Write-observation and Read-preservation TM Correctness Invariants (Appendix)

Mohsen Lesani Jens Palsberg
Computer Science Department
University of California, Los Angeles
{lesani, palsberg}@ucla.edu

Contents

1 Proof of Marking Theorem

For the sake of brevity, we use the shorthand notation
$\exists l = o.n_T(v_1){:}v_2 \in X$
for
$\exists l \in X : obj_X(l) = o \ \wedge \ name_X(l) = n \ \wedge \ thread_X(l) = T \ \wedge \ arg1_X(l) = v_1 \ \wedge \ retv_X(l) = v_2$
and similarly for universal quantification.

We also use W, R to denote labels.

Lemma 1. *For all $S \in TSequential$, $T \in S$, $S' = Visible(S,T)$, and $T', T'' \in S'$, we have $T' \precsim_{S'} T'' \iff T' \precsim_S T''$.*

Proof.

$$\begin{aligned} & T' \precsim_{S'} T'' \\ \iff & S'|T' \lhd_{S'} S'|T'' \ \vee \ T' = T'' \\ \iff & S|T' \lhd_{S'} S|T'' \ \vee \ T' = T'' \\ \iff & S|T' \lhd_{S} S|T'' \ \vee \ T' = T'' \\ \iff & T' \precsim_S T'' \end{aligned}$$

In these four steps we apply:
1) the definition of $\precsim_{S'}$,
2) that the definition of $Visible(S,T)$ implies both $S'|T' = S|T'$ and $S'|T'' = S|T''$,
3) $S' \Subset S$, and
4) the definition of $\precsim_S$. □

Lemma 2. *For all $S \in TSequential$, $T \in S$, $i \in I$, $v, v' \in V$, $R = read_T(i){:}v \in GlobalReads(S)$, $S' = Visible(S,T)$, $T' \in S'$, and $W' = write_{T'}(i,v') \in GlobalWrites(S)$, we have*

$$NoWriteBetween_{(S'|i)}(W', R) \iff NoWriterBetween_{S,i}(T', \preceq\!\!\!\lessdot_S, T)$$

Proof.

$$
\begin{aligned}
& NoWriteBetween_{(S'|i)}(W', R) \\
\iff\ & \forall W'' \in Writes(S'|i) \colon W'' \preceq_{(S'|i)} W' \vee R \preceq_{(S'|i)} W'' \\
\iff\ & \forall T'' \in S'|i \colon \forall i' \in I : \forall v'' \in V : \forall W'' = write_{T''}(i', v'') \in S'|i \colon W'' \preceq_{(S'|i)} W' \vee R \preceq_{(S'|i)} W'' \\
\iff\ & \forall T'' \in S'|i \colon \forall v'' \in V : \forall W'' = write_{T''}(i, v'') \in S'|i \colon W'' \preceq_{(S'|i)} W' \vee R \preceq_{(S'|i)} W'' \\
\iff\ & \forall T'' \in S' \colon \forall v'' \in V : \forall W'' = write_{T''}(i, v'') \in S' \colon W'' \preceq_{S'} W' \vee R \preceq_{S'} W'' \\
\iff\ & \forall T'' \in S' \colon \forall v'' \in V : \forall W'' = write_{T''}(i, v'') \in S' \colon T'' \preceq\!\!\!\lessdot_{S'} T' \vee T \preceq\!\!\!\lessdot_{S'} T'' \\
\iff\ & \forall T'' \in S' \colon \forall v'' \in V : \forall W'' = write_{T''}(i, v'') \in S' \colon T'' \preceq\!\!\!\lessdot_{S} T' \vee T \preceq\!\!\!\lessdot_{S} T'' \\
\iff\ & \forall T'' \in S' \colon \forall v'' \in V : \forall W'' = write_{T''}(i, v'') \in S' \colon T'' \lessdot_{S} T \Rightarrow T'' \preceq\!\!\!\lessdot_{S} T' \\
\iff\ & \forall T'' \in S \colon \forall v'' \in V : \forall W'' = write_{T''}(i, v'') \in S \colon \\
& \quad \big[[(T'' = T) \vee (T'' \lessdot_S T \wedge T'' \in Committed(S))] \wedge [T'' \lessdot_S T]\big] \Rightarrow T'' \preceq\!\!\!\lessdot_S T' \\
\iff\ & \forall T'' \in S \colon \forall v'' \in V : \forall W'' = write_{T''}(i, v'') \in S \colon \\
& \quad (T'' \in Committed(S) \wedge\ T'' \lessdot_S T) \Rightarrow T'' \preceq\!\!\!\lessdot_S T' \\
\iff\ & \forall T'' \in Writers_S(i) \colon T'' \lessdot_S T \Rightarrow T'' \preceq\!\!\!\lessdot_S T' \\
\iff\ & \forall T'' \in Writers_S(i) \colon T'' \preceq\!\!\!\lessdot_S T' \vee T \preceq\!\!\!\lessdot_S T'' \\
\iff\ & NoWriterBetween_{S,i}(T', \preceq\!\!\!\lessdot_S, T)
\end{aligned}
$$

In these twelve steps, we apply:
1) the definition of $NoWriteBetween$,
2) the definition of $Writes$,
3) the definition of projection $S'|i$,
4) R, W' and W'' access location i,
5) $S' \in TSequential$ and $R \in GlobalReads(S')$ and $W' \in GlobalWrites(S')$ (that are concluded from $S \in TSequential$, $R \in GlobalReads(S)$, $W' \in GlobalWrites(S)$ and $S' = Visible(S,T)$.),
6) Lemma 1,
7) Boolean logic and that $\preceq\!\!\!\lessdot_S$ is total,
8) the definition of $Visible$,
9) logical simplification,
10) the definition of $Writers$,
11) Boolean logic and that $\preceq\!\!\!\lessdot_S$ is total, and
12) the definition of $NoWriterBetween$. □

Lemma 3. *$TSequential \subset Sequential$*

Proof. Straightforward from definitions of $TSequential$, $THistory$ and $Sequential$. $\square$

Lemma 4. $\forall i \in I\colon \ \forall v, v' \in V\colon \ \forall T, T' \in Trans\colon$ *if* $R = read_T(i){:}v$, $W = write_{T'}(i, v)$, $W' = write_T(i, v')$, $S \in TSequential$, $W \prec_S R$, $NoWriteBetween_S(W, R)$ *and* $W' \prec_S R$, *then* $T = T'$.

Proof. Suppose (1) $S \in TSequential$, (2) $W \prec_S R$, (3) $NoWriteBetween_S(W, R)$ and (4) $W' \prec_S R$. From [1] and Lemma 3, we have (5) $S \in Sequential$. From [4] and [5], we have (6) $\neg(R \prec_S W')$. From [3] we have (7) $W' \preceq_S W \vee R \prec_S W'$. From [6] and [7], we have (8) $W' \preceq_S W$. From [2] and [8], we have (9) $W' \preceq_S W \preceq_S R$. From [9], [1], and that W' and R are by T and W is by T', we have $T = T'$. $\square$

Lemma 5. *Suppose $S \in TSequential$. We have:*

$$\begin{aligned}
& \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = read_T(i){:}v \in LocalReads(S)\colon \\
& \quad \exists T' \in Visible(S,T)\colon \exists W = write_{T'}(i,v) \in Visible(S,T)\colon \\
& \quad W \prec_{(Visible(S,T)\ |\ i)} R \ \wedge\ NoWriteBetween_{(Visible(S,T)\ |\ i)}(W,R) \\
\iff\ & S \in LocalTSeqSpec
\end{aligned}$$

Proof. Suppose $S \in TSequential$. Thus, from Lemma 3, we have $S \in Sequential$. Let $S' = Visible(S,T)$. From $S \in TSequential$ and Lemma 1, we have $S' \in TSequential$. Thus, from Lemma 3, we have $S' \in Sequential$. From the definition of $Visible$, we have $S'|T = S|T$.

$$\begin{aligned}
& \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = read_T(i){:}v \in LocalReads(S)\colon \\
& \quad \exists T' \in S'\colon \exists W = write_{T'}(i,v) \in S'\colon \\
& \quad\quad W \prec_{(S'\ |\ i)} R \ \wedge\ NoWriteBetween_{(S'\ |\ i)}(W,R) \\
\iff\ & \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = read_T(i){:}v \in LocalReads(S)\colon \\
& \quad \exists v' \in V\colon \exists W' = write_T(i,v') \in S\colon W' \prec_S R\ \wedge \\
& \quad \exists T' \in S'\colon \exists W = write_{T'}(i,v) \in S'\colon \\
& \quad\quad W \prec_{(S'\ |\ i)} R \ \wedge\ NoWriteBetween_{(S'\ |\ i)}(W,R) \\
\iff\ & \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = read_T(i){:}v \in LocalReads(S)\colon \\
& \quad \exists v' \in V\colon \exists W' = write_T(i,v') \in S'\colon W' \prec_S R\ \wedge \\
& \quad \exists T' \in S'\colon \exists W = write_{T'}(i,v) \in S'\colon \\
& \quad\quad W \prec_{(S'\ |\ i)} R \ \wedge\ NoWriteBetween_{(S'\ |\ i)}(W,R) \\
\iff\ & \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = read_T(i){:}v \in LocalReads(S)\colon \\
& \quad \exists v' \in V\colon \exists W' = write_T(i,v') \in S'\colon W' \prec_{S'} R\ \wedge \\
& \quad \exists T' \in S'\colon \exists W = write_{T'}(i,v) \in S'\colon \\
& \quad\quad W \prec_{(S'\ |\ i)} R \ \wedge\ NoWriteBetween_{(S'\ |\ i)}(W,R) \\
\iff\ & \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = read_T(i){:}v \in LocalReads(S)\colon \\
& \quad \exists v' \in V\colon \exists W' = write_T(i,v') \in S'\colon W' \prec_{(S'\ |\ i)} R\ \wedge \\
& \quad \exists T' \in S'\colon \exists W = write_{T'}(i,v) \in S'\colon \\
& \quad\quad W \prec_{(S'\ |\ i)} R \ \wedge\ NoWriteBetween_{(S'\ |\ i)}(W,R) \\
\iff\ & \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = read_T(i){:}v \in LocalReads(S)\colon \\
& \quad \exists v' \in V\colon \exists W' = write_T(i,v') \in S'\colon W' \prec_{(S'\ |\ i)} R\ \wedge \\
& \quad \exists W = write_T(i,v) \in S'\colon \\
& \quad\quad W \prec_{(S'\ |\ i)} R \ \wedge\ NoWriteBetween_{(S'\ |\ i)}(W,R) \\
\iff\ & \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = read_T(i){:}v \in LocalReads(S)\colon \\
& \quad \exists W = write_T(i,v) \in S'\colon \\
& \quad\quad W \prec_{(S'\ |\ i)} R \ \wedge\ NoWriteBetween_{(S'\ |\ i)}(W,R) \\
\iff\ & \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = read_T(i){:}v \in LocalReads(S)\colon \\
& \quad \exists W = write_T(i,v) \in S\colon \\
& \quad\quad W \prec_{(S'\ |\ i)} R \ \wedge\ NoWriteBetween_{(S'\ |\ i)}(W,R)
\end{aligned}$$

$$
\begin{aligned}
\iff\ & \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = read_T(i){:}v \in LocalReads(S)\colon \\
& \quad \exists W = write_T(i,v) \in S\colon \\
& \quad\quad W \prec_{S'} R \,\wedge\, NoWriteBetween_{(S' \mid i)}(W,R) \\
\iff\ & \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = read_T(i){:}v \in LocalReads(S)\colon \\
& \quad \exists W = write_T(i,v) \in S\colon \\
& \quad\quad W \prec_{S} R \,\wedge\, NoWriteBetween_{(S' \mid i)}(W,R) \\
\iff\ & \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = read_T(i){:}v \in LocalReads(S)\colon \\
& \quad \exists W = write_T(i,v) \in S\colon \\
& \quad\quad W \prec_{S} R \,\wedge\, \forall W' \in Writes(S' \mid i)\colon W' \preceq_{(S' \mid i)} W \vee R \prec_{(S' \mid i)} W' \\
\iff\ & \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = read_T(i){:}v \in LocalReads(S)\colon \\
& \quad \exists W = write_T(i,v) \in S\colon \\
& \quad\quad W \prec_{S} R \,\wedge\, \neg\exists W' \in Writes(S' \mid i)\colon \neg(W' \preceq_{(S' \mid i)} W) \,\wedge\, \neg(R \prec_{(S' \mid i)} W') \\
\iff\ & \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = read_T(i){:}v \in LocalReads(S)\colon \\
& \quad \exists W = write_T(i,v) \in S\colon \\
& \quad\quad W \prec_{S} R \,\wedge\, \neg\exists W' \in Writes(S' \mid i)\colon W \prec_{(S' \mid i)} W' \prec_{(S' \mid i)} R \\
\iff\ & \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = read_T(i){:}v \in LocalReads(S)\colon \\
& \quad \exists W = write_T(i,v) \in S\colon \\
& \quad\quad W \prec_{S} R \,\wedge\, \neg\exists v' \in V\colon \exists W' = write_T(i,v')\colon W \prec_{(S' \mid i)} W' \prec_{(S' \mid i)} R \\
\iff\ & \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = read_T(i){:}v \in LocalReads(S)\colon \\
& \quad \exists W = write_T(i,v) \in S\colon \\
& \quad\quad W \prec_{S} R \,\wedge\, \neg\exists v' \in V\colon \exists W' = write_T(i,v')\colon W \prec_{(S \mid i)} W' \prec_{(S \mid i)} R \\
\iff\ & \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = read_T(i){:}v \in LocalReads(S)\colon \\
& \quad \exists W = write_T(i,v) \in S\colon \\
& \quad\quad W \prec_{S} R \,\wedge\, \neg\exists W' \in Writes(S \mid i)\colon W \prec_{(S \mid i)} W' \prec_{(S \mid i)} R \\
\iff\ & \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = read_T(i){:}v \in LocalReads(S)\colon \\
& \quad \exists W = write_T(i,v) \in S\colon \\
& \quad\quad W \prec_{S} R \,\wedge\, \forall W' \in Writes(S \mid i)\colon \neg(W \prec_{(S \mid i)} W') \,\vee\, \neg(W' \prec_{(S \mid i)} R) \\
\iff\ & \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = read_T(i){:}v \in LocalReads(S)\colon \\
& \quad \exists W = write_T(i,v) \in S\colon W \prec_{S} R \,\wedge \\
& \quad\quad \forall W' \in Writes(S \mid i)\colon W' \preceq_{(S \mid i)} W \,\vee\, R \prec_{(S \mid i)} W' \\
\iff\ & \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = read_T(i){:}v \in LocalReads(S)\colon \\
& \quad \exists W = write_T(i,v) \in S|T|i\colon W \prec_{S|T|i} R \,\wedge \\
& \quad\quad \forall W' \in Writes(S|T|i)\colon W' \preceq_{(S|T|i)} W \,\vee\, R \prec_{(S|T|i)} W' \\
\iff\ & \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = read_T(i){:}v \in LocalReads(S)\colon \\
& \quad \exists W = write_T(i,v) \in S|T|i\colon \\
& \quad\quad W \prec_{S|T|i} R \,\wedge\, NoWriteBetween_{(S|T|i)}(W,R) \\
\iff\ & S \in LocalTSeqSpec
\end{aligned}
$$

In these twenty steps, we apply: 1) the definition of *LocalReads*,

2) the definition of $Visible$,
3) $S'|T = S|T$ and that both W' and R are by T,
4) that both W' and R are on i,
5) Lemma 4,
6) duplicate conjunction,
7) the definition of $Visible$,
8) that both R and W are on i,
9) $S'|T = S|T$ and that both R and W are by T,
10) the definition of $NoWriteBetween$,
11) first-order logic,
12) $(S' \mid i) \in Sequential$,
13) from $(S' \mid i) \in TSequential$, R and W are by transaction T and W' is between them, we have W' is by T,
14) $S'|T = S|T$,
15) from $(S \mid i) \in TSequential$, R and W are by transaction T and W' is between them, we have W' is by T.
16) first-order logic,
17) $(S \mid i) \in Sequential$,
18) $(S \mid i) \in Sequential$, $thread_H(R) = thread_H(W) = T$ and $arg1_H(R) = arg1_H(W) = i$,
19) the definition of $NoWriteBetween$,
20) the definition of $LocalTSeqSpec$.

□

Lemma 6. *Suppose $S \in TSequential \cap TComplete$. We have:*

$$
\begin{aligned}
& S \in TSeqSpec \\
\iff\ & S \in LocalTSeqSpec\ \wedge \\
& \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = read_T(i){:}v \in GlobalReads(S)\colon \\
& \exists T' \in Committed(S)\colon \exists W = write_{T'}(i,v) \in GlobalWrites(S)\colon \\
& \quad (T' \lessdot_S T)\ \wedge\ NoWriterBetween_{S,i}(T', \preceq_S, T)
\end{aligned}
$$

Proof. Suppose $S \in TSequential \cap TComplete$. From $S \in TSequential$ and Lemma 1, we have $Visible(S,T) \in TSequential$.

$$
\begin{aligned}
& S \in TSeqSpec \\
\iff\ & \forall T \in S\colon \forall i \in I\colon (Visible(S,T) \mid i) \in SeqSpec(i) \\
\iff\ & \forall T \in S\colon \forall i \in I\colon \\
& \quad \forall T'' \in (Visible(S,T) \mid i)\colon \forall v \in V\colon \forall R = read_{T''}(i){:}v \in (Visible(S,T) \mid i)\colon \\
& \quad \exists T' \in (Visible(S,T) \mid i)\colon \exists W = write_{T'}(i,v) \in (Visible(S,T) \mid i)\colon \\
& \quad W \prec_{(Visible(S,T) \mid i)} R\ \wedge\ NoWriteBetween_{(Visible(S,T) \mid i)}(W,R) \\
\iff\ & \forall T \in S\colon \forall i \in I\colon \\
& \quad \forall T'' \in Visible(S,T)\colon \forall v \in V\colon \forall R = read_{T''}(i){:}v \in Visible(S,T)\colon \\
& \quad \exists T' \in Visible(S,T)\colon \exists W = write_{T'}(i,v) \in Visible(S,T)\colon \\
& \quad W \prec_{(Visible(S,T) \mid i)} R\ \wedge\ NoWriteBetween_{(Visible(S,T) \mid i)}(W,R) \\
\iff\ & \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = read_T(i){:}v \in S\colon \\
& \quad \exists T' \in Visible(S,T)\colon \exists W = write_{T'}(i,v) \in Visible(S,T)\colon \\
& \quad W \prec_{(Visible(S,T) \mid i)} R\ \wedge\ NoWriteBetween_{(Visible(S,T) \mid i)}(W,R) \\
\iff\ & \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = read_T(i){:}v \in LocalReads(S)\colon \\
& \quad \exists T' \in Visible(S,T)\colon \exists W = write_{T'}(i,v) \in Visible(S,T)\colon \\
& \quad W \prec_{(Visible(S,T) \mid i)} R\ \wedge\ NoWriteBetween_{(Visible(S,T) \mid i)}(W,R) \\
& \wedge \\
& \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = read_T(i){:}v \in GlobalReads(S)\colon \\
& \quad \exists T' \in Visible(S,T)\colon \exists W = write_{T'}(i,v) \in Visible(S,T)\colon \\
& \quad W \prec_{(Visible(S,T) \mid i)} R\ \wedge\ NoWriteBetween_{(Visible(S,T) \mid i)}(W,R) \\
\iff\ & S \in LocalTSeqSpec\ \wedge \\
& \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = read_T(i){:}v \in GlobalReads(S)\colon \\
& \quad \exists T' \in Visible(S,T)\colon \exists W = write_{T'}(i,v) \in Visible(S,T)\colon \\
& \quad W \prec_{(Visible(S,T) \mid i)} R\ \wedge\ NoWriteBetween_{(Visible(S,T) \mid i)}(W,R)
\end{aligned}
$$

$$\begin{aligned}
\iff\ & S \in \mathit{LocalTSeqSpec}\ \wedge \\
& \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = \mathit{read}_T(i){:}v \in \mathit{GlobalReads}(S)\colon \\
& \qquad \exists T' \in \mathit{Visible}(S,T)\colon \exists W = \mathit{write}_{T'}(i,v) \in \mathit{Visible}(S,T)\colon \\
& \qquad W \prec_{\mathit{Visible}(S,T)} R\ \wedge\ \mathit{NoWriteBetween}_{(\mathit{Visible}(S,T)\ \mid\ i)}(W,R) \\
\iff\ & S \in \mathit{LocalTSeqSpec}\ \wedge \\
& \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = \mathit{read}_T(i){:}v \in \mathit{GlobalReads}(S)\colon \\
& \qquad \exists T' \in \mathit{Visible}(S,T)\colon \exists W = \mathit{write}_{T'}(i,v) \in \mathit{Visible}(S,T)\colon \\
& \qquad T' \lessdot_{\mathit{Visible}(S,T)} T\ \wedge\ \mathit{NoWriteBetween}_{(\mathit{Visible}(S,T)\ \mid\ i)}(W,R) \\
\iff\ & S \in \mathit{LocalTSeqSpec}\ \wedge \\
& \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = \mathit{read}_T(i){:}v \in \mathit{GlobalReads}(S)\colon \\
& \qquad \exists T' \in \mathit{Visible}(S,T)\colon \exists W = \mathit{write}_{T'}(i,v) \in \mathit{Visible}(S,T)\colon \\
& \qquad T' \lessdot_S T\ \wedge\ \mathit{NoWriteBetween}_{(\mathit{Visible}(S,T)\ \mid\ i)}(W,R) \\
\iff\ & S \in \mathit{LocalTSeqSpec}\ \wedge \\
& \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = \mathit{read}_T(i){:}v \in \mathit{GlobalReads}(S)\colon \\
& \qquad \exists T' \in \mathit{Visible}(S,T)\colon \exists W = \mathit{write}_{T'}(i,v) \in \mathit{GlobalWrites}(S)\colon \\
& \qquad T' \lessdot_S T\ \wedge\ \mathit{NoWriteBetween}_{(\mathit{Visible}(S,T)\ \mid\ i)}(W,R) \\
\iff\ & S \in \mathit{LocalTSeqSpec}\ \wedge \\
& \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = \mathit{read}_T(i){:}v \in \mathit{GlobalReads}(S)\colon \\
& \qquad \exists T' \in \mathit{Visible}(S,T)\colon \exists W = \mathit{write}_{T'}(i,v) \in \mathit{GlobalWrites}(S)\colon \\
& \qquad T' \lessdot_S T\ \wedge\ \mathit{NoWriterBetween}_{S,i}(T', \preceq\!\!\lessdot_S, T) \\
\iff\ & S \in \mathit{LocalTSeqSpec}\ \wedge \\
& \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = \mathit{read}_T(i){:}v \in \mathit{GlobalReads}(S)\colon \\
& \qquad \exists T' \in \mathit{Visible}(S,T)\colon \exists W = \mathit{write}_{T'}(i,v) \in \mathit{GlobalWrites}(S)\colon \\
& \qquad (T' \lessdot_S T)\ \wedge\ T' \in \mathit{Committed}(S)\ \wedge\ \mathit{NoWriterBetween}_{S,i}(T', \preceq\!\!\lessdot_S, T) \\
\iff\ & S \in \mathit{LocalTSeqSpec}\ \wedge \\
& \forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = \mathit{read}_T(i){:}v \in \mathit{GlobalReads}(S)\colon \\
& \qquad \exists T' \in \mathit{Committed}(S)\colon \exists W = \mathit{write}_{T'}(i,v) \in \mathit{GlobalWrites}(S)\colon \\
& \qquad (T' \lessdot_S T)\ \wedge\ \mathit{NoWriterBetween}_{S,i}(T', \preceq\!\!\lessdot_S, T)
\end{aligned}$$

In these thirteen steps, we apply:
1) the definition of $TSeqSpec$ and $S \in TSequential \cap TComplete$,
2) the definition of $SeqSpec(i)$,
3) R and W access location i,
4) that we can choose $T'' = T$,
5) $Reads(S) = LocalReads(S) \cup GlobalReads(S)$,
6) Lemma 5,
7) that R and W are both on location i
8) that R and W are by transactions T and T' respectively, $Visible(S,T) \in TSequential$, and $R \in GlobalReads(Visible(S,T))$ (because $R \in GlobalReads(R)$ and $Visible(S,T)|T = S|T$),
9) Lemma 1,
10) $T' \lessdot_S T$ and $NoWriteBetween_{(Visible(S,T)\ \mid\ i)}(W,R)$,
11) Lemma 2,

12) $T' \in Visible(S,T)$ and $(T' \lessdot_S T)$, and
13) the definition of $Visible(S,T)$. □

Lemma 7. (Invariance) *If $H \equiv H'$, then $Marking(H) = Marking(H')$ and $ReadPres(H) = ReadPres(H')$ and $WriteObs(H) = WriteObs(H')$.*

Proof. Immediate from the definitions of $Marking$, $ReadPres$, and $WriteObs$. □

Lemma 8. $\forall H \in THistory\colon \forall \sqsubseteq \in Marking(H)\colon \exists S \in TSequential\colon H \equiv S \ \wedge \ \preccurlyeq_H \subseteq \preccurlyeq_S \ \wedge \ \preccurlyeq_S \subseteq \sqsubseteq$.

Proof. Let $H \in THistory$ and let $\sqsubseteq \in Marking(H)$. We have that $\sqsubseteq$ is a total order of $Trans$ so we can choose a permutation π on $1..n$ such that $\forall i, j \in 1..n\colon (i < j) \Leftrightarrow (T_{\pi(i)} \sqsubset T_{\pi(j)})$. Define: $S = H|T_{\pi(1)}, \ldots, H|T_{\pi(n)}$. It is straightforward to prove that $S \in TSequential \ \wedge \ H \equiv S \ \wedge \ \preccurlyeq_H \subseteq \preccurlyeq_S \ \wedge \ \preccurlyeq_S \subseteq \sqsubseteq$. □

Lemma 9. *Suppose $\sqsubseteq \in Marking(H) \ \wedge \ p_2 \notin Writers_H(i)$.*
If $NoWriterBetween_{H,i}(T_1, \sqsubseteq, p_2)$ and $NoWriterBetween_{H,i}(p_2, \sqsubseteq, T_3)$,
then $NoWriterBetween_{H,i}(T_1, \sqsubseteq, T_3)$.

Proof.

$$
\begin{aligned}
& NoWriterBetween_{H,i}(T_1, \sqsubseteq, p_2) \ \wedge \ NoWriterBetween_{H,i}(p_2, \sqsubseteq, T_3) \\
\iff\ & \forall T \in Writers_H(i)\colon (T \sqsubseteq T_1 \ \vee \ p_2 \sqsubseteq T) \ \wedge \ (T \sqsubseteq p_2 \ \vee \ T_3 \sqsubseteq T) \\
\iff\ & \forall T \in Writers_H(i)\colon (T \sqsubseteq T_1 \ \wedge \ (T \sqsubseteq p_2 \ \vee \ T_3 \sqsubseteq T)) \ \vee \\
& \qquad\qquad (p_2 \sqsubseteq T \ \wedge \ T \sqsubseteq p_2) \ \vee \ (p_2 \sqsubseteq T \ \wedge \ T_3 \sqsubseteq T) \\
\implies\ & \forall T \in Writers_H(i)\colon (T \sqsubseteq T_1) \ \vee \ (T_3 \sqsubseteq T) \\
\iff\ & NoWriterBetween_{H,i}(T_1, \sqsubseteq, T_3)
\end{aligned}
$$

The first step uses the definition of $NoWriterBetween$. The second step uses $\wedge$ distribution over $\vee$. The third step simplifies the first disjunct using conjunction elimination, eliminates the second disjunct using $p_2 \notin Writers_H(i)$ and simplifies the third disjunct using conjunction elimination. The fourth step uses the definition of $NoWriterBetween$. □

Lemma 10. *Suppose $S \in TSequential \cap TComplete$. We have:*

$$S \in TSeqSpec \iff S \in Markable$$

Proof. Let $S \in TSequential \cap TComplete$. From Lemma 6, the definition of $Markable$, and $S \in TComplete$, we have that we must prove:

$$\begin{aligned}
& S \in LocalTSeqSpec \ \wedge \\
& \forall T \in S \colon \forall i \in I \colon \forall v \in V \colon \forall R = read_T(i){:}v \in GlobalReads(S) \colon \\
& \exists T' \in Committed(S) \colon \exists W = write_{T'}(i,v) \in GlobalWrites(S) \colon \\
& \quad (T' \lessdot_S T) \ \wedge \ NoWriterBetween_{S,i}(T', \preceq_S, T) \\
\iff & \exists \sqsubseteq \in Marking(S) \colon \ \preceq_S \subseteq \sqsubseteq \ \wedge \ \sqsubseteq \in ReadPres(S) \wedge \ \sqsubseteq \in WriteObs(S)
\end{aligned}$$

From the definition of $WriteObs$ and $LastPreAccessor$ we have that:

$$\begin{aligned}
& \sqsubseteq \in WriteObs(S) \\
\iff & S \in LocalTSeqSpec \ \wedge \\
& \forall T \in Trans \colon \forall i \in I \colon \forall v \in V \colon \forall R = read_T(i){:}v \in GlobalReads(S) \colon \\
& \exists T' \in Trans \colon \exists W = write_{T'}(i,v) \in GlobalWrites(S) \colon \\
& \quad T' \in Writers_S(i) \ \wedge \ T' \neq T \ \wedge \ T' \sqsubset R \ \wedge \ NoWriterBetween_{S,i}(T', \sqsubseteq, R) \\
\iff & S \in LocalTSeqSpec \ \wedge \\
& \forall T \in Trans \colon \forall i \in I \colon \forall v \in V \colon \forall R = read_T(i){:}v \in GlobalReads(S) \colon \\
& \exists T' \in Trans \colon \exists W = write_{T'}(i,v) \in GlobalWrites(S) \colon \\
& \quad T' \in Committed(S) \ \wedge \ T' \neq T \ \wedge \ T' \sqsubset R \ \wedge \ NoWriterBetween_{S,i}(T', \sqsubseteq, R)
\end{aligned}$$

We are now ready to prove the two directions of the equivalence.
$\Rightarrow$:
Assume that

$$\begin{aligned}
& S \in LocalTSeqSpec \ \wedge \\
& \forall T \in S \colon \forall i \in I \colon \forall v \in V \colon \forall R = read_T(i){:}v \in GlobalReads(S) \colon \\
& \exists T' \in Committed(S) \colon \exists W = write_{T'}(i,v) \in GlobalWrites(S) \colon \\
& \quad (T' \lessdot_S T) \ \wedge \ NoWriterBetween_{S,i}(T', \preceq_S, T)
\end{aligned}$$

Define:

$$\begin{aligned}
p_1 \sqsubset p_2 \iff & (p_1 \lessdot_S p_2) \ \vee \\
& (thread_S(p_1) \preceq_S p_2) \ \vee \\
& (p_1 \preceq_S thread_S(p_2)) \\
p_1 \sqsubseteq p_2 \iff & p_1 \sqsubset \ \vee \ p_2 p_1 = p_2
\end{aligned}$$

We show that

$$\begin{aligned}
& \sqsubseteq \in Marking(S) \ \wedge \\
& \preceq_S \subseteq \sqsubseteq \ \wedge \ \sqsubseteq \in ReadPres(S) \ \wedge \\
& S \in LocalTSeqSpec \ \wedge \\
& \forall T \in Trans \colon \forall i \in I \colon \forall v \in V \colon \forall R = read_T(i){:}v \in GlobalReads(S) \colon \\
& \exists T' \in Trans \colon \exists W = write_{T'}(i,v) \in GlobalWrites(S) \colon \\
& \quad T' \in Committed(S) \ \wedge \ T' \neq T \ \wedge \ T' \sqsubset R \ \wedge \ NoWriterBetween_{S,i}(T', \sqsubseteq, R)
\end{aligned}$$

It is straightforward to prove $\sqsubseteq \in Marking(S)$ and $\preccurlyeq_S \subseteq \sqsubseteq$, $\sqsubseteq \in ReadPres(S)$. Additionally, the first conjunct of $WriteObs(S)$ (that is, $S \in LocalTSeqSpec$) is immediate from the assumption. So, we still need to prove the second conjunct of $WriteObs(S)$.

Let $T \in Trans$, $i \in I$, $v \in V$, $R = read_T(i){:}v \in GlobalReads(S)$. From the assumption (the left-hand side), we have that we can find (1) $T' \in Committed(S)$ and (2) $W = write_{T'}(i, v) \in GlobalWrites(S)$ such that (3) $(T' \prec\!\!\!\prec_S T)$ and (4) $NoWriterBetween_{S,i}(T', \preccurlyeq_S, T)$. Let us now prove each conjunct of $T' \neq T \ \wedge \ T' \sqsubseteq R \ \wedge \ NoWriterBetween_{S,i}(T', \sqsubseteq, R)$ in turn.

From [3] and that $\preccurlyeq_S$ is a total order of $Trans(S)$, we have (5) $T' \neq T$. From [3] and the definition of $\sqsubseteq$, we have $T' \sqsubseteq R$. From [4] and $\preccurlyeq_S \subseteq \sqsubseteq$, we have (6) $NoWriterBetween_{S,i}(T', \sqsubseteq, T)$. From $T \preccurlyeq_S T$ and the definition of $\sqsubseteq$, we have (7) $R \sqsubseteq T$. From [6], [7] and the definition of $\sqsubseteq$ and transitivity of $\preccurlyeq_S$, we have $NoWriterBetween_{S,i}(T', \sqsubseteq, R)$.

$\Leftarrow$:

Assume the right-hand side and choose $\sqsubseteq \in Marking(S)$ such that:

$$
\begin{aligned}
&\preccurlyeq_S \subseteq \sqsubseteq \ \ \wedge \ \sqsubseteq \in ReadPres(S) \ \wedge \\
&S \in TLocalSeqSpec \ \wedge \\
&\forall T \in Trans\colon \forall i \in I\colon \forall v \in V\colon \forall R = read_T(i){:}v \in GlobalReads(S)\colon \\
&\exists T' \in Committed(S)\colon \exists\ W = write_{T'}(i, v) \in GlobalWrites(S)\colon \\
&\quad T' \neq T \ \wedge \ T' \sqsubseteq R \ \wedge \ NoWriterBetween_{S,i}(T', \sqsubseteq, R)
\end{aligned}
$$

We show that

$$
\begin{aligned}
&S \in LocalTSeqSpec \ \wedge \\
&\forall T \in S\colon \forall i \in I\colon \forall v \in V\colon \forall R = read_T(i){:}v \in GlobalReads(S)\colon \\
&\exists T' \in Committed(S)\colon \exists W = write_{T'}(i, v) \in GlobalWrites(S)\colon \\
&\quad (T' \prec\!\!\!\prec_S T) \ \wedge \ NoWriterBetween_{S,i}(T', \preccurlyeq_S, T)
\end{aligned}
$$

The first conjunct (of the left-hand side), $S \in LocalTSeqSpec$, is immediate from the assumption. From the assumption we have (1) $\preccurlyeq_S \subseteq \sqsubseteq$, (2) $\sqsubseteq \in ReadPres(S)$. Let $T \in Trans$, $i \in I$, $v \in V$, $R = read_T(i){:}v \in GlobalReads(S)$. From the above property of $\sqsubseteq$, we have that we can find (3) $T' \in Committed(S)$ and (4) $W = write_{T'}(i, v) \in GlobalWrites(S)$ such that (5) $T' \neq T$ and (6) $T' \sqsubseteq R$ and (7) $NoWriterBetween_{S,i}(T', \sqsubseteq, R)$. From [1], that $\sqsubseteq$ is a total order on $Trans(S)$ ($\sqsubseteq \in Marking(S)$), and that $\preccurlyeq_S$ is a total order on $Trans(S)$ ($S \in TSequential$), we have (8) $\forall T, T' \in Trans\colon T' \sqsubseteq T \Rightarrow T' \preccurlyeq_S T$.

First we prove $T' \prec\!\!\!\prec_S T$. From [2] ,we have (9) $NoWriterBetween_{S,i}(T, \sqsubseteq, R)$. From [3] and [4], we have (10) $T' \in Writers_S(i)$. From [9] and [10], we have (11) $T' \sqsubseteq T \ \vee \ R \sqsubseteq T'$. From [6], $T' \neq R$ and $\sqsubseteq$ is a total order on $\{R\} \cup Writers_S(i)$ ($\sqsubseteq \in Marking(S)$), we have (12) $R \not\sqsubseteq T'$. From [11] and [12], we have (13) $T' \sqsubseteq T$. From [8] and [13], we have (14) $T' \preccurlyeq_S T$. From [14] and [5], we have $T' \prec\!\!\!\prec_S T$.

Second, we prove $NoWriterBetween_{S,i}(T', \preccurlyeq_S, T)$. From [2], we have (15) $NoWriterBetween_{S,i}(R, \sqsubseteq, T)$. From $R \notin Writers_S(i)$, [7], [15], and Lemma 9, we have (16) $NoWriterBetween_{S,i}(T', \sqsubseteq, T)$. From [16] and [8] we have $NoWriterBetween_{S,i}(T', \preccurlyeq_S, T)$. □

Theorem (Marking) $\mathit{FinalStateOpaque} = \mathit{Markable}$.

Proof.

$$
\begin{aligned}
& \mathit{FinalStateOpaque} \\
= \; & \{H \in \mathit{THistory} \mid \exists H' \in \mathit{TExtension}(H) \colon \exists S \in \mathit{TSequential} \colon \\
& \qquad H' \equiv S \wedge \preccurlyeq_{H'} \subseteq \preccurlyeq_S \wedge S \in \mathit{TSeqSpec}\} \\
= \; & \{H \in \mathit{THistory} \mid \exists H' \in \mathit{TExtension}(H) \colon \exists S \in \mathit{TSequential} \colon \\
& \qquad H' \equiv S \wedge \preccurlyeq_{H'} \subseteq \preccurlyeq_S \wedge S \in \mathit{Markable}\} \\
= \; & \{H \in \mathit{THistory} \mid \exists H' \in \mathit{TExtension}(H) \colon \exists S \in \mathit{TSequential} \colon H' \equiv S \wedge \preccurlyeq_{H'} \subseteq \preccurlyeq_S \wedge \\
& \quad \exists \sqsubseteq \in \mathit{Marking}(S) \colon \preccurlyeq_S \subseteq \sqsubseteq \wedge \sqsubseteq \in \mathit{ReadPres}(S) \cap \mathit{WriteObs}(S)\} \\
= \; & \{H \in \mathit{THistory} \mid \exists H' \in \mathit{TExtension}(H) \colon \exists S \in \mathit{TSequential} \colon H' \equiv S \wedge \preccurlyeq_{H'} \subseteq \preccurlyeq_S \wedge \\
& \quad \exists \sqsubseteq \in \mathit{Marking}(H') \colon \preccurlyeq_S \subseteq \sqsubseteq \wedge \sqsubseteq \in \mathit{ReadPres}(H') \cap \mathit{WriteObs}(H')\} \\
= \; & \{H \in \mathit{THistory} \mid \exists H' \in \mathit{TExtension}(H) \colon \exists \sqsubseteq \in \mathit{Marking}(H') \colon \\
& \quad \sqsubseteq \in \mathit{ReadPres}(H') \cap \mathit{WriteObs}(H') \wedge \\
& \quad \exists S \in \mathit{TSequential} \colon H' \equiv S \wedge \preccurlyeq_{H'} \subseteq \preccurlyeq_S \wedge \preccurlyeq_S \subseteq \sqsubseteq \} \\
= \; & \{H \in \mathit{THistory} \mid \exists H' \in \mathit{TExtension}(H) \colon \exists \sqsubseteq \in \mathit{Marking}(H') \colon \\
& \quad \preccurlyeq_{H'} \subseteq \sqsubseteq \wedge \sqsubseteq \in \mathit{ReadPres}(H') \cap \mathit{WriteObs}(H') \wedge \\
& \quad \exists S \in \mathit{TSequential} \colon H' \equiv S \wedge \preccurlyeq_{H'} \subseteq \preccurlyeq_S \wedge \preccurlyeq_S \subseteq \sqsubseteq \} \\
= \; & \{H \in \mathit{THistory} \mid \exists H' \in \mathit{TExtension}(H) \colon \exists \sqsubseteq \in \mathit{Marking}(H') \colon \\
& \quad \preccurlyeq_{H'} \subseteq \sqsubseteq \wedge \sqsubseteq \in \mathit{ReadPres}(H') \cap \mathit{WriteObs}(H')\} \\
= \; & \mathit{Markable}
\end{aligned}
$$

In these eight steps we apply:
1) the definition of $\mathit{FinalStateOpaque}$,
2) Lemma 10 and $S \in \mathit{TComplete}$ (because $H' \in \mathit{TExtension}(H)$ and $H' \equiv S$),
3) the definition of $\mathit{Markable}$ and $S \in \mathit{TComplete}$,
4) Lemma 7,
5) logical rearrangement,
6) transitivity of $\subseteq$,
7) Lemma 8, and
8) the definition of $\mathit{Markable}$. □

2 TL2 Marking

Shared objects:	Thread-local objects: For each $T \in Trans$:
r: $SafeReg[I]$, initially $\bot$	$rver_T$: $SafeReg$, initially $\bot$
ver: $AtomicReg[I]$, initially 0	$rset_T$: $BasicSet$, initially $\emptyset$
$lock$: $TryLock[I]$, initially $\mathbb{R}$	$wset_T$: $BasicMap$, initially $\emptyset$
$clock$: $SCounter$, initially 0	

```
R01 :  def read_T(i)
R02 :    if (rver_T = ⊥)
R03 :      snap := clock.read()
R04 :      rver_T.write(snap)

R05 :    if (i ∈ dom(wset_T))
R06 :      return wset_T(i)

R07 :    t := ver[i].read()
R08 :    v := reg[i].read()
R09 :    l := lock[i].read()
R10 :    t' := ver[i].read()
R11 :    if(¬(l = false ∧ t = t' ∧ t' ≤ rver_T))
R12 :      return A

R13 :    rver_T.add(i)
R14 :    return v
```

```
W01 :  def write_T(i, v)
W02 :    wset_T.put(i ↦ v)
W03 :    return ok
```

```
C01 :  def commit_T
C02 :    foreach (i ∈ dom(wset_T))
C03 :      locked := lock[i].trylock()
C04 :      if (locked)
C05 :        lset.add(i)
C06 :      else
C07 :        foreach (i ∈ lset) lock[i].unlock()
C08 :        return A

C09 :    wver := clock.iaf
C10 :    if (wver ≠ rver_T + 1)
C11 :      foreach (i ∈ rset_T)
C12 :        l := lock[i].read()
C13 :        t := ver[i].read()
C14 :        if (¬(l = false ∧ t ≤ rver_T))
C15 :          foreach (i ∈ lset) lock[i].unlock()
C16 :          return A

C17 :    foreach ((i ↦ v) ∈ wset_T)
C18 :      reg[i].write(v)
C19 :      ver[i].write(wver)
C20 :      lock[i].unlock()

C21 :    return C
```

In addition to the orders imposed by the data and control dependencies and lock synchronization, the following orders are required: $R06 \prec R07$, $R07 \prec R08$, $R08 \prec R09$, $C12 \prec C13$, $C18 \prec C19$

Figure 1: TL2 Algorithm

Consider an execution history X of TL2 such that $H = X|mem$ and $H \in TComplete$. Let

$$
\begin{aligned}
readAcc(R) &= R08 \text{ in } R \\
writeAcc(T,i) &= C18 \text{ for } i \text{ in } Commit_T \\
Eff(T) &= \begin{cases} R03 \text{ (in the first read of } T) & \text{if } T \in Aborted(H) \\ C09 \text{ (in } commit_T) & \text{if } T \in Committed(H) \end{cases}
\end{aligned}
$$

Let $\prec_{clock}$ represent the linearization order of the strong counter *clock*. The marking $\sqsubseteq$ for H is the reflexive closure of $\sqsubset$ that is define as follows:

$$
\begin{aligned}
&Let\ T, T' \in Trans(H):\\
&\quad T \sqsubset T' \Leftrightarrow Eff(T) \prec_{clock} Eff(T')\\
&Let\ R \in Reads(H), i = arg1(R), T \in Writers_H(i):\\
&\quad T \sqsubset R \Leftrightarrow writeAcc(T,i) \precsim_X readAcc(R)\\
&\quad R \sqsubset T \Leftrightarrow readAcc(R) \prec_X writeAcc(T,i)
\end{aligned}
$$

Figure 2: The marking of TL2.

The marking relation for TL2 is defined in Figure 2. The effect order of transactions is the linearization order of their calls to the *clock* strong counter. The access order of read operations and writer transactions to location i is the execution order of their access to the $reg[i]$ register.

3 DSTM (visible reads) Marking

```
Loc {writer: SafeReg, rset: BasicSet, oldVal: SafeReg, newVal: SafeReg}
Shared objects:
    state: CASReg[Trans], initially ℝ
    ref: CASReg[I], initially new Loc(T_0, ∅, 0, 0)
```

```
def read_T(i)
  r := ref[i].read()
  v := currentValue_T(r)
  r' = r.clone()
  r'.rset.add(T)
  b := ref[i].cas(r, r')
  s := state_T.read()
  if (¬b ∨ (s = 𝔸))
    return A
  else
    return v
```

```
def commit_T()
  b := state_T.cas(ℝ, ℂ)
  if (b)
    return C
  else
    return A
```

```
def currentValue_T(r)
  T' = r.writer.read()
  if (¬(T' = T))
    state_T'.cas(ℝ, A)
  s := state_T'.read()
  if (s = 𝔸)
    return r.oldVal
  else
    return r.newVal
```

```
def write_T(i, v)
  r := ref[i].read()
  w := r.writer.read()
  if (w = T)
    r.newVal.write(v)
    return ok
  v' := currentValue_T(r)
  foreach (T' ∈ r.rset)
    state_T'.cas(ℝ, 𝔸)
  r' := new Loc(T, ∅, v', v)
  b := ref[i].cas(r, r')
  if (b)
    return ok
  else
    return A
```

Figure 3: DSTM (visible reads) Algorithm

Consider an execution history X of DSTM such that $H = X|mem$ and $H \in TComplete$. Let

$$\begin{aligned} readAcc(R) &= R06 \text{ in } R \\ writeAcc(T,i) &= W12 \text{ in the first write to } i \text{ by } T \\ Eff(T) &= \begin{cases} C02 \text{ of the commit operation} & \text{if } T \text{ is committed} \\ R06 \text{ of the last successful read} & \text{if } T \text{ is aborted and has a successful read} \\ \text{Any point in } T & \text{if } T \text{ is aborted and has no successful read} \end{cases} \end{aligned}$$

Let $\prec_{ref[i]}$ represent the linearization order of $ref[i]$. The marking $\sqsubseteq$ for H is the reflexive closure of $\sqsubset$ that is define as follows:

$$\begin{aligned} &Let\ T, T' \in Trans(H): \\ &\quad T \sqsubset T' \Leftrightarrow Eff(T) \precsim_X Eff(T') \\ &Let\ R \in Reads(H), i = arg1(R), T \in Writers_H(i): \\ &\quad T \sqsubset R \Leftrightarrow writeAcc(T,i) \prec_{ref[i]} readAcc(R) \\ &\quad R \sqsubset T \Leftrightarrow readAcc(R) \prec_{ref[i]} writeAcc(T,i) \end{aligned}$$

Figure 4: The marking of DSTM (visible reads).

The marking relation for DSTM (visible reads) is defined in Figure 4.

Committed transactions take effect at the final *cas* of their state from $\mathbb{R}$ to $\mathbb{C}$, $C02$, of their commit operation. Aborted transactions that have successful read operations take effect at state check, $R06$, of their last successful read.

The access order of read operations and writer transactions to location i is the linearization order of their *cas* calls to the $ref[i]$ register.

4 Opacity

$$
\begin{array}{rcl}
\mathit{Reads}(H) & = & \{R \mid R \in H \ \wedge\ \mathit{obj}_H(R) = \mathit{this} \ \wedge \\
& & \qquad \mathit{name}_H(R) = \mathit{read} \ \wedge\ \mathit{retv}_H(R) \neq \mathbb{A}\} \\
\mathit{Writes}(H) & = & \{W \mid W \in H \ \wedge\ \mathit{obj}_H(W) = \mathit{this} \ \wedge \\
& & \qquad \mathit{name}_H(W) = \mathit{write} \ \wedge\ \mathit{retv}_H(W) \neq \mathbb{A}\} \\
\mathit{Trans}(H) & = & \{T \mid \exists l \in H \colon \mathit{thread}_H(l) = T\} \\
\mathit{TSequential} & = & \{S \in \mathit{THistory} \mid \preccurlyeq_S \text{ is a total order of } \mathit{Trans}(S)\} \\
\mathit{Committed}(H) & = & \{T \mid \exists l \in H \colon \mathit{thread}_H(l) = T \ \wedge\ \mathit{retv}_H(l) = \mathbb{C}\} \\
\mathit{Aborted}(H) & = & \{T \mid \exists l \in H \colon \mathit{thread}_H(l) = T \ \wedge\ \mathit{retv}_H(l) = \mathbb{A}\} \\
\mathit{Completed}(H) & = & \mathit{Committed}(H) \cup \mathit{Aborted}(H) \\
\mathit{Live}(H) & = & \mathit{Trans}(H) \setminus \mathit{Completed}(H) \\
\mathit{TComplete} & = & \{H \in \mathit{THistory} \mid \forall T \in \mathit{Trans}(H) \colon T \in \mathit{Completed}(H)\} \\
\mathit{CommitPending}(H) & = & \{T \in \mathit{Live}(H) \mid \exists l \in H \colon \mathit{thread}_H(l) = T \ \wedge\ \mathit{name}_H(l) = \mathit{commit} \\
& & \qquad \mathit{iEv}(l) \Subset H \ \wedge\ \neg(\mathit{rEv}(l) \Subset H)\} \\
\mathit{TExtension}(H) & = & \{H' \in \mathit{THistory} \mid H \text{ is a prefix of } H' \ \wedge\ \forall T \in \mathit{Trans}(H') \Rightarrow T \in \mathit{Trans}(H) \ \wedge \\
& & \qquad \mathit{Live}(H) \setminus \mathit{CommitPending}(H) \subseteq \mathit{Aborted}(H') \ \wedge \\
& & \qquad \mathit{CommitPending}(H) \subseteq \mathit{Completed}(H')\} \\
\mathit{Visible}(S,T) & = & \mathit{filter}\left(S, \lambda T'.(T' = T) \vee \left((T' \prec\!\!\prec_S T) \wedge T' \in \mathit{Committed}(S)\right)\right) \\
\mathit{NoWriteBetween}_S(W,R) & = & \forall W' \in \mathit{Writes}(S) \colon W' \preceq_S W \ \vee\ R \prec_S W' \\
\mathit{SeqSpec}(i) & = & \{S \in \mathit{Sequential} \mid \forall R \in \mathit{Reads}(S) \colon \exists W \in \mathit{Writes}(S) \colon \\
& & \qquad W \prec_S R \ \wedge\ \mathit{NoWriteBetween}_S(W,R) \ \wedge \\
& & \qquad \mathit{retv}_S(R) = \mathit{arg2}_S(W)\} \\
\mathit{TSeqSpec} & = & \{S \in \mathit{TSequential} \cap \mathit{TComplete} \mid \forall T \in S \colon \forall i \in I \colon \\
& & \qquad (\mathit{Visible}(S,T) \mid i) \in \mathit{SeqSpec}(i)\} \\
\mathit{FinalStateOpaque} & = & \{H \in \mathit{THistory} \mid \exists H' \in \mathit{TExtension}(H) \colon \exists S \in \mathit{TSequential} \colon \\
& & \qquad H' \equiv S \wedge\ \preccurlyeq_{H'} \subseteq \preccurlyeq_S \ \wedge S \in \mathit{TSeqSpec}\}
\end{array}
$$

Figure 5: *FinalStateOpaque*

Opacity of a TM algorithm is defined in two steps. First, it is defined what it means for a transaction history to be opaque which is called final-state-opacity. Then, a TM algorithm is defined to be opaque if every transaction history of every source program running on top of that TM algorithm is final-state-opaque.

FinalStateOpaque is defined in Figure 5. We use T prefix before some of the terms to avoid confusion with the terms that we defined above for execution histories of objects. We say that a transaction history is sequential if it is a sequence of transactions. A transaction T is committed or aborted in a transaction history H if there is respectively a commit or abort response event for T in H. A completed transaction is either committed or aborted. A live transaction is a transaction that is not completed. A transaction history is complete if all its transactions are completed. A pending transaction has a pending event and a commit-pending transaction has a commit pending event. An extension of a history is obtained by committing or aborting its commit-pending transactions and aborting the other live transactions. If H is a transaction history and p is a predicate on transaction identifiers, we define $filter(H, p)$ to be the subsequence of H that contains the events of transactions T for which $p(T)$ is true. The visible history for a transaction T in a sequential transaction history S, $Visible(S, T)$, is the sequence of committed transactions before T in S and T itself. The sequential specification of a location i, $SeqSpec(i)$, is the set of sequential histories of read and write method calls on location i where every read returns the value given as the argument to the latest preceding write (regardless of thread identifiers). It is essentially the sequential specification of a register. Transactional sequential specification is the set of complete sequential transaction histories S that for every transaction T and location i, $Visible(S, T)|i$ is a member of the sequential specification of i. A transaction history H is final-state-opaque if there is an equivalent sequential transaction history S for an extension of H such that S is real-time-preserving and a member of transactional sequential specification. The sequential history S is called the justifying history. In other words, every correct concurrent execution is indistinguishable from a correct sequential execution.