell'_{\tau_i} \rangle_{i=j+1..c}, \langle \bot, F(s_i), \text{zap}(\sigma_{\tau_i}), \text{zap}(\sigma_{\tau_i}), [\quad] \rangle_{i=1..j}, \mathcal{T}^o \quad (Eq: C4.36.7)$$

From

$Eq: C4.18$

it is concluded that

$${\sigma_{sh}}_{j+1}^H = \text{merge}(\sigma_{sh}, \{(\ell_{\tau_i}')_{i=1..j}\}) \quad (Eq: C4.36.8)$$

From

$Eq: C4.19$

it is concluded that

$${\ell_{sh}}_{j+1}^H = \ell_{sh_1}' :: \text{seq}(\langle {\tau_i}^{cmt}, \ell_{\tau_i}' \rangle_{i=1..j}) \quad (Eq: C4.36.9)$$

From

$Eq: C4.36.6$
$Eq: C4.36.1$
$Eq: C4.36.7$
$Eq: C4.36.8$
$Eq: C4.36.9$

it is concluded that

$\langle \mathcal{T}_j^H \cdot \sigma_{sh_j}^H \cdot \ell_{sh_j}^H \rangle \xrightarrow{\langle \tau_j, \text{cmt} \rangle}_o \langle \mathcal{T}_{j+1}^H \cdot \sigma_{sh_{j+1}}^H \cdot \ell_{sh_{j+1}}^H \rangle$ $(Eq: C4.36.10)$

That is the conclusion $(Eq: C4.36)$.

From

$Eq: C4.34$

it is concluded that

$\langle \mathcal{T}_1^H \cdot \sigma_{sh_1}^H \cdot \ell_{sh_1}^H \rangle \xrightarrow{\langle \tau_1, \text{cmt} \rangle}_o \langle \mathcal{T}_2^H \cdot \sigma_{sh_2}^H \cdot \ell_{sh_2}^H \rangle \xrightarrow{\langle \tau_2, \text{cmt} \rangle}_o \dots \xrightarrow{\langle \tau_c, \text{cmt} \rangle}_o \langle \mathcal{T}_{c+1}^H \cdot \sigma_{sh_{c+1}}^H \cdot \ell_{sh_{c+1}}^H \rangle$ $(Eq: C4.37)$

From

$Eq: C4.27$

$Eq: C4.28$

it is concluded that

$\ell_{sh_{c+1}}^H = \sigma_{sh_2}$ $(Eq: C4.38)$

From

$Eq: C4.37$

$Eq: C4.20$

$Eq: C4.21$

$Eq: C4.22$

$Eq: C4.25$

$Eq: C4.38$

$Eq: C4.30$

it is concluded that

$\langle \mathcal{T}_1^o \cdot \sigma_{sh_1} \cdot \ell_{sh_1}{}' \rangle \xrightarrow{\langle \tau_1, \text{cmt} \rangle}_o \langle \mathcal{T}_2^H \cdot \sigma_{sh_2}^H \cdot \ell_{sh_2}^H \rangle \xrightarrow{\langle \tau_2, \text{cmt} \rangle}_o \dots \xrightarrow{\langle \tau_c, \text{cmt} \rangle}_o \langle \mathcal{T}_2^o \cdot \sigma_{sh_2} \cdot \ell_{sh_2}{}' \rangle$ $(Eq: C4.39)$

We define

$Conf_2^o = \langle \mathcal{T}_2^o \cdot \sigma_{sh_2} \cdot \ell_{sh_2}{}' \rangle$ $(Eq: C4.40)$

From

$Eq. C4.39$

$Eq: 4$

$Eq. C4.40$

it is concluded that

$Conf_1^o \xrightarrow{\langle \tau_1, \text{cmt} \rangle}_o \langle \mathcal{T}_2^H \cdot \sigma_{sh_2}^H \cdot \ell_{sh_2}^H \rangle \xrightarrow{\langle \tau_2, \text{cmt} \rangle}_o \dots \xrightarrow{\langle \tau_c, \text{cmt} \rangle}_o Conf_2^o$ $(Eq: C4.41)$

From

$Eq: C4.41$

there exists $Exec$

$Exec = Conf_1^o \xrightarrow{\langle \tau_1, \text{cmt} \rangle}_o \langle \mathcal{T}_2^H \cdot \sigma_{sh_2}^H \cdot \ell_{sh_2}^H \rangle \xrightarrow{\langle \tau_2, \text{cmt} \rangle}_o \dots \xrightarrow{\langle \tau_c, \text{cmt} \rangle}_o Conf_2^o$ $(Eq: C4.42)$

By DEFINITION 3, definition of $Trace$, on $Eq: C4.42$

$Trace(Exec) = \langle \tau_1, \text{cmt} \rangle, \langle \tau_2, \text{cmt} \rangle, \dots, \langle \tau_c, \text{cmt} \rangle$ $(Eq: C4.43)$

From

$Eq: C4.43$

it is concluded that

$Trace(Exec) \;/\; rand = \langle \tau_1, \text{cmt} \rangle, \langle \tau_2, \text{cmt} \rangle, \dots, \langle \tau_c, \text{cmt} \rangle$ $(Eq: C4.44)$

From

$Eq: C4.7$

$Eq: 1$

it is concluded that

$L = \langle \tau_1, \text{cmt} \rangle, \langle \tau_2, \text{cmt} \rangle, \dots, \langle \tau_c, \text{cmt} \rangle$ $(Eq: C4.45)$

From

$Eq: C4.44$

$Eq: C4.45$

it is concluded that
$Trace(Exec) \,/\, rand = L$ $(Eq: C4.46)$

From
$Eq: C4.1$
$Eq: C4.10$
it is concluded that
$\mathcal{T}_1 = \langle \tau_i, end; s_i, \sigma_{\tau_i}, \overleftarrow{\sigma_{\tau_i}}'; stmt \mapsto st_i, \ell_{\tau_i} \rangle_{i=1..c}, \mathcal{T}$ $(Eq: C4.47)$

From
$Eq: C4.47$
$Eq: C4.16$
$Eq: 5$
it is concluded that
$\forall i \neq 1..c$:
$\langle \tau', s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_i \in \mathcal{T} \Rightarrow$
$[\langle \tau', F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_i \in \mathcal{T}^o \; and \; \ell_\tau{}' \equiv \ell_\tau \; and \; (\tau' = \bot \Rightarrow \ell'_\tau = [\quad])]$ $(Eq: C4.48)$

It is trivial that
$\forall \tau_{i=1..c}$: $[\text{stmt}]\text{zap}(\sigma_{\tau_i}) = \bot$ $(Eq: C4.49)$

From DEFINITION 7
$F(\bot) = \bot$ $(Eq: C4.50)$

From
$Eq: C4.4$
$Eq: C4.23$
$Eq: C4.48$
$Eq: C4.49$
$Eq: C4.50$
it is concluded that
$\forall i$:
$\langle \tau', s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_i \in \mathcal{T}_2 \Rightarrow$
$[\langle \tau', F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_i \in \mathcal{T}_2^o \; and \; \ell_\tau{}' \equiv \ell_\tau \; and \; (\tau' = \bot \Rightarrow \ell'_\tau = [\quad])]$ $(Eq: C4.51)$

The conclusion of this case is:
$Eq: C4.40$
$Eq: C4.42$
$Eq: C4.44$
$Eq: C4.51$
$Eq: C4.31$

5. Case ABT:
We define j to be number of the thread that reduction is done in.
$\mathcal{T}_1 = \langle \tau, s, \sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau \rangle_j, \mathcal{T}$ $(Eq: C5.1)$
$\sigma_{sh_1} = \sigma_{sh}$ $(Eq: C5.2)$
$\ell_{sh_1} = \ell_{sh}$ $(Eq: C5.3)$
$\mathcal{T}_2 = \langle \bot, [\![\text{stmt}]\!] \overleftarrow{\sigma_\tau}, \overleftarrow{\sigma_\tau}/\text{stmt}, \overleftarrow{\sigma_\tau}, [] \rangle_j \;, \mathcal{T}$ $(Eq: C5.4)$
$\sigma_{sh_2} = \sigma_{sh}$ $(Eq: C5.5)$
$\ell_{sh_2} = \ell_{sh}$ $(Eq: C5.6)$

From DEFINITION 4
$Label_{MT}\left(Conf_1 \xrightarrow{\langle \tau, \text{abt} \rangle} Conf_2\right) = \langle \tau, \text{abt} \rangle$ $(Eq: C5.7)$

We define st to be the statement that $stmt$ is mapped to in $\overleftarrow{\sigma_\tau}$. Therefore, we have
$\overleftarrow{\sigma_\tau} = \overleftarrow{\sigma_\tau}'; \text{stmt} \mapsto st$ $(Eq: C5.8)$

From
$Eq: C5.1$
$Eq: C5.8$
it is concluded that
$\mathcal{T}_1 = \langle \tau, s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; \text{stmt} \mapsto st, \ell_\tau \rangle_j, \mathcal{T}$ $(Eq: C5.9)$

From
$Eq: C5.9$
it is concluded that
$\langle \tau, s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; \text{stmt} \mapsto st, \ell_\tau \rangle_j \in \mathcal{T}_1$ $(Eq: C5.10)$

From
$Eq: C5.4$
$Eq: C5.8$
it is concluded that
$\mathcal{T}_2 = \langle \bot, st, \overleftarrow{\sigma_\tau}', \overleftarrow{\sigma_\tau}'; \text{stmt} \mapsto st, [\quad] \rangle_j, \mathcal{T}$ $(Eq: C5.11)$

From
$Eq: C5.10$
$Eq: 5$
it is concluded that
$\langle \tau, F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; \text{stmt} \mapsto F(st), \ell'_\tau \rangle_j \in \mathcal{T}_1^o$ $(Eq: C5.12)$
${\ell_\tau}' \equiv \ell_\tau \; and \; (\tau = \bot \Rightarrow \ell'_\tau = [\quad])$ $(Eq: C5.13)$

From
$Eq: C5.12$
it is concluded that $\mathcal{T}_1^o$ is of the form (there exists a $\mathcal{T}^o$ such that)
$\mathcal{T}_1^o = \langle \tau, F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; \text{stmt} \mapsto F(st), \ell'_\tau \rangle_j, \mathcal{T}^o$ $(Eq: C5.14)$

From the rule $OABT$, it is concluded that
$\langle \langle \tau, F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; \text{stmt} \mapsto F(st), \ell'_\tau \rangle_j, \mathcal{T}^o \cdot \sigma_{sh} \cdot {\ell_{sh_1}}' \rangle \xrightarrow{\langle \tau, \text{abt} \rangle}_o$ $(Eq: C5.15)$
$\langle \langle \bot, F(st), \overleftarrow{\sigma_\tau}', \overleftarrow{\sigma_\tau}'; \text{stmt} \mapsto F(st), [\quad] \rangle_j, \mathcal{T}^o \cdot \sigma_{sh} \cdot {\ell_{sh_1}}' \rangle$

We define
$\mathcal{T}_2^o = \langle \bot, F(st), \overleftarrow{\sigma_\tau}', \overleftarrow{\sigma_\tau}'; \text{stmt} \mapsto F(st), [\quad] \rangle_j, \mathcal{T}^o$ $(Eq: C5.16)$
${\ell_{sh_2}}' = {\ell_{sh_1}}'$ $(Eq: C5.17)$
$Conf_2^o = \langle \mathcal{T}_2^o \cdot \sigma_{sh_2} \cdot {\ell_{sh_2}}' \rangle$ $(Eq: C5.18)$

From
$Eq: C5.15$
$Eq: C5.14$
$Eq: C5.2$
$Eq: C5.16$
$Eq: C5.5$
$Eq: C5.17$
it is concluded that
$\langle \mathcal{T}_1^o \cdot \sigma_{sh_1} \cdot {\ell_{sh_1}}' \rangle \xrightarrow{\langle \tau, \text{abt} \rangle}_o \langle \mathcal{T}_2^o \cdot \sigma_{sh_2} \cdot {\ell_{sh_2}}' \rangle$ $(Eq: C5.19)$

From
$Eq: C5.19$
$Eq: 4$
$Eq: C5.18$
it is concluded that
$Conf_1^o \xrightarrow{\langle \tau, \text{abt} \rangle}_o Conf_2^o$
We define
$Exec = Conf_1^o \xrightarrow{\langle \tau, \text{abt} \rangle}_o Conf_2^o$ $(Eq: C5.20)$

By DEFINITION 3 on $Eq: C.20$

$Trace(Exec) = \langle \tau, \text{abt} \rangle$ $(Eq: C5.21)$

From
$Eq: C5.7$
$Eq: 1$
it is concluded that
$L = \langle \tau, \text{abt} \rangle$ $(Eq: C5.22)$

From
$Eq: C5.21$
$Eq: C5.22$
it is concluded that
$Trace(Exec)/\ rand = L$ $(Eq: C5.23)$

From
$Eq: C5.9$
$Eq: C5.14$
$Eq: 5$
it is concluded that
$\forall i \neq j$:
$\langle \tau', s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_i \in \mathcal{T} \Rightarrow$
$[\langle \tau', F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell_\tau' \rangle_i \in \mathcal{T}^o \ and \ \ell_\tau{}' \equiv \ell_\tau \ and \ (\tau' = \perp \Rightarrow \ell_\tau' = [\quad])]$ $(Eq: C5.24)$

From
$Eq: C5.11$
$Eq: C5.16$
$Eq: C5.24$
it is concluded that
$\forall i$:
$\langle \tau', s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_i \in \mathcal{T}_2 \Rightarrow$
$[\langle \tau', F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell_\tau' \rangle_i \in \mathcal{T}_2^o \ and \ \ell_\tau{}' \equiv \ell_\tau \ and \ (\tau' = \perp \Rightarrow \ell_\tau' = [\quad])]$ $(Eq: C5.25)$

From
$Eq: C5.3$
$Eq: C5.6$
it is concluded that
$\ell_{sh_1} = \ell_{sh_2}$ $(Eq: C5.26)$

From
$Eq: C5.17$
$Eq: C5.26$
$Eq: 6$
it is concluded that
$\ell_{sh_2}{}' \equiv \ell_{sh_2}$ $(Eq: C5.27)$

The conclusion of this case is
$Eq: C5.18$
$Eq: C5.20$
$Eq: C5.23$
$Eq: C5.25$
$Eq: C5.27$

6. Case $Send$:
We define j to be number of the thread that reduction is done in.
$\mathcal{T}_1 = \langle \tau, ch\ send\ v; s, \sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau \rangle_j, \mathcal{T}$ $(Eq: C6.1)$
$\sigma_{sh_1} = \sigma_{sh}$ $(Eq: C6.2)$
$\ell_{sh_1} = \ell_{sh}$ $(Eq: C6.3)$
$\mathcal{T}_2 = \langle \tau, s, \sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau \rangle_j, \mathcal{T}$ $(Eq: C6.4)$
$\sigma_{sh_2} = \sigma_{sh}$ $(Eq: C6.5)$
$\ell_{sh_2} = \ell_{sh}$ $(Eq: C6.6)$

From DEFINITION 4

$$Label_{MT}\left(Conf_1 \xrightarrow{\langle \tau, \text{ch send} \rangle} Conf_2\right) = \cdot \qquad (Eq: C6.7)$$

From

$Eq: C6.1$

it is concluded that

$$\langle \tau, ch\ send\ v; s, \sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau \rangle_j \in \mathcal{T}_1 \qquad (Eq: C6.8)$$

We define st to be the statement that $stmt$ is mapped to in $\overleftarrow{\sigma_\tau}$. Therefore, we have

$$\overleftarrow{\sigma_\tau} = \overleftarrow{\sigma_\tau}'; stmt \mapsto st \qquad (Eq: C6.9)$$

From

$Eq: C6.8$

$Eq: C6.9$

it is concluded that

$$\langle \tau, ch\ send\ v; s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_j \in \mathcal{T}_1 \qquad (Eq: C6.10)$$

From

$Eq: C6.10$

$Eq: 5$

it is concluded that

$$\langle \tau, F(ch\ send\ v; s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_j \in \mathcal{T}_1^o \qquad (Eq: C6.11)$$

$$\ell_\tau{}' \equiv \ell_\tau\ and\ (\tau = \perp \Rightarrow \ell'_\tau = [\quad]) \qquad (Eq: C6.12)$$

From DEFINITION 7, it is concluded that

$$F(ch\ send\ v; s) = x \coloneqq x; F(s) \qquad (Eq: C6.13)$$

From

$Eq: C6.11$

$Eq: C6.13$

it is concluded that

$$\langle \tau, x \coloneqq x; F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_j \in \mathcal{T}_1^o \qquad (Eq: C6.14)$$

From

$Eq: C6.14$

it is concluded that $\mathcal{T}_1^o$ is of the form (there exists a $\mathcal{T}^o$ such that)

$$\mathcal{T}_1^o = \langle \tau, x \coloneqq x; F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_j, \mathcal{T}^o \qquad (Eq: C6.15)$$

From the rule $OCMD$, it is concluded that

$$\langle \langle \tau, x \coloneqq x; F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_j, \mathcal{T}^o \cdot \sigma_{sh} \cdot \ell_{sh_1}{}' \rangle \xrightarrow{\perp}_o \qquad (Eq: C6.16)$$

$$\langle \langle \tau, F(s), [\![x \coloneqq x]\!]\sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_j, \mathcal{T}^o \cdot \sigma_{sh} \cdot \ell_{sh_1}{}' \rangle$$

We define

$$\mathcal{T}_2^o = \langle \tau, F(s), [\![x \coloneqq x]\!]\sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_j, \mathcal{T}^o \qquad (Eq: C6.17)$$

$$\ell_{sh_2}{}' = \ell_{sh_1}{}' \qquad (Eq: C6.18)$$

$$Conf_2^o = \langle \mathcal{T}_2^o \cdot \sigma_{sh_2} \cdot \ell_{sh_2}{}' \rangle \qquad (Eq: C6.19)$$

It is obvious that

$$[\![x \coloneqq x]\!]\sigma_\tau = \sigma_\tau \qquad (Eq: C6.20)$$

From

$Eq: C6.17$

$Eq: C6.20$

it is concluded that

$$\mathcal{T}_2^o = \langle \tau, F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_j, \mathcal{T}^o \qquad (Eq: C6.21)$$

From

$Eq: C6.16$
$Eq: C6.15$
$Eq: C6.2$
$Eq: C6.17$
$Eq: C6.5$
$Eq: C6.18$
it is concluded that

$$\langle \mathcal{T}_1^o \cdot \sigma_{sh_1} \cdot \ell_{sh_1}{}' \rangle \xrightarrow{\perp}_o \langle \mathcal{T}_2^o \cdot \sigma_{sh_2} \cdot \ell_{sh_2}{}' \rangle \qquad (Eq: C6.22)$$

From
$Eq: C6.22$
$Eq: 4$
$Eq: C6.19$
it is concluded that

$$Conf_1^o \xrightarrow{\perp}_o Conf_2^o$$

We define

$$Exec = Conf_1^o \xrightarrow{\perp}_o Conf_2^o \qquad (Eq: C6.23)$$

By DEFINITION 3 on $Eq: C6.23$

$$Trace(Exec) = \cdot \qquad (Eq: C6.24)$$

From
$Eq: C6.7$
$Eq: 1$
it is concluded that

$$L = \cdot \qquad (Eq: C6.25)$$

From
$Eq: C6.24$
$Eq: C6.25$
it is concluded that

$$Trace(Exec) \,/\, rand = L \qquad (Eq: C6.26)$$

From
$Eq: C6.1$
$Eq: C6.15$
$Eq: 5$
it is concluded that

$\forall i \neq j$:

$$\langle \tau', s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_i \in \mathcal{T} \Rightarrow$$
$$[\langle \tau', F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_i \in \mathcal{T}^o \; and \; \ell_\tau{}' \equiv \ell_\tau \; and \; (\tau' = \perp \Rightarrow \ell'_\tau = [\quad])] \qquad (Eq: C6.27)$$

From
$Eq: C6.4$
$Eq: C6.9$
it is concluded that

$$\mathcal{T}_2 = \langle \tau, s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle, \mathcal{T} \qquad (Eq: C6.28)$$

From
$Eq: C6.28$
$Eq: C6.21$
$Eq: C6.27$
$Eq: C6.12$
it is concluded that

$\forall i$:

$$\langle \tau', s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_i \in \mathcal{T}_2 \Rightarrow$$
$$[\langle \tau', F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_i \in \mathcal{T}_2^o \; and \; \ell_\tau{}' \equiv \ell_\tau \; and \; (\tau' = \perp \Rightarrow \ell'_\tau = [\quad])] \qquad (Eq: C6.29)$$

From
$Eq: C6.3$

$Eq: C6.6$

it is concluded that

$\ell_{sh_1} = \ell_{sh_2}$ $(Eq: C6.30)$

From

$Eq: C6.18$

$Eq: C6.30$

$Eq: 6$

it is concluded that

$\ell_{sh_2}{}' \equiv \ell_{sh_2}$ $(Eq: C6.31)$

The conclusion of this case is

$Eq: C6.19$

$Eq: C6.23$

$Eq: C6.26$

$Eq: C6.29$

$Eq: C6.31$

7. Case $Receive$:

We define j to be number of the thread that reduction is done in.

$\mathcal{T}_1 = \langle \tau, x \coloneqq ch\ receive; s, \sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau \rangle_j, \mathcal{T}$ $(Eq: C7.1)$

$\sigma_{sh_1} = \sigma_{sh}$ $(Eq: C7.2)$

$\ell_{sh_1} = \ell_{sh}$ $(Eq: C7.3)$

$\mathcal{T}_2 = \langle \tau, s, \sigma_\tau[x \mapsto v], \overleftarrow{\sigma_\tau}, \ell_\tau \rangle_j, \mathcal{T}$ $(Eq: C7.4)$

$\sigma_{sh_2} = \sigma_{sh}$ $(Eq: C7.5)$

$\ell_{sh_2} = \ell_{sh}$ $(Eq: C7.6)$

From DEFINITION 4

$Label_{MT}\left(Conf_1 \xrightarrow{\langle \tau, \text{ch receive} \rangle} Conf_2\right) = \cdot$ $(Eq: C7.7)$

From

$Eq: C7.1$

it is concluded that

$\langle \tau, x \coloneqq ch\ receive; s, \sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau \rangle_j \in \mathcal{T}_1$ $(Eq: C7.8)$

We define st to be the statement that $stmt$ is mapped to in $\overleftarrow{\sigma_\tau}$. Therefore, we have

$\overleftarrow{\sigma_\tau} = \overleftarrow{\sigma_\tau}'; stmt \mapsto st$ $(Eq: C7.9)$

From

$Eq: C7.8$

$Eq: C7.9$

it is concluded that

$\langle \tau, x \coloneqq ch\ receive; s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_j \in \mathcal{T}_1$ $(Eq: C7.10)$

From

$Eq: C7.10$

$Eq: 5$

it is concluded that

$\langle \tau, F(x \coloneqq ch\ receive; s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_j \in \mathcal{T}_1^o$ $(Eq: C7.11)$

$\ell_\tau{}' \equiv \ell_\tau\ and\ (\tau = \perp \Rightarrow \ell'_\tau = [\quad])$ $(Eq: C7.12)$

From DEFINITION 7, it is concluded that

$F(x \coloneqq ch\ receive; s) = x \coloneqq rand.gen; F(s)$ $(Eq: C7.13)$

From

$Eq: C7.11$

$Eq: C7.13$

it is concluded that

$\langle \tau, x \coloneqq rand.gen; F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_j \in \mathcal{T}_1^o$ $(Eq: C7.14)$

From
$Eq: C7.14$
it is concluded that $\mathcal{T}_1^o$ is of the form (there exists a $\mathcal{T}^o$ such that)
$\mathcal{T}_1^o = \langle \tau, x \coloneqq rand.gen; F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_j, \mathcal{T}^o$ $(Eq: C7.15)$

From the rule $OAPP$, it is concluded that
$\langle \langle \tau, x \coloneqq rand.gen; F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_j, \mathcal{T}^o \cdot \sigma_{sh} \cdot {\ell_{sh_1}}' \rangle \xrightarrow{\langle \tau, rand.gen \rangle}_o$
$\langle \langle \tau, F(s), \sigma_\tau[rand \mapsto ([\![rand]\!]\sigma_{sh}).gen, x \mapsto rv([\![rand]\!]\sigma_{sh}).gen], \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau :: (\text{rand.gen}) \rangle_j, \mathcal{T}^o \cdot \sigma_{sh} \cdot {\ell_{sh_1}}' \rangle$
$(Eq: C7.16)$

As, by definition, $rand$ is stateless
$([\![rand]\!]\sigma_{sh}).gen = rand$ $(Eq: C7.17)$

The random value generator can generate any value (The assumptions are true for any value that it generates.). If it generates v:
$v = rv([\![rand]\!]\sigma_{sh}).gen)$ $(Eq: C7.18)$

From
$Eq: C7.16$
$Eq: C7.17$
$Eq: C7.18$
it is concluded that
$\langle \langle \tau, x \coloneqq rand.gen; F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_j, \mathcal{T}^o \cdot \sigma_{sh} \cdot {\ell_{sh_1}}' \rangle \xrightarrow{\langle \tau, rand.gen \rangle}_o$ $(Eq: C7.19)$
$\langle \langle \tau, F(s), \sigma_\tau[x \mapsto v], \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau :: (\text{rand.gen}) \rangle_j, \mathcal{T}^o \cdot \sigma_{sh} \cdot {\ell_{sh_1}}' \rangle$

We define
$\mathcal{T}_2^o = \langle \tau, F(s), \sigma_\tau[x \mapsto v], \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau :: (\text{rand.gen}) \rangle_j, \mathcal{T}^o$ $(Eq: C7.20)$
${\ell_{sh_2}}' = {\ell_{sh_1}}'$ $(Eq: C7.21)$
$Conf_2^o = \langle \mathcal{T}_2^o \cdot \sigma_{sh_2} \cdot {\ell_{sh_2}}' \rangle$ $(Eq: C7.22)$

From
$Eq: C7.19$
$Eq: C7.15$
$Eq: C7.2$
$Eq: C7.20$
$Eq: C7.5$
$Eq: C7.21$
it is concluded that
$\langle \mathcal{T}_1^o \cdot \sigma_{sh_1} \cdot {\ell_{sh_1}}' \rangle \xrightarrow{\langle \tau, rand.gen \rangle}_o \langle \mathcal{T}_2^o \cdot \sigma_{sh_2} \cdot {\ell_{sh_2}}' \rangle$ $(Eq: C7.23)$

From
$Eq: C7.23$
$Eq: 4$
$Eq: C7.22$
it is concluded that
$Conf_1^o \xrightarrow{\langle \tau, rand.gen \rangle}_o Conf_2^o$
We define
$Exec = Conf_1^o \xrightarrow{\langle \tau, rand.gen \rangle}_o Conf_2^o$ $(Eq: C7.24)$

By DEFINITION 3 on $Eq: C6.24$
$Trace(Exec) = \langle \tau, rand.gen \rangle$ $(Eq: C7.25)$

From
$Eq: C6.7$
$Eq: 1$
it is concluded that
$L = \cdot$ $(Eq: C7.26)$

From
$Eq: C7.25$
$Eq: C7.26$
it is concluded that
$Trace(Exec) \ / \ rand = \ L$ $(Eq: C7.27)$

From
$Eq: C7.1$
$Eq: C7.15$
$Eq: 5$
it is concluded that
$\forall i \neq j$:
$\langle \tau', s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_i \in \mathcal{T} \Rightarrow$
$[\langle \tau', F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_i \in \mathcal{T}^o \ and \ {\ell_\tau}' \equiv \ell_\tau \ and \ (\tau' = \perp \Rightarrow \ell'_\tau = [\quad])]$ $(Eq: C7.28)$

From
$Eq: C7.4$
$Eq: C7.9$
it is concluded that
$\mathcal{T}_2 = \langle \tau, s, \sigma_\tau[x \mapsto v], \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_j, \mathcal{T}$ $(Eq: C7.29)$

By DEFINITION 6
${\ell_\tau}' :: ("rand.gen") \equiv {\ell_\tau}'$ $(Eq: C7.30)$

From
$Eq: C7.30$
$Eq: C7.12$
it is concluded that
${\ell_\tau}' :: ("rand.gen") \equiv \ell_\tau$ $(Eq: C7.31)$

From
$Eq: C7.29$
$Eq: C7.20$
$Eq: C7.28$
$Eq: C7.31$
it is concluded that
$\forall i$:
$\langle \tau', s, \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto st, \ell_\tau \rangle_i \in \mathcal{T}_2 \Rightarrow$
$[\langle \tau', F(s), \sigma_\tau, \overleftarrow{\sigma_\tau}'; stmt \mapsto F(st), \ell'_\tau \rangle_i \in \mathcal{T}_2^o \ and \ {\ell_\tau}' \equiv \ell_\tau \ and \ (\tau' = \perp \Rightarrow \ell'_\tau = [\quad])]$ $(Eq: C7.32)$

From
$Eq: C7.3$
$Eq: C7.6$
it is concluded that
$\ell_{sh_1} = \ell_{sh_2}$ $(Eq: C7.33)$

From
$Eq: C7.33$
$Eq: C7.21$
$Eq: 6$
it is concluded that
${\ell_{sh_2}}' \equiv \ell_{sh_2}$ $(Eq: C7.34)$

The conclusion of this case is
$Eq: C7.22$
$Eq: C7.24$
$Eq: C7.27$
$Eq: C7.32$
$Eq: C7.34$

LEMMA 6:
If
a history H is opaque, $(Eq: 1)$
then
for every object o, the history H/o is also opaque.

Proof:
By DEFINITION 17 on
$Eq: 1$
there exists a sequential history S equivalent to some history H' in $Complete(H)$, such that $(Eq: 2)$
S preserves the real-time order of H, $(Eq: 3)$
every transaction $T_i \in S$ is legal in S. $(Eq: 4)$

It is trivial that
$H' \in Complete(H) \Rightarrow H'/o \in Complete(H/o)$ $(Eq: 5)$
If S is an equivalent sequential history for $H \Rightarrow S/o$ is an equivalent sequential history for H/o $(Eq: 6)$
If S preserves the real-time order of H, S/o preserves the real-time order of H/o. $(Eq: 7)$

From
$Eq: 2$
$Eq: 5$
$Eq: 6$
it is concluded that
there exists the sequential history S/o equivalent to some history H'/o in $Complete(H/o)$ $(Eq: 8)$

From
$Eq: 3$
$Eq: 7$
it is concluded that
S/o preserves the real-time order of H/o. $(Eq: 9)$

By DEFINITION 16 on
$Eq: 4$
it is concluded that
For every transaction $T_i \in S$
the filtered history for T_i in S is legal. $(Eq: 10)$

By DEFINITION 15 on
$Eq: 10$
it is concluded that
For every transaction $T_i \in S$
for each obj, $H_i \mid obj \in Seq(obj)$. (where H_i is filtered history for T_i in S) $(Eq: 11)$

From
$Eq: 11$
it is concluded that
For every transaction $T_i \in S/o$
for each obj, $H_i \mid obj \in Seq(obj)$. (where H_i is filtered history for T_i in S/o) $(Eq: 12)$

By DEFINITION 15 on
$Eq: 12$
it is concluded that
For every transaction $T_i \in S/o$
the filtered history for T_i in S/o is legal. $(Eq: 13)$

By DEFINITION 16 on
$Eq: 13$
it is concluded that
every transaction $T_i \in S/o$ is legal in S/o. $(Eq: 14)$

By DEFINITION 17 on

$Eq: 8$
$Eq: 9$
$Eq: 14$

it is concluded that

the history H/o is also opaque.

10.2. Communication Safety

10.2.1. Definitions

DEFINITION 18: Let $\sqsubseteq$ be the smallest partial order of $\{\mathbb{r}, \mathbb{a}, \mathbb{c}\}$ such that $(\mathbb{r} \sqsubseteq \mathbb{c})\ and\ (\mathbb{r} \sqsubseteq \mathbb{a})$.

DEFINITION 19: Define $\mathcal{M}_1 \leq \mathcal{M}_2$ iff $\forall \tau \in dom(\mathcal{M}_1)$: $\mathcal{M}_1(\tau) \sqsubseteq \mathcal{M}_2(\tau)$.

DEFINITION 20: Define $dom(\mathcal{T}) = \{\tau \mid \langle \tau, s, \sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau \rangle \in \mathcal{T}\} \setminus \{\bot\}$

DEFINITION 21: Dependency respect:
A configuration is dependency-respecting iff
for each dependency in the configuration, the dependent transaction is committed only if the depended transaction is committed.
Formally:
Suppose
$Conf = \langle \mathcal{T} \cdot \sigma_{sh} \cdot \ell_{sh} \cdot \mathcal{M} \cdot \mathcal{C} \cdot \mathcal{D} \rangle$
$DepRespect(Conf) \triangleq$
$\forall \tau_r \rightsquigarrow \tau_s \in \mathcal{D}: (\mathcal{M}(\tau_r) = \mathbb{c} \Rightarrow \mathcal{M}(\tau_s) = \mathbb{c})$.

DEFINITION 22: State-consistency
A configuration is state-consistent iff
for every transaction that is running, its state is running and
for every transaction id, there is at most one running transaction.
Formally:
Suppose
$Conf = \langle \mathcal{T} \cdot \sigma_{sh} \cdot \ell_{sh} \cdot \mathcal{M} \cdot \mathcal{C} \cdot \mathcal{D} \rangle$
$StateConsistent(Conf) \triangleq$
$\forall \tau \in dom(\mathcal{T})$:
$\mathcal{M}(\tau) = \mathbb{r}\ and$
$\forall \tau \neq \bot: |\{\langle \tau', s, \sigma_{\tau'}, \overleftarrow{\sigma_{\tau'}}, \ell_{\tau'} \rangle \in \mathcal{T} \mid \tau' = \tau\}| \leq 1$.

10.2.2. Property Statement

THEOREM 3: Communication Safety: An initial configuration $Conf_0$ cannot execute to an unsafe configuration.
PROOF:
By contradiction on LEMMA 7.
■

10.2.3. Helper Lemmas

LEMMA 7:
At any runtime state, if a receiver is committed, the sender is committed.
Formally:
If
$Exec = Conf_0 \xrightarrow{l_0} Conf_1 \xrightarrow{l_1} \ldots \xrightarrow{l_{n-1}} Conf_n$ EQ. 1
$Conf_n = \langle \mathcal{T}_n \cdot \sigma_{sh_n} \cdot \ell_{sh_n} \cdot \mathcal{M}_n \cdot \mathcal{C}_n \cdot \mathcal{D}_n \rangle$ EQ. 2
then
$\forall \tau_r \rightsquigarrow \tau_s \in Comm(Exec)$:
$\mathcal{M}_n(\tau_r) = \mathbb{c} \Rightarrow \mathcal{M}_n(\tau_s) = \mathbb{c}$

PROOF:
By LEMMA 8 on
EQ. 1
EQ. 2
it is concluded that
$DepRespect(Conf_n)$ EQ. 3

By DEFINITION 21 on
EQ. 2
EQ. 3
it is concluded that
$\forall \tau_r \rightsquigarrow \tau_s \in \mathcal{D}_n: (\mathcal{M}_n(\tau_r) = \mathbb{c} \Rightarrow \mathcal{M}_n(\tau_s) = \mathbb{c})$ EQ. 4

By LEMMA 13 on
EQ. 1
EQ. 2
it is concluded that
$Comm(Exec) \subseteq \mathcal{D}_n$ EQ. 5

From
EQ. 4
EQ. 5
it is concluded that
$\forall \tau_r \curvearrowright \tau_s \in Comm(Exec): (\mathcal{M}_n(\tau_r) = \mathbb{c} \Rightarrow \mathcal{M}_n(\tau_s) = \mathbb{c})$ EQ. 6
■

LEMMA 8: Every execution from an initial configuration leads to a dependency-respecting and state-consistent configuration.
Formally:
If
$Exec = Conf_0 \xrightarrow{l_0} Conf_1 \xrightarrow{l_1} \ldots \xrightarrow{l_{n-1}} Conf_n$ EQ. 7
$Conf_n = \langle \mathcal{T}_n \cdot \sigma_{sh_n} \cdot \ell_{sh_n} \cdot \mathcal{M}_n \cdot \mathcal{C}_n \cdot \mathcal{D}_n \rangle$ EQ. 8
then
$DepRespect(Conf_n)$
$StateConsistent(Conf_n)$

PROOF:
Induction on the length of $Exec$:
Base case:
By definition $Conf_0 = \langle \mathcal{T}_0 \cdot \sigma_{sh_0} \cdot [] \cdot \emptyset \cdot \emptyset \cdot \emptyset \rangle$
Thus
$\mathcal{D}_0 = \emptyset$ EQ. 9

From
EQ. 9
it is concluded that
$\forall \tau_r \curvearrowright \tau_s \in \mathcal{D}_0: (\mathcal{M}_0(\tau_r) = \mathbb{c} \Rightarrow \mathcal{M}_0(\tau_s) = \mathbb{c})$ EQ. 10

By DEFINITION 21 on
EQ. 10
it is concluded that
$DepRespect(Conf_0)$ EQ. 11

By definition $\mathcal{T}_0 = \langle \bot, P_i, \sigma_{sh_0}, \sigma_{sh_0}; stmt \mapsto \bot, [\quad] \rangle_{i=1..n}$
Thus
$dom(\mathcal{T}_0) = \emptyset$ EQ. 12

From
EQ. 12
it is concluded that
$\forall \tau: (\tau \in dom(\mathcal{T}_o) \Rightarrow \mathcal{M}_0(\tau) = \mathbb{t})$ *and*
$\forall \tau \neq \bot: |\{\langle \tau', s, \sigma_{\tau'}, \overleftarrow{\sigma_{\tau'}}, \ell_{\tau'} \rangle \in \mathcal{T} \mid \tau' = \tau\}| \leq 1$ EQ. 13

By DEFINITION 22 on
EQ. 13
it is concluded that
$StateConsistent(Conf_0)$ EQ. 14

The conclusion for this case is
EQ. 11
EQ. 14

Inductive case:
Induction hypothesis:

If

$Exec' = Conf_0 \xrightarrow{l_0} Conf_1 \xrightarrow{l_1} \dots \xrightarrow{l_{n-2}} Conf_{n-1}$

$Conf_{n-1} = \langle \mathcal{T}_{n-1} \cdot \sigma_{sh_{n-1}} \cdot \ell_{sh_{n-1}} \cdot \mathcal{M}_{n-1} \cdot \mathcal{C}_{n-1} \cdot \mathcal{D}_{n-1} \rangle$

then

$DepRespect(Conf_{n-1})$

$StateConsistent(Conf_{n-1})$

From

EQ. 7

it is concluded that

$Conf_0 \xrightarrow{l_0} Conf_1 \xrightarrow{l_1} \dots \xrightarrow{l_{n-2}} Conf_{n-1}$ EQ. 15

$Conf_{n-1} \xrightarrow{l_{n-1}} Conf_n$ EQ. 16

We define

$Exec' = Conf_0 \xrightarrow{l_0} Conf_1 \xrightarrow{l_1} \dots \xrightarrow{l_{n-2}} Conf_{n-1}$ EQ. 17

$Conf_{n-1} = \langle \mathcal{T}_{n-1} \cdot \sigma_{sh_{n-1}} \cdot \ell_{sh_{n-1}} \cdot \mathcal{M}_{n-1} \cdot \mathcal{C}_{n-1} \cdot \mathcal{D}_{n-1} \rangle$ EQ. 18

By induction hypothesis on

EQ. 17

EQ. 18

it is concluded that

$DepRespect(Conf_{n-1})$ EQ. 19

$StateConsistent(Conf_{n-1})$ EQ. 20

By LEMMA 9 on

EQ. 16

EQ. 19

EQ. 20

it is concluded that

$DepRespect(Conf_n)$

$StateConsistent(Conf_n)$

■

LEMMA 9: The operational semantics preserves dependency-respect and state-consistency.
Formally:

If

$Conf_1 \xrightarrow{l} Conf_2$ EQ. 21

$DepRespect(Conf_1)$ EQ. 22

$StateConsistent(Conf_1)$ EQ. 23

then

$DepRespect(Conf_2)$

$StateConsistent(Conf_2)$

PROOF:

We define

$Conf_1 = \langle \mathcal{T}_1 \cdot \sigma_{sh_1} \cdot \ell_{sh_1} \cdot \mathcal{M}_1 \cdot \mathcal{C}_1 \cdot \mathcal{D}_1 \rangle$ EQ. 24

$Conf_2 = \langle \mathcal{T}_2 \cdot \sigma_{sh_2} \cdot \ell_{sh_2} \cdot \mathcal{M}_2 \cdot \mathcal{C}_2 \cdot \mathcal{D}_2 \rangle$ EQ. 25

Consider an arbitrary transaction id τ_r

Suppose $\mathcal{M}_2(\tau_r) = \mathbb{c}$ EQ. 26

We show that

$\forall \tau_r \rightsquigarrow \tau_s \in \mathcal{D}_2 : \mathcal{M}_2(\tau_s) = \mathbb{c}$ EQ. 27

We consider two cases:

If $\mathcal{M}_1(\tau_r) \neq \mathbb{c}$ EQ. 28

From

EQ. 24

EQ. 25

EQ. 28

EQ. 26

CMT is the only rule that updates the state of a transaction in $\mathcal{M}$ to $\mathbb{c}$,
it is concluded that
the reduction of EQ. 21 is done by the CMT rule.
From the CMT rule, it is concluded that

$\mathcal{M}_2 = \mathcal{M}_1[\tau_i \mapsto \mathbb{c}]_{i=1..n}$ EQ. 29

$\exists i \in \{1..n\}: \tau_r = \tau_i$ EQ. 30

$$\text{Cluster}(\{\tau_{i=1..n}\}, \mathcal{M}_1, \mathcal{D}_1) = \forall i \in \{1 \dots n\}: \begin{bmatrix} \forall \tau: ((\tau_i \rightsquigarrow \tau) \in \mathcal{D}_1) \Rightarrow \\ \begin{pmatrix} (\mathcal{M}_1(\tau) = \mathbb{c})\ or \\ (\exists j \in \{1 \dots n\}: \tau = \tau_j) \end{pmatrix} \end{bmatrix} \quad \text{EQ. 31}$$

$\mathcal{D}_2 = \mathcal{D}_1$ EQ. 32

Replacing τ with τ_s and
substituting
EQ. 30
EQ. 32
in EQ. 31, we have

$$\forall \tau_s: \big((\tau_r \rightsquigarrow \tau_s) \in \mathcal{D}_2\big) \Rightarrow \begin{pmatrix} (\mathcal{M}_1(\tau_s) = \mathbb{c})\ or \\ (\exists j \in \{1 \dots n\}: \tau_s = \tau_j) \end{pmatrix} \quad \text{EQ. 33}$$

From
EQ. 29
it is concluded that

$\forall \tau_s: (\mathcal{M}_1(\tau_s) = \mathbb{c}) \Rightarrow (\mathcal{M}_2(\tau_s) = \mathbb{c})$ EQ. 34

$\forall i \in \{1 \dots n\}: \ (\mathcal{M}_2(\tau_i) = \mathbb{c})$ EQ. 35

Substituting
EQ. 34 for the first disjunct and
EQ. 35 for the second disjunct
of EQ. 33
it is concluded that

$$\forall \tau_s: \big((\tau_r \rightsquigarrow \tau_s) \in \mathcal{D}_2\big) \Rightarrow \begin{pmatrix} (\mathcal{M}_2(\tau_s) = \mathbb{c})\ or \\ (\mathcal{M}_2(\tau_s) = \mathbb{c}) \end{pmatrix} \quad \text{EQ. 36}$$

Simplifying EQ. 36
it is concluded that

$\forall \tau_s: \big((\tau_r \rightsquigarrow \tau_s) \in \mathcal{D}_2\big) \Rightarrow (\mathcal{M}_2(\tau_s) = \mathbb{c})$ EQ. 37

that is equivalent to

$\forall (\tau_r \rightsquigarrow \tau_s) \in \mathcal{D}_2: \mathcal{M}_2(\tau_s) = \mathbb{c}$ EQ. 38

If $\mathcal{M}_1(\tau_r) = \mathbb{c}$ EQ. 39

From DEFINITION 21 on
EQ. 22
EQ. 24
it is concluded that

$\forall \tau_r \rightsquigarrow \tau_s \in \mathcal{D}_1: (\mathcal{M}_1(\tau_r) = \mathbb{c} \Rightarrow \mathcal{M}_1(\tau_s) = \mathbb{c})$ EQ. 40

From
EQ. 39
EQ. 40
it is concluded that

$\forall \tau_r \rightsquigarrow \tau_s \in \mathcal{D}_1: \mathcal{M}_1(\tau_s) = \mathbb{c}$ EQ. 41

By DEFINITION 22 on
EQ. 23
EQ. 24
it is concluded that

$\forall \tau \in dom(\mathcal{T}_1): \mathcal{M}_1(\tau) = \mathbb{r}$ EQ. 42

By LEMMA 10 on
EQ. 21
EQ. 24
EQ. 25
EQ. 39
EQ. 42
it is concluded that
$\{\tau_s | \tau_r \curvearrowright \tau_s \in D_2\} = \{\tau_s | \tau_r \curvearrowright \tau_s \in D_1\}$ EQ. 43

From
EQ. 41
EQ. 43
it is concluded that
$\forall \tau_r \curvearrowright \tau_s \in \mathcal{D}_2: \mathcal{M}_1(\tau_s) = \mathbb{c}$ EQ. 44

By LEMMA 12 on
EQ. 21
EQ. 24
EQ. 25
EQ. 42
it is concluded that
$\mathcal{M}_1 \leq \mathcal{M}_2$ EQ. 45

From DEFINITION 19 and DEFINITION 18 on
EQ. 45
it is concluded that
$\forall \tau: \mathcal{M}_1(\tau) = \mathbb{c} \Rightarrow \mathcal{M}_2(\tau) = \mathbb{c}$ EQ. 46

From
EQ. 44
EQ. 46
it is concluded that
$\forall \tau_r \curvearrowright \tau_s \in \mathcal{D}_2: \mathcal{M}_2(\tau_s) = \mathbb{c}$ EQ. 47

From
EQ. 26
EQ. 27
it is concluded that
$\forall \tau_r: \mathcal{M}_2(\tau_r) = \mathbb{c}: (\forall \tau_r \curvearrowright \tau_s \in \mathcal{D}_2 \Rightarrow \mathcal{M}_2(\tau_s) = \mathbb{c})$ EQ. 48
That is equivalent to
$\forall \tau_r \curvearrowright \tau_s \in \mathcal{D}_2: (\mathcal{M}_2(\tau_r) = \mathbb{c} \Rightarrow \mathcal{M}_2(\tau_s) = \mathbb{c})$ EQ. 49

By DEFINITION 21 on
EQ. 25
EQ. 49
it is concluded that
$DepRespect(Conf_2)$ EQ. 50

By LEMMA 11 on
EQ. 21
EQ. 23
it is concluded that
$StateConsistent(Conf_2)$ EQ. 51

The conclusion is
EQ. 50
EQ. 51
■

LEMMA 10: The set of dependencies of a committed transaction do not change.

If

$Conf_1 \xrightarrow{\iota} Conf_2$ EQ. 52

$Conf_1 = \langle \mathcal{T}_1 \cdot \sigma_{sh_1} \cdot \ell_{sh_1} \cdot \mathcal{M}_1 \cdot \mathcal{C}_1 \cdot \mathcal{D}_1 \rangle$ EQ. 53

$Conf_2 = \langle \mathcal{T}_2 \cdot \sigma_{sh_2} \cdot \ell_{sh_2} \cdot \mathcal{M}_2 \cdot \mathcal{C}_2 \cdot \mathcal{D}_2 \rangle$ EQ. 54

$\mathcal{M}_1(\tau) = \mathbb{c}$ EQ. 55

$\forall \tau: (\tau \in dom(\mathcal{T}_1): \mathcal{M}_1(\tau) = \mathbb{r})$ EQ. 56

then

$\{\tau_s | \tau \rightsquigarrow \tau_s \in D_2\} = \{\tau_s | \tau \rightsquigarrow \tau_s \in D_1\}$

PROOF:

Case analysis on EQ. 52

Case: Six Rules (Rules other than $Receive$):

$\mathcal{D}_2 = \mathcal{D}_1$ EQ. 57

Therefore

$\{\tau_s | \tau \rightsquigarrow \tau_s \in D_2\} = \{\tau_s | \tau \rightsquigarrow \tau_s \in D_1\}$

Case: Rule $Receive$:

Form rule $Receive$ on

EQ. 53

EQ. 54

it is concluded that

$\tau_r \neq \perp$ EQ. 58

$\mathcal{T}_1 = \langle \tau_r, x \coloneqq ch\ receive; s, \sigma_{\tau_r}, \overleftarrow{\sigma_{\tau_r}}, \ell_{\tau_r} \rangle, \mathcal{T}$ EQ. 59

$\mathcal{D}_2 = \mathcal{D}_1 \cup \{\tau_r \rightsquigarrow \tau_s\}$ EQ. 60

By DEFINITION 20 on

EQ. 59

EQ. 67

it is concluded that

$\tau_r \in dom(\mathcal{T}_1)$ EQ. 61

From

EQ. 56

EQ. 61

it is concluded that

$\mathcal{M}_1(\tau_r) = \mathbb{r}$ EQ. 62

From

EQ. 55

EQ. 62

it is concluded that

$\tau_r \neq \tau$ EQ. 63

From

EQ. 60

EQ. 63

it is concluded that

$\{\tau_s | \tau \rightsquigarrow \tau_s \in D_2\} = \{\tau_s | \tau \rightsquigarrow \tau_s \in D_1\}$

■

LEMMA 11: The semantics preserves state-consistency.

If

$Conf_1 \xrightarrow{\iota} Conf_2$ EQ. 64

$StateConsistent(Conf_1)$ EQ. 65

then

$StateConsistent(Conf_2)$

PROOF:

Suppose

$Conf_1 = \langle \mathcal{T}_1 \cdot \sigma_{sh_1} \cdot \ell_{sh_1} \cdot \mathcal{M}_1 \cdot \mathcal{C}_1 \cdot \mathcal{D}_1 \rangle$ EQ. 66

$Conf_2 = \langle \mathcal{T}_2 \cdot \sigma_{sh_2} \cdot \ell_{sh_2} \cdot \mathcal{M}_2 \cdot \mathcal{C}_2 \cdot \mathcal{D}_2 \rangle$ EQ. 67

By DEFINITION 22 on
EQ. 65
EQ. 66
it is concluded that
$\forall \tau \in dom(\mathcal{T}_1): (\mathcal{M}_1(\tau) = \mathbb{r})$ EQ. 68
$\forall \tau \neq \perp: |\{\langle \tau', s, \sigma_{\tau\prime}, \overleftarrow{\sigma_{\tau\prime}}, \ell_{\tau\prime}\rangle \in \mathcal{T}_1 | \ \tau' = \tau\}| \leq 1$ EQ. 69

We show that
$\forall \tau \neq \perp: |\{\langle \tau', s, \sigma_{\tau\prime}, \overleftarrow{\sigma_{\tau\prime}}, \ell_{\tau\prime}\rangle \in \mathcal{T}_2 | \ \tau' = \tau\}| \leq 1$ EQ. 70
Case analysis on EQ. 66
Case CMD, APP, CMT, ABT, $Send$, $Receive$:
In each of these rules, we have
$\forall \tau \neq \perp: \{\langle \tau', s, \sigma_{\tau\prime}, \overleftarrow{\sigma_{\tau\prime}}, \ell_{\tau\prime}\rangle \in \mathcal{T}_2 | \ \tau' = \tau\} \subseteq \{\langle \tau', s, \sigma_{\tau\prime}, \overleftarrow{\sigma_{\tau\prime}}, \ell_{\tau\prime}\rangle \in \mathcal{T}_1 | \ \tau' = \tau\}$ EQ. 71

From
EQ. 69
EQ. 75
it is concluded that
$\forall \tau \neq \perp: |\{\langle \tau', s, \sigma_{\tau\prime}, \overleftarrow{\sigma_{\tau\prime}}, \ell_{\tau\prime}\rangle \in \mathcal{T}_2 | \ \tau' = \tau\}| \leq |\{\langle \tau', s, \sigma_{\tau\prime}, \overleftarrow{\sigma_{\tau\prime}}, \ell_{\tau\prime}\rangle \in \mathcal{T}_1 | \ \tau' = \tau\}| \leq 1$ EQ. 72

Case BEG:
From the BEG rule, we have
$\mathcal{T}_2 = \langle \langle \text{fresh}(\tau'), s, \text{snap}(\sigma_\tau, \sigma_{sh}), \sigma_\tau[\text{stmt} \mapsto \text{"beg; } s\text{"}], []\rangle, \mathcal{T} \cdot \sigma_{sh} \cdot \ell_{sh} \cdot \mathcal{M}' \cdot \mathcal{C} \cdot \mathcal{D}\rangle$ EQ. 73
$\tau' is\ fresh$ EQ. 74

From
EQ. 69
EQ. 73
EQ. 74
it is concluded that
$|\{\langle \tau', s, \sigma_{\tau\prime}, \overleftarrow{\sigma_{\tau\prime}}, \ell_{\tau\prime}\rangle \in \mathcal{T}_2 \mid \tau' = \tau\}| = 1 \leq 1$

It remains to show that
$\forall \tau \in dom(\mathcal{T}_2): (\mathcal{M}_2(\tau) = \mathbb{r})$ EQ. 75
We proceed by
Case analysis on the rule used to derive $Conf_1 \xrightarrow{l} Conf_2$:
Cases CMD, APP, CMT, ABT, $Send$, $Receive$:
In each of these rules, we have
$dom(\mathcal{T}_2) \subseteq dom(\mathcal{T}_1)$, and if
we let $\mathcal{M}_1'$ be $\mathcal{M}_1$ restricted to $dom(\mathcal{T}_2)$ and
we let $\mathcal{M}_2'$ be $\mathcal{M}_2$ restricted to $dom(\mathcal{T}_2)$,
then we have
$\mathcal{M}_2' = \mathcal{M}_1'$ EQ. 76

So $\forall \tau \in dom(\mathcal{T}_2)$, from
EQ. 68
EQ. 76
it is concluded that
$\mathcal{M}_2(\tau) = \mathcal{M}_2'(\tau) = \mathcal{M}_1'(\tau) = \mathcal{M}_1(\tau) = \mathbb{r}$

Case BEG:
We have
$dom(\mathcal{T}_2) = dom(\mathcal{T}_1) \cup \{\tau\}$ and
$\mathcal{M}_2 = \mathcal{M}_1 \cup \{\tau \mapsto \mathbb{r}\}$, where $is\ fresh.$ EQ. 77

From
EQ. 68
EQ. 77
it is concluded that
$\forall \tau \in dom(\mathcal{T}_2): (\mathcal{M}_2(\tau) = \mathbb{r})$

By DEFINITION 22 on
EQ. 75
EQ. 70
it is concluded that
$StateConsistent(Conf_2)$
■

LEMMA 12:
If
$Conf_1 \xrightarrow{l} Conf_2$ EQ. 78
$Conf_1 = \langle \mathcal{T}_1 \cdot \sigma_{sh_1} \cdot \ell_{sh_1} \cdot \mathcal{M}_1 \cdot \mathcal{C}_1 \cdot \mathcal{D}_1 \rangle$ EQ. 79
$Conf_2 = \langle \mathcal{T}_2 \cdot \sigma_{sh_2} \cdot \ell_{sh_2} \cdot \mathcal{M}_2 \cdot \mathcal{C}_2 \cdot \mathcal{D}_2 \rangle$ EQ. 80
$\forall \tau \in dom(\mathcal{T}_1) : (\mathcal{M}_1(\tau) = \mathbb{r})$ EQ. 81
then
$\mathcal{M}_1 \leq \mathcal{M}_2$

PROOF:
Case analysis on the rule used to derive $Conf_1 \xrightarrow{l} Conf_2$.
Cases CMD, APP, $Send$, $Receive$:
We have $\mathcal{M}_1 = \mathcal{M}_2$,
Hence $\mathcal{M}_1 \leq \mathcal{M}_2$.

Case BEG:
We have $\mathcal{M}_1 = \mathcal{M}_1 \cup \{\tau \mapsto \mathbb{r}\}$ where $\tau \notin dom(\mathcal{M}_1)$.
Hence, $\forall \tau \in dom(\mathcal{M}_1) : \mathcal{M}_1(\tau) = \mathcal{M}_2(\tau)$, so $\mathcal{M}_1 \leq \mathcal{M}_2$.

Case CMT:
we have
$\mathcal{M}_2 = \mathcal{M}_1[\tau_i \mapsto \mathbb{c}]_{i=1..c}$ EQ. 82
$\mathcal{T}_1 = \langle \tau_i, end; s_i, \sigma_{\tau_i}, \overline{\sigma_{\tau_i}}, \ell_{\tau_i} \rangle_{i=1..c}, \mathcal{T}$ EQ. 83

From
EQ. 82
EQ. 83
it is concluded that
$dom(\mathcal{M}_1) = dom(\mathcal{M}_2)$ EQ. 84
$\forall \tau' \in dom(\mathcal{M}_1) \setminus \{\tau_{i=1..c}\} : \mathcal{M}_1(\tau') = \mathcal{M}_2(\tau')$ EQ. 85

From
EQ. 83
EQ. 81
it is concluded that
$\forall i \in \{1..n\} : \mathcal{M}_1(\tau_i) = \mathbb{r}$ EQ. 86

From
EQ. 86
EQ. 82
DEFINITION 18
it is concluded that
$\forall i \in \{1..n\} : \mathcal{M}_1(\tau_i) = \mathbb{r} \sqsubseteq \mathbb{a} = \mathcal{M}_2(\tau_i)$ EQ. 87

From DEFINITION 19 on
EQ. 84
EQ. 85
EQ. 87
it is concluded that
$\mathcal{M}_1 \leq \mathcal{M}_2$

Case of ABT:
We have

$\mathcal{M}_2 = \mathcal{M}_1[\tau \mapsto \mathbb{a}]$ EQ. 88
$\mathcal{T}_1 = \langle \tau, s, \sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau \rangle, \mathcal{T}$ EQ. 89

From
EQ. 88
EQ. 89
it is concluded that
$dom(\mathcal{M}_1) = dom(\mathcal{M}_2)$ EQ. 90
$\forall \tau' \in dom(\mathcal{M}_1) \setminus \{\tau\}: \mathcal{M}_1(\tau') = \mathcal{M}_2(\tau')$ EQ. 91

From
EQ. 89
EQ. 81
it is concluded that
$\mathcal{M}_1(\tau) = \mathbb{r}$ EQ. 92

From
EQ. 88
EQ. 92
DEFINITION 18
it is concluded that
$\mathcal{M}_1(\tau) = \mathbb{r} \sqsubseteq \mathbb{a} = \mathcal{M}_2(\tau)$ EQ. 93

From DEFINITION 19 on
EQ. 90
EQ. 93
EQ. 91
we have
$\mathcal{M}_1 \leq \mathcal{M}_2$

■

LEMMA 13: The set of dependencies $\mathcal{D}$ and the communication relation $Comm$ are equivalent.
If
$Exec = Conf_0 \xrightarrow{l_0} Conf_1 \xrightarrow{l_1} \dots \xrightarrow{l_{n-1}} Conf_n$ EQ. 94
$Conf_n = \langle \mathcal{T}_n \cdot \sigma_{sh_n} \cdot \ell_{sh_n} \cdot \mathcal{M}_n \cdot \mathcal{C}_n \cdot \mathcal{D}_n \rangle$ EQ. 95
then
$Comm(Exec) = \mathcal{D}_n$

PROOF:
We first show the completeness of D:
$\forall \tau_r \rightsquigarrow \tau_s \in Comm(Exec): \tau_r \rightsquigarrow \tau_s \in \mathcal{D}_n$

By DEFINITION 1 on
EQ. 94
$\tau_r \rightsquigarrow \tau_s \in Comm(Exec)$
it is concluded that
$\exists i, j, ch \quad 0 \leq i < j < n$:
$l_i = (\tau_s, ch\ send)$ EQ. 96
$l_j = (\tau_r, ch\ receive)$ EQ. 97
$\forall k: \quad (i < k < j) \Rightarrow \forall \tau_s{}': l_k \neq (\tau_s{}', ch\ send)$ EQ. 98

The only rule where its label matches $(\tau_s, c\ send)$ is the rule $Send$.Thus, from EQ. 96 we have
$Conf_i = \langle \langle \tau_s, ch\ send\ v; s, \sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau \rangle, \mathcal{T} \cdot \sigma_{sh} \cdot \ell_{sh} \cdot \mathcal{M} \cdot \mathcal{C}_i \cdot \mathcal{D} \rangle$ EQ. 99
$Conf_{i+1} = \langle \langle \tau_s, s, \sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau \rangle, \mathcal{T} \cdot \sigma_{sh} \cdot \ell_{sh} \cdot \mathcal{M} \cdot \mathcal{C}_{i+1} \cdot \mathcal{D} \rangle$ EQ. 100
$\mathcal{C}_{i+1} = \mathcal{C}_i[ch \mapsto \langle \tau_s, v \rangle]$ EQ. 101

From
EQ. 101
it is concluded that
$\mathcal{C}_{i+1}(ch) = \langle \tau_s, v \rangle$ EQ. 102

From
EQ. 94
it is concluded that
$Exec = Conf_{i+1} \xrightarrow{l_{i+1}} \dots \xrightarrow{l_{j-1}} Conf_j$ EQ. 103

We define that
$Conf_j = \langle \mathcal{T}_j \cdot \sigma_{sh_j} \cdot \ell_{sh_j} \cdot \mathcal{M}_j \cdot \mathcal{C}_j \cdot \mathcal{D}_j \rangle$ EQ. 104

By LEMMA 15 (plus induction on the number of steps) on
EQ. 103
EQ. 100
EQ. 104
EQ. 98
it is concluded that
$\mathcal{C}_j(ch) = \mathcal{C}_{i+1}(ch)$ EQ. 105

From
EQ. 102
EQ. 105
It is concluded that
$\mathcal{C}_j(ch) = \langle \tau_s, v \rangle$ EQ. 106

The only rule that its label matches $(\tau_r, c\ receive)$ is the $Receive$ rule. Thus, from EQ. 97 and EQ. 106, we have
$Conf_j = \langle \langle \tau_r, x \coloneqq ch\ receive; s, \sigma_\tau, \overline{\sigma_\tau}, \ell_\tau \rangle, \mathcal{T} \cdot \sigma_{sh} \cdot \ell_{sh} \cdot \mathcal{M} \cdot \mathcal{C} \cdot \mathcal{D}_j \rangle$ EQ. 107
$Conf_{j+1} = \langle \langle \tau_r, s, \sigma_\tau[x \mapsto v], \overline{\sigma_\tau}, \ell_\tau \rangle, \mathcal{T} \cdot \sigma_{sh} \cdot \ell_{sh} \cdot \mathcal{M} \cdot \mathcal{C} \cdot \mathcal{D}_{j+1} \rangle$ EQ. 108
$\mathcal{D}_{j+1} = \mathcal{D}_j \cup \{\tau_r \rightsquigarrow \tau_s\}$ EQ. 109

From
EQ. 109
it is concluded that
$\tau_r \rightsquigarrow \tau_s \in \mathcal{D}_{j+1}$ EQ. 110

Form
EQ. 94
it is concluded that
$Conf_{j+1} \xrightarrow{l_{j+1}} \dots \xrightarrow{l_{n-1}} Conf_n$ EQ. 111

By LEMMA 16 (plus induction on the number of steps) on
EQ. 111
EQ. 108
EQ. 95
it is concluded that
$\mathcal{D}_{j+1} \subseteq \mathcal{D}_n$ EQ. 112

From
EQ. 112
EQ. 110
it is concluded that
$\tau_r \rightsquigarrow \tau_s \in \mathcal{D}_n$

We now show the accuracy of D:
We show that
$\forall \tau_r \rightsquigarrow \tau_s \in \mathcal{D}_n : \tau_r \rightsquigarrow \tau_s \in Comm(Exec)$

We define that for $1 \leq i \leq n$
$Conf_i = \langle \mathcal{T}_i \cdot \sigma_{sh_i} \cdot \ell_{sh_i} \cdot \mathcal{M}_i \cdot \mathcal{C}_i \cdot \mathcal{D}_i \rangle$ EQ. 113

We accuracy this by proving the stronger property
$\forall i : 0 \leq i \leq n : \mathcal{D}_i \subseteq Comm(Exec)$

We proceed by induction on i:

Base case:

By definition $Conf_0 = \langle \mathcal{T}_0 \cdot \sigma_{sh_0} \cdot [] \cdot \emptyset \cdot \emptyset \cdot \emptyset \rangle$

Thus

$\mathcal{D}_0 = \emptyset$ EQ. 114

From

EQ. 114

it is concluded that

$\mathcal{D}_0 \subseteq Comm(Exec)$ EQ. 115

Inductive case:

Induction hypothesis:

$\mathcal{D}_{i-1} \subseteq Comm(Exec)$ EQ. 116

Suppose $\tau_r \rightsquigarrow \tau_s \in \mathcal{D}_i$: EQ. 117

We consider two cases:

Case $\tau_r \rightsquigarrow \tau_s \in \mathcal{D}_{i-1}$: EQ. 118

By

EQ. 116

EQ. 118

it is concluded that

$\tau_r \rightsquigarrow \tau_s \in Comm(Exec)$ EQ. 119

Case $\tau_r \rightsquigarrow \tau_s \notin \mathcal{D}_{n-1}$: EQ. 120

From

EQ. 120

EQ. 117

The only rule that updates $\mathcal{D}$ is the $Receive$ rule.

it is concluded that

$Conf_{i-1} \xrightarrow{l_{i-1}} Conf_i$ is by the $Receive$ rule.

From rule $Receive$ on

EQ. 113

it is concluded that

$l_{i-1} = \langle \tau_r, ch\ receive \rangle$ EQ. 121

$\mathcal{C}_{i-1}(ch) = \langle \tau_s, v \rangle$ EQ. 122

From LEMMA 14 on

$Conf_0 \xrightarrow{l_0} \dots \xrightarrow{l_{i-2}} Conf_{i-1} \xrightarrow{l_{i-1}} Conf_i$

EQ. 113

EQ. 122

it is concluded that

$\exists \tau_s, p$:

$0 \leq p < i-1, l_p = (\tau_s, ch\ send)$ EQ. 123

$\forall k: (p < k < i-1) \Rightarrow \big(\forall \tau: l_k \neq (\tau, ch\ send)\big)$

Thus

$\exists \tau_s, p$:

$0 \leq p < i, l_p = (\tau_s, ch\ send)$ EQ. 124

$\forall k: (p < k < i-1) \Rightarrow \big(\forall \tau: l_k \neq (\tau, ch\ send)\big)$

From

EQ. 121

EQ. 124

it is concluded that

$\exists p, q = i-1, ch$: $0 \leq p < q < n$,

$l_p = (\tau_s, ch\ send), l_q = (\tau_r, ch\ receive)$ EQ. 125

$\forall k: (p < k < q) \Rightarrow \big(\forall \tau: l_k \neq (\tau, ch\ send)\big)$

From DEFINITION 1 on
EQ. 125
it is concluded that
$\tau_r \curvearrowright \tau_s \in Comm(Exec)$

■

LEMMA 14: Every message is sent by a sender.
If
$Exec = Conf_0 \xrightarrow{l_0} Conf_1 \xrightarrow{l_1} \dots \xrightarrow{l_{n-1}} Conf_n$ EQ. 126
$Conf_n = \langle \mathcal{T}_n \cdot \sigma_{sh_n} \cdot \ell_{sh_n} \cdot \mathcal{M}_n \cdot \mathcal{C}_n \cdot \mathcal{D}_n \rangle$ EQ. 127
$\mathcal{C}_n(ch) = \langle \tau_s, v \rangle$ EQ. 128
then
$\exists \tau_s, i$:
$0 \leq i < n, l_i = (\tau_s, ch\ send)$
$\forall j: (i < j < n) \Rightarrow \left(\forall \tau: l_j \neq (\tau, ch\ send)\right)$

PROOF:
First, we show that
$\exists \tau_s, j: 0 \leq j < n, l_j = (\tau_s, ch\ send)$ EQ. 129

Proof by contradiction: If
$\nexists \tau_s, j: 0 \leq j < n, l_j = (\tau_s, ch\ send)$ EQ. 130
That is equivalent to
$\forall \tau_s, j: 0 \leq j < n \Rightarrow l_j \neq (\tau_s, ch\ send)$ EQ. 131
That is equivalent to
$\forall j: 0 \leq j < n \Rightarrow \forall \tau_s: l_j \neq (\tau_s, ch\ send)$ EQ. 132

By definition
$Conf_0 = \langle \mathcal{T}_0 \cdot \sigma_{sh_0} \cdot [] \cdot \emptyset \cdot \mathcal{C}_0 \cdot \emptyset \rangle$ EQ. 133
$\mathcal{C}_0 = \emptyset$
Thus
$ch \notin \mathcal{C}_0$ EQ. 134

By LEMMA 15 (plus induction on the number of steps) on
EQ. 126
EQ. 133
EQ. 127
EQ. 132
it is concluded that
$\mathcal{C}_n(ch) = \mathcal{C}_0(ch)$ EQ. 135

From
EQ. 128
EQ. 135
it is concluded that
$\mathcal{C}_0(ch) = \langle \tau_s, v \rangle$ EQ. 136

There is a contradiction between
EQ. 134
EQ. 136

From
EQ. 129
let i be the largest possible j that is
$\exists \tau_s, i: 0 \leq i < n, l_i = (\tau_s, ch\ send)$
$\nexists \tau'_s, j: i < j < n, l_i = (\tau'_s, ch\ send)$ EQ. 137
that is equivalent to
$\exists \tau_s, i: 0 \leq i < n, l_i = (\tau_s, ch\ send)$
$\forall \tau'_s, j: (i < j < n) \Rightarrow \left(l_i \neq (\tau'_s, ch\ send)\right)$ EQ. 138

that is equivalent to

$\exists \tau_s, i: 0 \leq i < n, l_i = (\tau_s, ch\ send)$
$\forall j: (i < j < n) \Rightarrow \left(\forall \tau_s': l_i \neq (\tau_s', ch\ send)\right)$ EQ. 139

■

LEMMA 15:
If no message is sent to a channel, the value of a channel remains unchanged.
Formally:
If

$Conf_1 \xrightarrow{l} Conf_2$ EQ. 140
$Conf_1 = \langle \mathcal{T}_1 \cdot \sigma_{sh_1} \cdot \ell_{sh_1} \cdot \mathcal{M}_1 \cdot \mathcal{C}_1 \cdot \mathcal{D}_1 \rangle$ EQ. 141
$Conf_n = \langle \mathcal{T}_2 \cdot \sigma_{sh_2} \cdot \ell_{sh_2} \cdot \mathcal{M}_2 \cdot \mathcal{C}_2 \cdot \mathcal{D}_2 \rangle$ EQ. 142
$\forall \tau: l \neq \langle \tau, ch\ send \rangle$ EQ. 143

then

$\mathcal{C}_2(ch) = \mathcal{C}_1(ch)$

PROOF:
Case analysis on $Conf_1 \xrightarrow{l} Conf_2$

Case rule $Send$:

$\mathcal{C}_2 = \mathcal{C}_1[ch' \mapsto \langle \tau, v \rangle]$ EQ. 144
$l = \langle \tau, ch'\ send \rangle$ EQ. 145

We consider two cases

If $(ch = ch')$ EQ. 146

From

EQ. 145
EQ. 146

it is concluded that

$l = \langle \tau, ch\ send \rangle$ EQ. 147

That is a contradiction to EQ. 143.

If $(ch \neq ch')$ EQ. 148

From

EQ. 144
EQ. 148

it is concluded that

$\mathcal{C}_2(ch) = \mathcal{C}_1(ch)$ EQ. 149

Case other six rules:

In each of these rules:

$\mathcal{C}_2 = \mathcal{C}_1$ EQ. 150

Thus:

$\mathcal{C}_2(ch) = \mathcal{C}_1(ch)$ EQ. 151

■

LEMMA 16:
Dependencies are maintained through the execution.
Formally:
If

$Conf_1 \xrightarrow{l} Conf_2$ EQ. 152
$Conf_1 = \langle \mathcal{T}_1 \cdot \sigma_{sh_1} \cdot \ell_{sh_1} \cdot \mathcal{M}_1 \cdot \mathcal{C}_1 \cdot \mathcal{D}_1 \rangle$ EQ. 153
$Conf_2 = \langle \mathcal{T}_2 \cdot \sigma_{sh_2} \cdot \ell_{sh_2} \cdot \mathcal{M}_2 \cdot \mathcal{C}_2 \cdot \mathcal{D}_2 \rangle$ EQ. 154

then

$\mathcal{D}_1 \subseteq \mathcal{D}_2$

PROOF:
We proceed by case analysis on the rule used to derive $Conf_1 \xrightarrow{l} Conf_2$. For six of the rules, we have $\mathcal{D}_1 = \mathcal{D}_2$, hence $\mathcal{D}_1 \subseteq \mathcal{D}_2$. For the seventh rule, $Receive$, we have $\mathcal{D}_1 = \mathcal{D}_2 \cup \{\tau \rightsquigarrow \tau'\}$, hence $\mathcal{D}_1 \subseteq \mathcal{D}_2$.

■

11. Updates to the Semantics in Figure 3

We have fixed a few typos in the syntax and semantics, after personal communication with the authors of [15].

11.1. Syntax

The original grammar is

$s \to s; s \mid beg; t; end \mid c$	*Statement*
$t \to t; t \mid x \coloneqq o.m \mid c$	*Term*
$c \to c; c \mid e \coloneqq e \mid if\ b\ then\ c\ else\ c$	*Command*

The problem with the grammar in the original paper is that the grammar defines $beg;\ t;\ end$ as a single statement, while the semantics splits it into $beg;\ s$ and end, and reduces them in two different rules. The following two rewritings can be considered for the grammar.

$c \to (some\ command)$
$s \to c;\ s \mid beg\ t;\ s \mid skip$
$t \to c;\ t \mid o.m;\ t \mid end$

$s \to i; s \mid i$	*Statement*
$i \to beg \mid end \mid x \coloneqq o.m \mid$ c $\mid$ skip	*Instruction*

If the first one is used, some of s's need to be changed to t's in the semantics.
If the second one is used, the semantics remains unchanged.
Programs with nested begs and ends can be written with the first grammar. Similarly unmatched begs and ends can be written with the second grammar. The semantics is not intended for these programs. Although this does not have any effect on the correctness of semantics and theorems, a pre-phase can filter such programs.
To have the minimum possible change to the semantics, we selected the second grammar.

11.2. Operational Semantics

- The grammar has an if command, while the semantics of if does not change the evaluation flow in the CMD rule. Therefore if is removed from the set of commands.

- In the definition of snap, $o.m$ is changed to o
It is fixed from
$\text{snap}(\sigma_\tau, \sigma_{sh}) = \sigma_\tau[o \mapsto [\![o.m]\!]\sigma_{sh}] \quad \forall o \in \text{objects}(P)$
to
$\text{snap}(\sigma_\tau, \sigma_{sh}) = \sigma_\tau[o \mapsto [\![o]\!]\sigma_{sh}] \quad \forall o \in \text{objects}(P)$

- In the definition of $OAPP$, σ_{sh} is changed to σ_τ
It is updated form
$\langle\langle \tau, x \coloneqq o.m; s, \sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau\rangle, \mathcal{T} \cdot \sigma_{sh} \cdot \ell_{sh}\rangle \xrightarrow{\langle \tau, o.m\rangle}_o \langle\langle \tau, s, \sigma_\tau[\text{o} \mapsto ([\![o]\!]\sigma_{sh}).m, x \mapsto rv(([\![o]\!]\sigma_{sh}).m)], \overleftarrow{\sigma_\tau}, \ell_\tau :: (\text{"}o.m\text{"})\rangle, \mathcal{T} \cdot \sigma_{sh} \cdot \ell_{sh}\rangle$
to
$\langle\langle \tau, x \coloneqq o.m; s, \sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau\rangle, \mathcal{T} \cdot \sigma_{sh} \cdot \ell_{sh}\rangle \xrightarrow{\langle \tau, o.m\rangle}_o \langle\langle \tau, s, \sigma_\tau[\text{o} \mapsto ([\![o]\!]\sigma_\tau).m, x \mapsto rv(([\![o]\!]\sigma_\tau).m)], \overleftarrow{\sigma_\tau}, \ell_\tau :: (\text{"}o.m\text{"})\rangle, \mathcal{T} \cdot \sigma_{sh} \cdot \ell_{sh}\rangle$

- In the definition of $OABT$ rule, $\overleftarrow{\sigma_\tau}$[stmt] is changed to $[\![\text{stmt}]\!]\overleftarrow{\sigma_\tau}$ and $\overleftarrow{\sigma_\tau}$ is changed to $\overleftarrow{\sigma_\tau}/\text{stmt}$.
It is updated form
$\langle\langle \tau, s, \sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau\rangle, \mathcal{T} \cdot \sigma_{sh} \cdot \ell_{sh}\rangle \xrightarrow{\langle \tau, \text{abt}\rangle}_o \langle\langle \bot, \overleftarrow{\sigma_\tau}[\text{stmt}], \overleftarrow{\sigma_\tau}, \overleftarrow{\sigma_\tau}, []\rangle, \mathcal{T} \cdot \sigma_{sh} \cdot \ell_{sh}\rangle$
to
$\langle\langle \tau, s, \sigma_\tau, \overleftarrow{\sigma_\tau}, \ell_\tau\rangle, \mathcal{T} \cdot \sigma_{sh} \cdot \ell_{sh}\rangle \xrightarrow{\langle \tau, \text{abt}\rangle}_o \langle\langle \bot, [\![\text{stmt}]\!]\overleftarrow{\sigma_\tau}, \overleftarrow{\sigma_\tau}/\text{stmt}, \overleftarrow{\sigma_\tau}, []\rangle, \mathcal{T} \cdot \sigma_{sh} \cdot \ell_{sh}\rangle$

12. Memory Transactions Implementations

12.1. DSTM2

Memory
  Store of locations: $\mu: l \rightarrow \langle \tau_w, R, v_p, v_s \rangle$
    τ_w: The last writing transaction of location l
    R: The transactions that have read l
    v_p, v_s: Primary and shadow values of l
Transactions
  Each transaction descriptor has
    $state \in \{running, aborted, committed\}$

```
def start {
  thisTrans = new TransDesc
  // thisTrans is a thread local variable
}

def write(l, v) {
  if (μ(l).τ_w ≔ thisTrans)
    μ(l).v_s ≔ v
  else if (μ(l).τ_w.isCommitted)
    μ(l).τ_w ≔ thisTrans
    foreach (τ in μ(l).R) τ.setAborted
    μ(l).R ≔ ∅
    μ(l).v_p ≔ μ(l).v_s
    μ(l).v_s ≔ v
  else if (μ(l).τ_w.isAborted)
    μ(l).τ_w ≔ thisTrans
    foreach (τ in μ(l).R) τ.setAborted
    μ(l).R ≔ ∅
    μ(l).v_s ≔ v
  else if (μ(l).τ_w.isRunning)
    if (not (μ(l).τ_w.setAborted))
      write(l, v)
    else
      μ(l).τ_w ≔ thisTrans
      foreach (τ in μ(l).R) τ.setAborted
      μ(l).R ≔ ∅
      μ(l).v_s = v
}

def read(l) {
  if (μ(l).τ_w ≔ thisTrans)
    return μ(l).v_s
  else if (μ(l).τ_w.isCommitted)
    μ(l).R ≔ μ(l).R ∪ {thisTrans}
    return μ(l).v_s
  else if (μ(l).τ_w.isAborted)
    μ(l).R ≔ μ(l).R ∪ {thisTrans}
    return μ(l).v_p
  else if (μ(l).τ_w.isRunning)
    μ(l).τ_w.setAborted
    return read(l)
}

def commit {
  thisTrans.setCommitted
}
```

12.2. TL2

Memory
  $\mu: l \rightarrow \langle v, L \rangle$: Store of locations
    v: The value of the location l
    L is a pairs of $\langle lock, ver \rangle$
      $lock$ has two values 0 and 1.
      ver is the writing version of the value
Transactions
  Each transaction descriptor has:
    $rver$: Read version
    $rset$: Read set
    $wset$: Write set
  V: Global version clock (strong counter)

```
def start {
  thisTrans.rver ≔ V.read()
}

def write(l, v) {
  thisTrans.wset ≔ thisTrans.wset ∪ {l ↦ v}
}

def read(l) {
  if (l ∈ thisTrans.wset)
    return thisTrans.wset(l)

  (lock_1, ver_1) ≔ μ(l).L
  val ≔ μ(l).v
  (lock_2, ver_2) ≔ μ(l).L
  if (not(lock_1 = lock_2 = 0 and ver_2 < thisTrans.rver))
    abort

  thisTrans.rset ≔ thisTrans.rset ∪ {l}
  return val
}

def commit {
  foreach (l ∈ dom(thisTrans.wset))
    if (CAS(μ(l).L.lock, 0,1)
      locked ≔ locked ∪ {l}
    else
      foreach (l ∈ locked) μ(l).L.lock ≔ 0
      abort

  wver = V.inc()
  if (wver ≠ trans.rver + 1)
    foreach (l ∈ trans.rset)
      (lock, ver) ≔ μ(l).L
      if (l ∉ thisTrans.wset)
        if (not(lock = 0))
          foreach (l ∈ locked) μ(l).L.lock ≔ 0
          abort
        if (not(ver < trans.rver))
          foreach (l ∈ locked) μ(l).L.lock ≔ 0
          abort

  foreach ((l, v) ∈ (thisTrans.wset))
    μ(l).v ≔ v
    μ(l).L ≔ (0, wver)
}
```

13. Transactors Implementation

13.1. DSTM2

DSTM2 allows one writer at a time for each transactional object and therefore, each transactional object maintains two copies of its data. A reference to the descriptor of the last writing transaction is saved in the object. The current state of a transactional object is determined according to the state of the last writing transaction. With visible reads [13], a list of descriptors of the reader transactions is maintained in the transactional object and every read-write and write-write conflict is resolved early when the second operation is requested. A transaction is committed by atomically changing the state of its descriptor to committed which effectively updates all the objects that it has written.

We have extended DSTM2 in a similar fashion that we extended TL2; many of the implementation details are highly similar. We will now explain only the key difference between the two extensions. The key difference lies in the implementation of commit procedure i.e. cluster search and collective commit.

Cluster Search: The same cluster search algorithm that was explained for TL2 can be employed for DSTM2; but as there is no overhead of ordering in the collective commit procedure of DSTM2, a simple depth first traversal can replace the Tarjan algorithm. Getting the set of adjacent nodes of each current node is where the cluster search hooks to the depth first search algorithm. Before returning the set of adjacent transactions, each adjacent transaction is treated according to its state similar to the cluster search explained in the previous section.

Collective Commit: As the updates should be done atomically, the state lock of descriptor of each transaction is acquired. To prevent deadlock, the locks are acquired in the order of the unique numbers of the transaction descriptors. After the locks are acquired, the state of each descriptor is checked to be still terminated. This check is done to make sure that none of them was aborted by other transactions before all the locks were acquired. If any of them is found to be aborted, the locks are released and the current transaction starts abortion. With visible reads and early conflict detection, one of any two conflicting transactions is aborted before termination. As all the transactions of the cluster are terminated, they have not had any conflict with each other or other transactions. Therefore, the two moverness conditions are satisfied. The collective commitment can be performed. State of the descriptor of each transaction is set to committed and then the locks are released.

14. Transactors Implementation Pseudo Codes

14.1. Sending and Receiving Messages

The pseudo code of the send and receive methods are as follows:
Send:

```
def send(msg: T) {
  val senderTransDesc =
    thread local variable for transaction descriptor
  val cell = new Cell(msg, senderTransDesc)
  if (senderTransDesc != null) { //inside atomic
    cell.setTentative
    senderTransDesc.addNotifiable(notifiable)
  }

  if (isReceiverSuspended) {
    cellForSuspendedReceiver = cell
    desuspendReceiver
  } else
    mailbox.enqueue(cell)
}
```

Receive:

```
def receive(): T = {
  val currentTransDesc =
    thread local variable for transaction descriptor
  if (currentTransDesc == null) //outside of atomic
    a stable cell is required
  else //inside atomic
    a non-annihilated cell is required

  iterate the mailbox to find a required cell
  while (a required cell is not found) {
    suspend
    cell = cellForSuspendedReceiver
    if (the cell is not a required cell)
      mailbox.enqueue(cell)
  }

  val msg = cell.message

  if (currentTransDesc == null) //outside of atomic
    return msg

  val senderTransDesc = cell.senderTransDesc

  if (!cell.isStable) {
    currentTransDesc.addDependency(senderTransDesc)
    senderTransDesc.addNotifiable(currentTransDesc)
  }

  currentTrans.backupCell(cell)

  msg
}
```

14.2. Abortion

```
def abortion {
  val currentTransDesc =
    thread local variable for transaction descriptor

  for each cell in the backup cells
    if (!cell.isInvalid)
      mailbox.enqueue(cell)

  currentTransDesc.notifyNotifiersOfAbortion
}
```

14.3. Termination

```
def termination {
  thisTransDesc.setTerminated
  var state = TERMINATED;
  do {
    try {
      commitment()
    } catch {
      case we: WaitException ={
        thisTransDesc.waitForEvent
        thisTransDesc.getEvent match {
          case ABORT =
            state = ABORTED
          case DEP_RESOLVE =>
            ; // Retry collectiveCommit
          case COMMIT =>
            state = COMMITTED
        }
      }
      case we: AbortException ={
        state = ABORTED
      }
    }
  } while (state == TERMINATED)
  if (state == ABORTED)
    abort()
}
```

14.4. Commitment

```
def commitment {
  val cluster = clusterSearch(thisTransDesc)
  collectiveCommit(cluster)
}
```

14.4.1. DSTM2

14.4.1.1. Cluster Search

```
def clusterSearch(node: Node) {
   return depthFirstSearch(node)

   def depthFirstSearch(node: Node): Set[Node] = {
      // ...
      // Uses the getNeighbors method below
      // Return the set of visited nodes
   }
}

def getNeighbors = {
  val deps = transDesc.getDependencies
  val neighbors = Set[Node]()
  for (depTransDesc <- deps) {
    if (transDesc.isActive)
      throw new WaitException
    if (transDesc.isAborted)
      throw new AbortException
    if (!depTransDesc.isCommitted)
      neighbors += depTransDesc
  }
  neighbors
}
```

14.4.1.2. Collective Commit

```
def collectiveCommit(cluster: Set[Node]) {
  sort transaction of the cluster according to their id
  for each transDesc of the cluster in the order
    transDesc.acquireStatusLock
  for each transDesc of the cluster
    if (transDesc.status != running) {
      for each transDesc' of the cluster
        transDesc'.releaseStatusLock
      throw new AbortException
    }
  for each transDesc of the cluster {
    transDesc.status = Committed
    transDesc.notifyNotifiablesOfCommitment
  }
  for each transDesc of the cluster
    transDesc.releaseStatusLock
}
```

14.4.2. TL2

14.4.2.1. Cluster Search

```
def clusterSearch(node: Node) {
```

```
   val sccs = Set[Set[Node]]
   tarjan(node)
   if (sccs.size == 1)
      throw new AbortException
   val scc = the only element of sccs
   return scc

   def tarjan(node: Node): Set[Set[Node]] = {
      node.index = index
      node.lowlink = index
      index += 1
      stack.push(node)
      for (n <- node.getNeighbors) {
         if (n.index == initialValue) {
            tarjan(n)
            node.lowlink = min(node.lowlink, n.lowlink)
         } else
            node.lowlink = min(node.lowlink, n.index)
         if (node.lowlink == node.index) {
            var n: Node = null
            do {
               n = stack.pop
               scc += n
            } while (n != node)
            sccs += scc
         }
      }
   }
}

def getNeighbors = {
  val deps = transDesc.getDependencies
  val neighbors = Set[Node]()
  for (depTransDesc <- deps) {
    if (transDesc.isActive)
      throw new WaitException
    if (transDesc.isAborted)
      throw new AbortException
    if (!depTransDesc.isCommitted)
      neighbors += depTransDesc
  }
  neighbors
}
```

14.4.2.2. Collective Commit

$def\ commit(cluster)\{$

$orderGraph = new\ Graph$
$orderGraph.V = transactions\ of\ cluster$
$foreach\ (trans_1 \in cluster)$
  $foreach\ (trans_2 \in cluster)$
    $if\ (trans_1.rset\ \cap\ trans_2.wset)$
      $orderGraph.E \coloneqq orderGraph.E \cup \{trans_1 \to trans_2\}$
$if\ (orderGraph\ has\ a\ cycle)$
  $abort$

$wset \coloneqq \cup_{trans \in cluster}\ trans.wset$
$foreach\ \big(l \in dom(wset)\big)$
  $if\ (CAS(\mu(l).L.lock, 0, 1)$
    $locked \coloneqq locked \cup \{l\}$
  $else$
    $foreach\ (l \in locked)\ \mu(l).L.lock \coloneqq 0$
    $abort$

$wver = V.inc()$
$foreach\ (trans \in cluster)$
  $if\ (wver \neq trans.rver + 1)$
    $foreach\ (l \in trans.rset)$
      $(lock, ver) \coloneqq \mu(l).L$
      $if\ (l \notin thisTrans.wset)$
        $if\ \big(not(lock = 0)\big)$
          $foreach\ (l \in locked)\ \mu(l).L.lock \coloneqq 0$
          $abort$
      $if\ \big(not(ver < trans.rver)\big)$
        $foreach\ (l \in locked)\ \mu(l).L.lock \coloneqq 0$
        $abort$

$foreach\ (trans \in cluster)$
  $foreach\ ((l, v) \in wset)$
    $\mu(l).v \coloneqq v$
    $\mu(l).L \coloneqq (0, wver)$
$foreach\ (trans \in cluster)$
  $trans.setStateCommitted$
  $trans.notifyNotifiablesOfCommitment$
}
```
```

15. Implemented Cases

15.1. Barrier

Consider the following example: Barrier, the simplest thread coordination abstraction

15.1.1. retry

The following is the implementation of barrier with memory transactions (with Haskell retry mechanism) that we adopted from [28].

```
class Barrier(partiesCount: Int) {
   val count = new TInt(0)
   def await() {
      atomic {
         count.value = count.value + 1
      }
      atomic {
         if (!(count.value == partiesCount))
            retry
      }
   }
}
class Party(barrier: Barrier) extends Thread {
   override def run {
      // Do before await
      barrier.await
      // Do after await
   }
}
```

The field `count` counts the number of parties that have called the `await` method. There are two atomic blocks in the `await` method. The first one increments the value of `count`. The second one waits for equality of `count` to the number of expected parties, `partiesCount` that is initialized in the constructor. If the condition is not true, `retry` aborts the transaction and suspends the thread until `count`, the only object that is read in the previous execution of the transaction, is updated. When the value of `count` is incremented to `partiesCount`, all of the suspended parties retry the atomic block and as the condition is satisfied, pass the atomic block. Effectively, the parties continue together after calling the `await` method.

The implemented `Barrier` works properly if the `await` method is not called inside a transaction. But consider the following class that calls `await` inside an atomic block.

```
class TParty(barrier: Barrier) extends Thread {
   override def run {
      atomic {
         // code before await
         barrier.await
         // code after await
      }
   }
}
```

According to closed nesting semantics, the nesting can be syntactically written as follows:

```
atomic {
   // code before await
   count.value = count.value + 1
   if (!(count.value == partiesCount))
      retry
   // code after await
}
```

If the parties call the `await` method of `Barrier` inside nested atomic blocks, they can not progress. Intuitively, this is because the semantics of TM [10] requires an equivalent sequential order of transactions while in this case, each of the parties needs to observe updates of other parties to `count` before it can progress and commit.

15.1.2. TIC

A solution to this problem called TIC is offered by Smaragdakis et al. [28]. TIC commits the transaction and starts a new one before the `wait` statement. By their terminology, the transaction is punctuated before the `wait` statement. Committing before the wait statement exposes updates to other transactions and thus provides means of communication. But punctuation of an atomic block breaks its isolation. Furthermore, if an atomic block A_1 is inside method M_1 and M_1 is called by another method M_2 inside a nesting atomic block A_2, punctuating A_1 breaks isolation of not only A_1 but also A_2. To make this break explicit to the programmer, TIC designed a type system that tracks methods that contain punctuated atomic blocks. If the programmer wants to call such methods in an atomic block, the type system forces him to call it inside `expose()` and to write code to compensate breaking of isolation in an `establish{}` block. The barrier case is implemented as follows in TIC:

```
class TICBarrier(partiesCount: Int) {
   val count = new TInt(0)
   def await() {
      atomic {
         count.value = count.value + 1
```

```
         wait(count.value == partiesCount)
      }
   }
}
class TParty(barrier: TICBarrier) extends Thread {
   override def run {
     atomic {
         // Do some job
         expose (barrier.await)
         establish { //... }
         // Do some other job
     }
   }
}
```

Even if any compensation is possible, re-establishing local invariants is a burden on the programmer. More importantly, TIC breaks isolation to provide communication while isolation is the main promise of TM. Actually, TIC regards communication the same as I/O. Side effects caused by I/O operations are out of control of TM runtime system; thus they cannot be rolled back and retried. In contrast to I/O, proper mechanisms can be designed to perform communications tentatively and to discard and retry them on aborts. Our proposal provides the programmer with the facility to send and receive messages inside transactions.

15.1.3. Transactors

The transactions of parties need to communicate with each other before they are finished. We observe that to preserve isolation of transactions, a means of communication other than shared variables is needed so that the transactions can communicate tentatively before they are committed.

A class called `BarrierActor` that extends the base class `Transactor` is defined inside `Barrier` class. In the `act` method of `BarrierActor`, inside an atomic block, `BarrierActor` waits to receive `JoinNotificationRequest` message from the parties and adds the sender transactor of each received message to `parties` set. After receiving the request form `partiesCount` parties, it sends a `JoinNotification` message to all the parties in `parties` set. On construction of a `Barrier`, a new object called `barrierActor` of type `BarrierActor` is created and started. When a party calls the `await` method on a `Barrier` object, it sends a `JoinNotificationRequest` message to the `barrierActor` and waits to receive a `JoinNotification` message.

To see composability of the abstraction and the interactions of transactions, we compose the `await` method inside an atomic block.

```
class Barrier(partiesCount: Int) {
   class BarrierActor extends Transactor {
      override def act {
         atomic {
            val parties = Set[Transactor]()
            for(i <- 0 until partiesCount)
               receive {
                  case r: JoinNotificationRequest =>
                     parties += r.sender
               }
            for(party <- parties)
               party ! new JoinNotification
         }
      }
   }
   val barrierActor = new BarrierActor
   barrierActor.start
   def await() {
      barrierActor ! new JoinNotificationRequest
      self.receive { case JoinNotification =}
   }
}
class TParty(barrier: Barrier) extends Transactor {
   override def act {
      atomic {
         // Do before await
         barrier.await
         // Do after await
      }
   }
}
```

15.1.4. TE for ML

15.1.4.1. Implementation 1

```
   let client bc =
      let cc = newChan() in
         (thenEvt
             (sendEvt bc cc)
             (fun _ -recvEvt cc)
         )
   ;;
```

```
let leader bc =
    (thenEvt (recvEvt bc)
       (fun cc1 -(thenEvt (recvEvt bc)
          (fun cc2 -(thenEvt (sendEvt cc1 ())
             (fun _ -(sendEvt cc2 ()))
          ))
       ))
    )
;;

let barrier bc =
   sync (chooseEvt
      (client bc)
      (leader bc)
   )
;;

let party bc =
   (barrier bc)
;;

let main () =
   let bc = newChan() in
   let t1 = Thread.create (fun x -(party bc)) () in
   let t2 = Thread.create (fun x -(party bc)) () in
   let t3 = Thread.create (fun x -(party bc)) () in
      Thread.join t1;
      Thread.join t2;
      Thread.join t3
;;
```

15.1.4.2. Implementation 2

```
let client bc =
   let cc = newChan() in
      sync (thenEvt
         (sendEvt bc cc)
         (fun x -recvEvt cc)
      )
;;

let leader bc =
   sync (
      (thenEvt (recvEvt bc)
         (fun cc1 -(thenEvt (recvEvt bc)
        (fun cc2 -(thenEvt (recvEvt bc)
        (fun cc3 -(thenEvt (sendEvt cc1 ())
         (fun _ -(thenEvt (sendEvt cc2 ())
         (fun _ -(sendEvt cc3 ())))))))))))
   )
;;


let main () =
   let bc = newChan() in
   let t1 = Thread.create (fun x -(leader bc)) () in
   let t2 = Thread.create (fun x -(client bc)) () in
   let t3 = Thread.create (fun x -(client bc)) () in
   let t4 = Thread.create (fun x -(client bc)) () in
      Thread.join t1;
      Thread.join t2;
      Thread.join t3;
      Thread.join t4
;;
```

15.2. Synchronous Queue

```
class SyncQueue[T] {

  val sCh = new Transactor[T]
  val rCh = new Transactor[Ack]

  def send(message: T) {
    atomic {
      sCh ! message
      rCh.receive
    }
  }

  def receive(): T = {
```

```
    atomic {
      val message = sCh.receive
      rCh ! new Ack
      message
    }
  }
}
```

15.3. Rendezvous

```
class Rendezvous[T]() {

  class PartyInfo(var element: T, var party: Transactor[Pair[T, T]])

  class RendezvousActor extends Transactor[PartyInfo] {

    override def act {
      val partiesInfo = new Array[PartyInfo](3)
      atomic {
        for (i <- 0 until 3)
          partiesInfo(i) = receive
        for (i <- 0 until 3) {
          val party = partiesInfo(i).party
          val index1 = (i+1)%3
          val index2 = (i+2)%3
          party ! new Pair(partiesInfo(index1).element, partiesInfo(index2).element)
        }
      }
    }
  }
  val rendezvousActor = new RendezvousActor
  rendezvousActor.start


  def swap(message: T): Pair[T, T] = {
    atomic {
      val thisTransactor =    self.asInstanceOf[Transactor[Pair[T, T]]]
      rendezvousActor ! new PartyInfo(message, thisTransactor)
      thisTransactor.receive
    }
  }
}
```

15.4. Server

```
abstract class Server[T] extends Transactor[T] {

  val executor = Executors.newCachedThreadPool()

  override def act {
    while(true) {
      val cell = serverReceive
      val fun = (_:Unit) ={
        setForEndReceiver(cell)
      }
      executor.execute(new Runnable() {
        def run = {
          service(fun)
        }
      })
    }
  }

  def service(getRequest: Unit => T)
}

class MyIdServer extends Server[IdRequest] {
  val id = new TInt(0)

  override def service(getRequest: Unit => IdRequest) {
    val newId = atomic {
      id.value = id.value + 1
      id.value
    }

    atomic {
      val request = getRequest()
      val sender = request.sender
      sender ! new IdRespond(newId)
```

```
        }
    }
}
```