Definitions, Theorems, and Proofs of Snapshot Consistency in Agda

Tzu-Chi Lin *Hsiang-Shang Ko*

A Formalizing Behavioral Correctness and Snapshot Consistency

A.1 Overall Structure

In this appendix we present the content of §4 in detail. The definitions, theorems and lemmas, and their proofs are all formalized with the proof assistant Agda. Here we omit the complete proofs, the details of which are all written and checked in Agda, and merely present the important definitions, theorems, and lemmas in the usual mathematical style. Throughout this appendix we will annotate definitions, theorems, etc with the corresponding Agda identifiers enclosed in $\langle\cdot\rangle_{\texttt{Agda}}$, so that readers who are proficient in Agda can look up the identifiers in the source code easily.

The proofs here do not depend on the detail of $\mathbb{P}$ and the invariants on program states, which are proved by an SMT solver and will be formulated as assumptions in section A.2. We will then define $\mathbb{S}$, formulate a generic definition of snapshot consistency and prove the snapshot consistency of $\mathbb{S}$ in section A.3. Next we will formally define the simulation relation between $\mathbb{P}$ and $\mathbb{S}$, but instead of considering the entire $\mathbb{P}$, it suffices to focus on a sub-system $\mathbb{P}^\dagger$ of $\mathbb{P}$ which consists of only the states satisfying the invariants and the transitions "respecting" the invariants. $\mathbb{P}^\dagger$will be defined in section A.4. The simulation relation between $\mathbb{P}^\dagger$ and $\mathbb{S}$, to be defined in section A.5, will be easier to handle (compared to the one between $\mathbb{P}$ and $\mathbb{S}$), and the snapshot consistency of $\mathbb{P}^\dagger$ is the same as that of $\mathbb{P}$ since the property is only about multi-recovery fragments, which can be shown (in section A.4) to be included in $\mathbb{P}^\dagger$. Finally we will present the behavioral correctness and snapshot consistency of $\mathbb{P}^\dagger$ in section A.6.

A.2 The Program Transition System $\mathbb{P}$

We assume that three sets are given,

$$\langle \mathit{Addr}\rangle_{\texttt{Agda}},\ \langle \mathit{Data}\rangle_{\texttt{Agda}},\ \text{and}\ \langle \mathit{RawState}^P\rangle_{\texttt{Agda}}$$

where *Addr* is the set of memory addresses, *Data* the set of values of memory cells, $\mathit{RawState}^P$ the set of all possible program states. The exact definitions of these sets are irrelevant to the Agda proof and omitted. We will need to read the memory cells in a program state, which is done by the function

$$\langle \mathit{read}\rangle_{\texttt{Agda}} : \mathit{RawState}^P \to (\mathit{Addr} \to \mathit{Data})$$

which returns the mapping from memory cell addresses to their values in a program state. We also assume that there is a predicate $\langle \mathit{Init}^R\rangle_{\texttt{Agda}}$ on $\mathit{RawState}^P$ that is used to identify the new disk states.

The (labelled) transition system $\mathbb{P}$ uses $\mathit{RawState}^P$ as its states, and its actions (labels) are defined by

$$\begin{aligned}\langle \mathit{Action}\rangle_{\texttt{Agda}} \triangleq\ & \{\, \mathsf{w}_{\mathit{addr},\mathit{data}} \mid \mathit{addr} \in \mathit{Addr}, \mathit{data} \in \mathit{Data} \,\} \\ \cup\ & \{\, \mathsf{w}^{\mathsf{c}}_{\mathit{addr},\mathit{data}} \mid \mathit{addr} \in \mathit{Addr}, \mathit{data} \in \mathit{Data} \,\} \\ \cup\ & \{\mathsf{sf}, \mathsf{r}, \mathsf{rl}, \mathsf{es}, \mathsf{sf}^{\mathsf{c}}, \mathsf{r}^{\mathsf{c}}, \mathsf{rl}^{\mathsf{c}}, \mathsf{es}^{\mathsf{c}}\}\end{aligned}$$

Most of the time the pair of address and data in a w or w^{c} action is not important, in which case we will omit the subscript. We will refer to a transition system whose labels are drawn from *Action* as a *disk model* — in particular, $\mathbb{P}$ is a disk model. The ternary (single-step) transition relation of $\mathbb{P}$ is

$$\to_{\mathbb{P}} \subseteq \mathit{RawState}^P \times \mathit{Action} \times \mathit{RawState}^P \qquad \langle \_[\![\_]\!]^{\mathrm{R}} \blacktriangleright \_\rangle_{\texttt{Agda}}$$

Its exact definition is, again, irrelevant for our purposes and omitted. We write

$$s \xrightarrow{a}_{\mathbb{P}} s'$$

when state s transits to s' through action a in $\mathbb{P}$.

Recall that there are two types of invariants on the states, the representation invariant $\langle \mathit{RI}\rangle_{\texttt{Agda}}$ and the crash representation invariant $\langle \mathit{CI}\rangle_{\texttt{Agda}}$, which are preserved or transformed by the transitions; these properties are proved by an SMT solver, and are made assumptions in this proof.

Assumption A.1 (type B per-operation correctness)**.** For all $s, s' \in \mathit{RawState}^P$, the following are assumed:

$$\langle \mathit{RIRI}\rangle_{\texttt{Agda}} \qquad s \xrightarrow{\mathsf{w}}_{\mathbb{P}} s' \wedge \mathit{RI}(s) \implies \mathit{RI}(s')$$

$$s \xrightarrow{\mathsf{sf}}_{\mathbb{P}} s' \wedge RI(s) \implies RI(s')$$
$$s \xrightarrow{\mathsf{rl}}_{\mathbb{P}} s' \wedge RI(s) \implies RI(s')$$
$$s \xrightarrow{\mathsf{es}}_{\mathbb{P}} s' \wedge RI(s) \implies RI(s')$$

$\langle RICI \rangle_{\texttt{Agda}}$ $\quad s \xrightarrow{\mathsf{w^c}}_{\mathbb{P}} s' \wedge RI(s) \implies CI(s')$

$$s \xrightarrow{\mathsf{sf^c}}_{\mathbb{P}} s' \wedge RI(s) \implies CI(s')$$
$$s \xrightarrow{\mathsf{rl}}_{\mathbb{P}} s' \wedge RI(s) \implies CI(s')$$
$$s \xrightarrow{\mathsf{es}}_{\mathbb{P}} s' \wedge RI(s) \implies CI(s')$$

$\langle CIRI \rangle_{\texttt{Agda}}$ $\quad s \xrightarrow{\mathsf{r}}_{\mathbb{P}} s' \wedge CI(s) \implies RI(s')$

$\langle CICI \rangle_{\texttt{Agda}}$ $\quad s \xrightarrow{\mathsf{r^c}}_{\mathbb{P}} s' \wedge CI(s) \implies CI(s')$

It is also proved by an SMT solver that the new disk states satisfy *CI*.

Assumption A.2 ($\langle init^R\text{-}CI \rangle_{\texttt{Agda}}$)**.**

$$Init^R(s) \implies CI(s)$$

A.3 The Specification Transition System $\mathbb{S}$

For the disk model $\mathbb{S}$, its states are those in the set

$$\langle State \rangle_{\texttt{Agda}} \triangleq (Addr \to Data) \times (Addr \to Data) \times \mathbb{N}$$

each of which contains a pair of mappings from *Addr* to *Data* and a natural number; these two mappings represent the volatile and stable parts of a state in the specification, and the natural number is the write count. Similarly to *read* in $\mathbb{P}$, the functions

$$volatile : State \to (Addr \to Data) \quad \langle State.volatile \rangle_{\texttt{Agda}}$$
$$stable : State \to (Addr \to Data) \quad \langle State.stable \rangle_{\texttt{Agda}}$$

extract the respective mappings from a *State*. The new states of $\mathbb{S}$ are characterized by the predicate $\langle Init(s) \rangle_{\texttt{Agda}} \triangleq \forall a.\ stable(s)(a) = defaultData$ where $\langle defaultData \rangle_{\texttt{Agda}} \in Data$ is some default value for memory cells. The transition relation

$$\to_{\mathbb{S}} \subseteq State \times Action \times State \qquad \langle \_[\![\_]\!] \blacktriangleright \_ \rangle_{\texttt{Agda}}$$

has been defined in figure 4 in the main text.

Next we define snapshot consistency generically for disk models. To do so we will need to define sequences of transitions and particular forms of traces (i.e., sequences of actions, which form a set $\langle Trace \rangle_{\texttt{Agda}}$). Then we are able to prove the snapshot consistency on $\mathbb{S}$.

Definition A.3 (fragments, $\langle RTC \rangle_{\texttt{Agda}}$)**.** Let $T = (S, \Lambda, \to)$ be a labelled transition system. A *fragment* in T is a sequence of transitions

$$s_0 \xrightarrow{a_1} s_1 \xrightarrow{a_2} \cdots \xrightarrow{a_n} s_n$$

where $s_i \in S$ and $a_j \in \Lambda$ for all i and j. We sometimes omit the intermediate states and write

$$s_0 \xrightarrow{a_1, a_2, \ldots, a_n}\!\!\!\!\!\rightarrow\ s_n$$

Note that a fragment may contain no transitions, in which case the starting and ending states are the same:

$$s_0 \twoheadrightarrow s_0$$

Definition A.4 (one-recovery traces, $\langle OneRecovery \rangle_{\texttt{Agda}}$)**.** A *one-recovery* trace has one of the following forms:

- $a_1, \ldots, a_{k-1}, \mathsf{sf}, b_1, \ldots, b_\ell, \mathsf{w^c}, (\mathsf{r^c})^m, \mathsf{r}$,
- $a_1, \ldots, a_{k-1}, \mathsf{sf}, b_1, \ldots, b_\ell, \mathsf{sf^c}, (\mathsf{r^c})^m, \mathsf{r}$,
- $b_1, \ldots, b_\ell, \mathsf{w^c}, (\mathsf{r^c})^m, \mathsf{r}$, and
- $b_1, \ldots, b_\ell, \mathsf{sf^c}, (\mathsf{r^c})^m, \mathsf{r}$,

where a_i are successful regular or flush operations and b_j are successful regular operations.

This is the trace part of one-recovery fragments defined in the main text, expanded to four cases to simplify the subsequent proof structure.

Definition A.5 (multi-recovery traces, $\langle MultiRecovery \rangle_{\texttt{Agda}}$)**.** The set of *multi-recovery* traces is inductively defined by the following two rules:

- a trace of the form $(\mathsf{r^c})^m\,\mathsf{r}$ is a multi-recovery trace, and
- the concatenation tr, tr' of a multi-recovery trace tr and a one-recovery trace tr' is a multi-recovery trace.

Note that, differently from the main text, the two notions above are defined on traces rather than fragments; to reconcile the difference, we will say that a fragment is one-/multi-recovery when its trace is one-/multi-recovery. Also note that the definition of multi-recovery fragments in this appendix is more specific than that in the main text (where the first state is required to be new and there are some trailing transitions), but below we will state our theorems in a way that makes them apply to the multi-recovery fragments as defined in the main text.

Definition A.6 (snapshot consistency of a one-recovery fragment, $\langle SnapshotConsistency \rangle_{\texttt{Agda}}$)**.** A one-recovery fragment *fr* is *snapshot-consistent* under an equivalence relation *ER* if

- $ER(s_2, s_4)$
  when $fr = s_1 \xrightarrow{a_1, \ldots, a_{k-1}}\!\!\!\!\!\rightarrow\ s_2 \xrightarrow{\mathsf{sf}, b_1, \ldots, b_\ell, \mathsf{w^c}, (\mathsf{r^c})^m, \mathsf{r}}\!\!\!\!\!\rightarrow\ s_4$,
- $ER(s_3, s_4)$ or $ER(s_2, s_4)$
  when $fr = s_1 \xrightarrow{a_1, \ldots, a_{k-1}}\!\!\!\!\!\rightarrow\ s_2 \xrightarrow{\mathsf{sf}, b_1, \ldots, b_\ell}\!\!\!\!\!\rightarrow\ s_3 \xrightarrow{\mathsf{sf^c}, (\mathsf{r^c})^m, \mathsf{r}}\!\!\!\!\!\rightarrow\ s_4$,

- $ER(s_2, s_4)$
  when $fr = s_2 \xrightarrow{b_1,\ldots,b_\ell,\mathsf{w}^\mathsf{c},(\mathsf{r}^\mathsf{c})^m,\mathsf{r}}\!\!\!\!\rightarrow\!\!\!\!\rightarrow s_4$, or
- $ER(s_3, s_4)$ or $ER(s_2, s_4)$
  when $fr = s_2 \xrightarrow{b_1,\ldots,b_\ell}\!\!\!\!\rightarrow s_3 \xrightarrow{\mathsf{sf}^\mathsf{c},(\mathsf{r}^\mathsf{c})^m,\mathsf{r}}\!\!\!\!\rightarrow s_4$.

Theorem A.7 (snapshot consistency of $\mathbb{S}$, $\langle Spec.SC\rangle_{\texttt{Agda}}$)**.** For every fragment $t_0 \xrightarrow{tr}\!\!\!\!\rightarrow t_1 \xrightarrow{tr'}\!\!\!\!\rightarrow t_2$ in $\mathbb{S}$ where $Init(t_0)$ holds, tr is multi-recovery, and tr' is one-recovery, the sub-fragment $t_1 \xrightarrow{tr'}\!\!\!\!\rightarrow t_2$ is snapshot-consistent under the equivalence relation $ER(t,t') \triangleq volatile(t) = volatile(t')$.

On the surface this theorem may appear weaker than the one claimed in the main text, but we can easily show that every one-recovery sub-fragment fr in a multi-recovery fragment is snapshot-consistent by applying the theorem to the sub-fragment ending with fr, so this theorem is in fact general enough. The theorem, combined with the simulation between $\mathbb{S}$ and $\mathbb{P}^\dagger$, will be used to establish the proof of the snapshot consistency of $\mathbb{P}^\dagger$ in later sections.

A.4 The Sub-System $\mathbb{P}^\dagger$ with Invariants

$\mathbb{P}^\dagger$ is a disk model whose set of states $\langle State^P\rangle_{\texttt{Agda}}$ is a subset of $RawState^P$ — states that satisfy either RI or CI.

The states of $\mathbb{P}^\dagger$ is defined as follows:

$$State^P \triangleq \{\, s \in RawState^P \mid RI(s) \vee CI(s) \,\}$$

The transition relation of $\mathbb{P}^\dagger$,

$$\rightarrow_{\mathbb{P}^\dagger} \subseteq State^P \times Action \times State^P \qquad \langle \_[\![\_]\!]^P \blacktriangleright \_\rangle_{\texttt{Agda}}$$

which is, similarly, a subset of $\rightarrow_{\mathbb{P}}$, is defined by

$$\xrightarrow{\mathsf{w}_{a,d}}_{\mathbb{P}^\dagger} \triangleq \{\, (s,s') \mid s \xrightarrow{\mathsf{w}_{a,d}}_{\mathbb{P}} s' \wedge RI(s) \wedge RI(s') \,\}$$
$$\xrightarrow{\mathsf{sf}}_{\mathbb{P}^\dagger} \triangleq \{\, (s,s') \mid s \xrightarrow{\mathsf{sf}}_{\mathbb{P}} s' \wedge RI(s) \wedge RI(s') \,\}$$
$$\xrightarrow{\mathsf{rl}}_{\mathbb{P}^\dagger} \triangleq \{\, (s,s') \mid s \xrightarrow{\mathsf{rl}}_{\mathbb{P}} s' \wedge RI(s) \wedge RI(s') \,\}$$
$$\xrightarrow{\mathsf{es}}_{\mathbb{P}^\dagger} \triangleq \{\, (s,s') \mid s \xrightarrow{\mathsf{es}}_{\mathbb{P}} s' \wedge RI(s) \wedge RI(s') \,\}$$
$$\xrightarrow{\mathsf{r}}_{\mathbb{P}^\dagger} \triangleq \{\, (s,s') \mid s \xrightarrow{\mathsf{r}}_{\mathbb{P}} s' \wedge CI(s) \wedge RI(s') \,\}$$
$$\xrightarrow{\mathsf{w}^\mathsf{c}_{a,d}}_{\mathbb{P}^\dagger} \triangleq \{\, (s,s') \mid s \xrightarrow{\mathsf{w}^\mathsf{c}_{a,d}}_{\mathbb{P}} s' \wedge RI(s) \wedge CI(s') \,\}$$
$$\xrightarrow{\mathsf{sf}^\mathsf{c}}_{\mathbb{P}^\dagger} \triangleq \{\, (s,s') \mid s \xrightarrow{\mathsf{sf}^\mathsf{c}}_{\mathbb{P}} s' \wedge RI(s) \wedge CI(s') \,\}$$
$$\xrightarrow{\mathsf{rl}^\mathsf{c}}_{\mathbb{P}^\dagger} \triangleq \{\, (s,s') \mid s \xrightarrow{\mathsf{rl}^\mathsf{c}}_{\mathbb{P}} s' \wedge RI(s) \wedge CI(s') \,\}$$
$$\xrightarrow{\mathsf{es}^\mathsf{c}}_{\mathbb{P}^\dagger} \triangleq \{\, (s,s') \mid s \xrightarrow{\mathsf{es}^\mathsf{c}}_{\mathbb{P}} s' \wedge RI(s) \wedge CI(s') \,\}$$
$$\xrightarrow{\mathsf{r}^\mathsf{c}}_{\mathbb{P}^\dagger} \triangleq \{\, (s,s') \mid s \xrightarrow{\mathsf{r}^\mathsf{c}}_{\mathbb{P}} s' \wedge CI(s) \wedge CI(s') \,\}$$

From assumption A.1, we can prove that every multi-recovery fragment which starts from a new disk state in $\mathbb{P}$ is also one in $\mathbb{P}^\dagger$, where a new disk state in $\mathbb{P}^\dagger$ is characterized by the predicate $\langle Init^P(s)\rangle_{\texttt{Agda}} \triangleq Init^R(s) \wedge CI(s)$, so when considering only such fragments in $\mathbb{P}$, which are ranged over by the statements of behavioral correctness and snapshot consistency, we can work with $\mathbb{P}^\dagger$ instead.

Lemma A.8 ($\langle lift\text{-}mr\rangle_{\texttt{Agda}}$)**.** For every multi-recovery fragment $s \xrightarrow{tr}\!\!\!\!\rightarrow_{\mathbb{P}} s'$ where $Init^R(s)$ holds, there exists a fragment $s \xrightarrow{tr}\!\!\!\!\rightarrow_{\mathbb{P}^\dagger} s'$ such that $Init^P(s)$, $CI(s)$, and $RI(s')$ hold.

A.5 Simulation of $\mathbb{P}^\dagger$ by $\mathbb{S}$

To establish the behavioral correctness and snapshot consistency of $\mathbb{P}^\dagger$, we first define a simulation of $\mathbb{P}^\dagger$ by $\mathbb{S}$. The simulation relation is the disjunction of the two abstraction relations $\langle AR\rangle_{\texttt{Agda}}$ and $\langle CR\rangle_{\texttt{Agda}}$. The two relations are transformed or preserved by each operation in $\mathbb{P}^\dagger$; these have been proved by an SMT solver, and are thus made assumptions.

Assumption A.9 (type A per-operation correctness)**.** For all $s, s' \in State^P$ and $t \in State$, the following are assumed:

$\langle ARAR\rangle_{\texttt{Agda}}$

$$s \xrightarrow{\mathsf{w}}_{\mathbb{P}^\dagger} s' \wedge AR(s,t) \implies \exists t'.\, t \xrightarrow{\mathsf{w}}_{\mathbb{S}} t' \wedge AR(s',t')$$
$$s \xrightarrow{\mathsf{sf}}_{\mathbb{P}^\dagger} s' \wedge AR(s,t) \implies \exists t'.\, t \xrightarrow{\mathsf{sf}}_{\mathbb{S}} t' \wedge AR(s',t')$$
$$s \xrightarrow{\mathsf{rl}}_{\mathbb{P}^\dagger} s' \wedge AR(s,t) \implies \exists t'.\, t \xrightarrow{\mathsf{rl}}_{\mathbb{S}} t' \wedge AR(s',t')$$
$$s \xrightarrow{\mathsf{es}}_{\mathbb{P}^\dagger} s' \wedge AR(s,t) \implies \exists t'.\, t \xrightarrow{\mathsf{es}}_{\mathbb{S}} t' \wedge AR(s',t')$$

$\langle ARCR\rangle_{\texttt{Agda}}$

$$s \xrightarrow{\mathsf{w}^\mathsf{c}}_{\mathbb{P}^\dagger} s' \wedge AR(s,t) \implies \exists t'.\, t \xrightarrow{\mathsf{w}^\mathsf{c}}_{\mathbb{S}} t' \wedge CR(s',t')$$
$$s \xrightarrow{\mathsf{sf}^\mathsf{c}}_{\mathbb{P}^\dagger} s' \wedge AR(s,t) \implies \exists t'.\, t \xrightarrow{\mathsf{sf}^\mathsf{c}}_{\mathbb{S}} t' \wedge CR(s',t')$$
$$s \xrightarrow{\mathsf{rl}^\mathsf{c}}_{\mathbb{P}^\dagger} s' \wedge AR(s,t) \implies \exists t'.\, t \xrightarrow{\mathsf{rl}^\mathsf{c}}_{\mathbb{S}} t' \wedge CR(s',t')$$
$$s \xrightarrow{\mathsf{es}^\mathsf{c}}_{\mathbb{P}^\dagger} s' \wedge AR(s,t) \implies \exists t'.\, t \xrightarrow{\mathsf{es}^\mathsf{c}}_{\mathbb{S}} t' \wedge CR(s',t')$$

$\langle CRAR\rangle_{\texttt{Agda}}$

$$s \xrightarrow{\mathsf{r}}_{\mathbb{P}^\dagger} s' \wedge CR(s,t) \implies \exists t'.\, t \xrightarrow{\mathsf{r}}_{\mathbb{S}} t' \wedge AR(s',t')$$

$\langle CRCR\rangle_{\texttt{Agda}}$

$$s \xrightarrow{\mathsf{r}^\mathsf{c}}_{\mathbb{P}^\dagger} s' \wedge CR(s,t) \implies \exists t'.\, t \xrightarrow{\mathsf{r}^\mathsf{c}}_{\mathbb{S}} t' \wedge CR(s',t')$$

Definition A.10 (simulation relation, $\langle SR\rangle_{\texttt{Agda}}$)**.**

$$SR(s,t) \triangleq AR(s,t) \vee CR(s,t)$$

From assumption A.9 we can show that SR is indeed a simulation relation.

Theorem A.11 ($\langle simSR\rangle_{\texttt{Agda}}$)**.**

$$\forall s, s' \in State^P, t \in State, a \in Action.$$
$$s \xrightarrow{a}_{\mathbb{P}^\dagger} s' \wedge SR(s,t) \implies \exists t'.\, t \xrightarrow{a}_{\mathbb{S}} t' \wedge SR(s',t')$$

Also proved with an SMT solver, for every pair of $s \in State^P$ and $t \in State$ that satisfy $AR(s,t)$, *observational equivalence* holds, that is, the content of s is equivalent to the content of the volatile part of t.

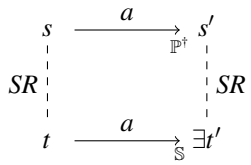

Figure 1: Illustration of theorem A.11

Assumption A.12 ($\langle AR \Rightarrow ObsEquiv \rangle_{\texttt{Agda}}$)**.**

$$\forall s \in State^P, t \in State. AR(s,t) \implies read(s) \equiv volatile(t)$$

A.6 Behavioral correctness and snapshot consistency of $\mathbb{P}^\dagger$

To state the behavioral correctness more easily, we give some auxiliary definitions. We define two multi-recovery fragments with the same trace, one in $\mathbb{P}$ and one in $\mathbb{S}$, to be $\langle Conformant \rangle_{\texttt{Agda}}$ if every pair of corresponding normal states are observationally equivalent. Since a multi-recovery fragment consists of multiple one-recovery fragments, we define $\langle Conformant\text{-}1R \rangle_{\texttt{Agda}}$ to describe conformance particularly between two one-recovery fragments, and $\langle Conformant\text{-}all \rangle_{\texttt{Agda}}$ to describe conformance between two fragments where every action in the trace is successful (i.e. without crashes).

Definition A.13 (*Conformant-all*)**.** For two fragments $frP = s \xrightarrow{tr}{}_{\mathbb{P}^\dagger} s'$ and $frS = t \xrightarrow{tr}{}_{\mathbb{S}} t'$, $Conformant\text{-}all(frP, frS)$ holds if

- tr is an empty trace,

or when tr is nonempty and can be written as tr', a where a is the last action, both of the following hold,

- $frP' = s \xrightarrow{tr'}{}_{\mathbb{P}^\dagger} s''$ and $frS' = t \xrightarrow{tr'}{}_{\mathbb{S}} t''$ satisfy $Conformant\text{-}all(frP', frS')$,
- s' and t' are observationally equivalent.

Definition A.14 (*Conformant-1R*)**.** For two one-recovery fragments $frP = s \xrightarrow{tr}{}_{\mathbb{P}^\dagger} s'$ and $frS = t \xrightarrow{tr}{}_{\mathbb{S}} t'$, $Conformant\text{-}1R(frP, frS)$ holds if one of the following holds.

- In the case of $frP = s_1 \xrightarrow{a_1,\ldots,a_{k-1}}{}_{\mathbb{P}^\dagger} s_2 \xrightarrow{\mathsf{sf}, b_1,\ldots,b_\ell}{}_{\mathbb{P}^\dagger} s_3 \xrightarrow{\mathsf{w}^\mathsf{c}, (\mathsf{r}^\mathsf{c})^m, \mathsf{r}}{}_{\mathbb{P}^\dagger} s_4$, and $frS = t_1 \xrightarrow{a_1,\ldots,a_{k-1}}{}_{\mathbb{S}} t_2 \xrightarrow{\mathsf{sf}, b_1,\ldots,b_\ell}{}_{\mathbb{S}} t_3 \xrightarrow{\mathsf{w}^\mathsf{c}, (\mathsf{r}^\mathsf{c})^m, \mathsf{r}}{}_{\mathbb{S}} t_4$, *Conformant-all* holds for the sub-fragment from s_1 to s_3 and the sub-fragment from t_1 to t_3, and s_4 is observationally equivalent to t_4.
- In the case of $frP = s_1 \xrightarrow{a_1,\ldots,a_{k-1}}{}_{\mathbb{P}^\dagger} s_2 \xrightarrow{\mathsf{sf}, b_1,\ldots,b_\ell}{}_{\mathbb{P}^\dagger} s_3 \xrightarrow{\mathsf{sf}^\mathsf{c}, (\mathsf{r}^\mathsf{c})^m, \mathsf{r}}{}_{\mathbb{P}^\dagger} s_4$, and $frS = t_1 \xrightarrow{a_1,\ldots,a_{k-1}}{}_{\mathbb{S}} t_2 \xrightarrow{\mathsf{sf}, b_1,\ldots,b_\ell}{}_{\mathbb{S}} t_3 \xrightarrow{\mathsf{sf}^\mathsf{c}, (\mathsf{r}^\mathsf{c})^m, \mathsf{r}}{}_{\mathbb{S}} t_4$, *Conformant-all* holds for the sub-fragment from s_1 to s_3 and the sub-fragment from t_1 to t_3, and s_4 is observationally equivalent to t_4.
- In the case of $frP = s_2 \xrightarrow{b_1,\ldots,b_\ell}{}_{\mathbb{P}^\dagger} s_3 \xrightarrow{\mathsf{w}^\mathsf{c}, (\mathsf{r}^\mathsf{c})^m, \mathsf{r}}{}_{\mathbb{P}^\dagger} s_4$, and $frS = t_2 \xrightarrow{b_1,\ldots,b_\ell}{}_{\mathbb{S}} t_3 \xrightarrow{\mathsf{w}^\mathsf{c}, (\mathsf{r}^\mathsf{c})^m, \mathsf{r}}{}_{\mathbb{S}} t_4$. *Conformant-all* holds for the sub-fragment from s_2 to s_3 and the sub-fragment from t_2 to t_3, and s_4 is observationally equivalent to t_4,
- In the case of $frP = s_2 \xrightarrow{b_1,\ldots,b_\ell}{}_{\mathbb{P}^\dagger} s_3 \xrightarrow{\mathsf{sf}^\mathsf{c}, (\mathsf{r}^\mathsf{c})^m, \mathsf{r}}{}_{\mathbb{P}^\dagger} s_4$, and $frS = t_2 \xrightarrow{b_1,\ldots,b_\ell}{}_{\mathbb{S}} t_3 \xrightarrow{\mathsf{sf}^\mathsf{c}, (\mathsf{r}^\mathsf{c})^m, \mathsf{r}}{}_{\mathbb{S}} t_4$, *Conformant-all* holds for the sub-fragment from s_2 to s_3 and the sub-fragment from t_2 to t_3, and s_4 is observationally equivalent to t_4.

Definition A.15 (*Conformant*)**.** For two multi-recovery fragments $frP = s \xrightarrow{tr}{}_{\mathbb{P}^\dagger} s'$ and $frS = t \xrightarrow{tr}{}_{\mathbb{S}} t'$, *Conformant* is inductively defined as follows:

- In the case of $frP = s \xrightarrow{(\mathsf{r}^\mathsf{c})^m, \mathsf{r}}{}_{\mathbb{P}^\dagger} s'$ and $frS = t \xrightarrow{(\mathsf{r}^\mathsf{c})^m, \mathsf{r}}{}_{\mathbb{S}} t'$, s' is observationally equivalent to t', or
- in the case of $frP = s \xrightarrow{tr}{}_{\mathbb{P}^\dagger} s'' \xrightarrow{tr'}{}_{\mathbb{P}^\dagger} s'$ and $frS = t \xrightarrow{(tr}{}_{\mathbb{S}} t'' \xrightarrow{tr'}{}_{\mathbb{S}} t'$, s' where tr is multi-recovery and tr' is one-recovery, all of the following hold:
  - The sub-fragment from s to s'' and the sub-fragment from t to t'' satisfy *Conformant*.
  - The sub-fragment from s'' to s' and the sub-fragment fron t'' to t' satisfy *Conformant-1R*.
  - s'' and t'' are observationally equivalent.

With *Conformant* defined, behavioral correctness can then be stated as follows. Note that our goal is to establish the behavioral correctness and snapshot consistency of the kind of multi-recovery fragments defined in the main text, whose traces are of the form

$$(r^c)^m, r, tr_1, \ldots, tr_n, tr'$$

where $tr_1, \ldots, tr_n$ are one-recovery fragments, and tr' is a trailing fragment without any crashes.

Theorem A.16 (behavioral correctness, $\langle BC \rangle_{\texttt{Agda}}$)**.** For all fragments $frP_1 = s \xrightarrow{tr}{}_{\mathbb{P}^\dagger} s'$ and $frP_2 = s' \xrightarrow{tr'}{}_{\mathbb{P}^\dagger} s''$ where tr is a multi-recovery trace and tr' is a trace consists of only successful regular and snapshot operations, there exist two

corresponding fragments $frS_1 = t \xrightarrow{tr}\!\!\!\!\rightarrow_{\mathbb{S}} t'$ and $frS_2 = t' \xrightarrow{tr'}\!\!\!\!\rightarrow_{\mathbb{S}} t''$ such that frP_1 and frS_1 satisfy *Conformant*, while frP_2 and frS_2 satisfy *Conformant-all*.

Theorem A.16 can be established with theorem A.11, as described in the main text and proved in Agda. Finally, we can show the snapshot consistency of $\mathbb{P}$ with the help of theorem A.16, the details of which has been presented both in the main text and Agda.

Theorem A.17 (snapshot consistency of $\mathbb{P}^\dagger$, $\langle Prog.SC \rangle_{\texttt{Agda}}$)**.** For every fragment in $\mathbb{P}^\dagger$ of the form $s_0 \xrightarrow{tr}\!\!\!\!\rightarrow_{\mathbb{P}^\dagger} s_1 \xrightarrow{tr'}\!\!\!\!\rightarrow_{\mathbb{P}^\dagger} s_2$, where $Init^P(s_0)$ holds, tr is multi-recovery, and tr' is one-recovery, the sub-fragment $s_1 \xrightarrow{tr'}\!\!\!\!\rightarrow_{\mathbb{P}^\dagger} s_2$ is snapshot-consistent under the equivalence relation $ER(s,s') \triangleq read(s) = read(s')$.