

# SYNCOPE: Automatic Enforcement of Distributed Consistency Guarantees

Kia Rahmani<sup>1</sup>, Gowtham Kaki<sup>1</sup>, and Suresh Jagannathan<sup>1</sup>

Purdue University, West Lafayette IN 47906, USA  
{rahmank,gkaki,suresh}@purdue.edu

**Abstract.** Designing reliable and highly available distributed applications typically requires data to be replicated over geo-distributed stores. But, such architectures force application developers to make an undesirable tradeoff between ease of reasoning, possible when replicated data is required to be strongly consistent, and performance, possible when such guarantees are weakened. Unfortunately, undesirable behaviors may arise under weak consistency that can violate application correctness, forcing designers to either implement ad-hoc mechanisms to avoid these anomalies, or choose to run applications using stronger levels of consistency than necessary. The former approach introduces unwanted complexity, while the latter sacrifices performance. In this paper, we describe a lightweight runtime verification system that relieves developers from having to make such tradeoffs. Instead, our approach leverages declarative axiomatic specifications that reflect the necessary constraints any correct implementation must satisfy to guide a runtime consistency enforcement and monitoring mechanism. This mechanism guarantees a *provably optimal* strategy that imposes no additional communication or blocking overhead beyond what is required to satisfy the specification, allowing distributed operations to run in a *provably safe* environment. Experimental results show that the performance of our automatically derived mechanisms is better than both specialized hand-written protocols and common store-offered consistency guarantees, providing strong evidence of its practical utility.

**Keywords:** Runtime Safety Enforcement and Monitoring, Weak Consistency, Distributed Systems, Haskell

## 1 Introduction

Historically, the *de facto* system abstraction for developing distributed programs has typically included ACID<sup>1</sup> properties. These properties guarantee replication transparency (i.e. requiring distributed systems to *appear* as a single compute and storage server to users), and make it straightforward to develop standardized implementation and reasoning techniques around *strongly consistent* (SC) distributed stores. Although such strong notions of consistency simplify reasoning,

---

<sup>1</sup> Atomicity, Consistency, Isolation and Durability

they also introduce extensive synchronization overhead which is often unacceptable for web-scale applications that need to be “always-on” even in the presence of network partitions. Applications are therefore usually designed to tolerate certain *inconsistencies*, in exchange for availability and low latency. An extreme example is *eventual consistency* (EC), where the local state of each node only represents an *unspecified order* of an *unspecified subset* of the aggregate collection of all updates submitted to the system globally. Consequently, application level invariants that hold under strong consistency might break under eventual consistency. Applications that cannot tolerate these anomalous behaviors under EC may choose to run under a stronger, albeit still weaker than SC, consistency model. Weak notions of consistency, however, are closely tied to specific data-store implementations. More often than not, however, users are offered a choice of consistency levels that negatively impacts performance. In order to overcome this issue, developers are forced to inject their code with *ad-hoc* anomaly tolerance mechanisms that are closely tied to application logic, confounding standardization, and complicates application reasoning, maintainability, and reusability.

In this paper, we propose a dramatically different alternative. SYNCOPE is a lightweight runtime verification system for Haskell that allows application developers to take advantage of weak consistency without having to re-engineer their code to accommodate anomaly preemption mechanisms. The key insight that drives SYNCOPE’s design is that the hardness of reasoning about the integrity of a distributed application stems from conflating application logic with consistency enforcement logic, requiring reasoning about both *operationally*. By separating application semantics from consistency enforcement semantics, however, admitting operational reasoning for the former, and declarative reasoning for the latter, programmers are liberated from having to worry about implementation details of anomaly preemption mechanisms, allowing them to be focused instead on application semantics, under the assumption that specified consistency requirements are automatically enforced by the data store at runtime. Our approach admits declarative reasoning for consistency enforcement via a specification language that allows programmers to formally specify consistency requirements. The design of our specification language is based on the observation that all anomalous behaviors allowed under EC occur as the result of nodes executing operations before certain *dependencies* are satisfied. Using SYNCOPE, one can specify arbitrary dependency relations between updates, and a runtime monitoring and verification system working on top of each EC data store replica guarantees that an operation will only proceed if it can witness all of its dependencies. For example, *lost-updates* is a well-known anomaly possible under EC that occurs when an operation *o* from a client session is routed to a replica different than the replica that served earlier operations from the same session, because of transient system properties, such as load balancing or network partitions. When this happens, *o* may successfully execute without witnessing updates from those earlier operations. In this case, because *o* is dependent on updates from *all previous operations from the same sessions*, SYNCOPE guarantees to temporarily block operations until these dependencies become available

at  $o$ 's replica. Of course, if this anomalous behavior can be tolerated by the application, this level of dependency tracking will be elided.

We make the following contributions: (i) We propose an expressive specification language to express fine-grained consistency requirements of applications in terms of the dependencies between operations. (ii) We describe a generic runtime consistency enforcement mechanism that analyzes each operation's consistency specification, and ensures that its dependencies are available at the replicas on which it executes. We formalize the system's operational semantics, and prove its correctness and optimality. (iii) We describe an implementation of these ideas in a tool called SYNCOPE, which works on top of an off-the-shelf EC data store. Evaluation over realistic applications and microbenchmarks, demonstrate the performance benefits of making fine-grained distinctions between consistency guarantees, and the ease of doing so via our specification language.

The remainder of the paper is organized as follows. A system model that describes the key notions of consistency and replication is presented in Sec. 2. In Sec. 3, we provide a detailed example to further motivate the problem. In Sec. 4 and Sec. 5, we formally present our specification language and the high level operational semantics of the runtime system, with correctness and optimality theorems. Sec. 6 elaborates on the algorithmic aspects of our runtime that is key to its efficient realization. Sec. 7 describes implementation of SYNCOPE, and evaluates its applicability and practical utility. Related work and conclusion are presented in Sec. 8 and Sec. 9.

## 2 System Model

A data store in our system model is a collection of *replicas* ( $\#1, \#2, \dots$ ), each of which maintains a copy of a set of replicated *data object* ( $\mathbf{x}, \mathbf{y}, \dots$ ). Each data object includes and maintains a *state value* ( $\mathbf{v}, \mathbf{v}', \dots$ ) and is equipped with a set of *operations* ( $\text{op}, \text{op}', \dots$ ). Operations may read the state of an object residing in a replica, and modify it by generating *update effects* ( $\eta, \eta', \dots$ ). These effects are then asynchronously sent to all other replicas where they are applied to the state of the object instance at the recipient replica using a user-supplied function. Figs. 1a and 1b illustrate this process.

Because there is no direct synchronization between replicas when an operation is executed, concurrent and possibly conflicting updates can be generated at different replicas. Conflict resolution is handled at the point when an effect is applied to the current state of the object, and must be designed to ensure that all replicas eventually converge to the same value, assuming generated effects quiesce. This model admits all inconsistencies and anomalies associated with eventual consistency [1, 2].

Clients in our model interact with the store by invoking operations on objects. A *session* is a sequence of operations invoked by a particular client. Consequently, operations (and effects) can be uniquely identified by the *session id* that invoked them, and their *sequence number* in that particular session, which is used by replicas to record the set of all updates that are locally applied. Since,

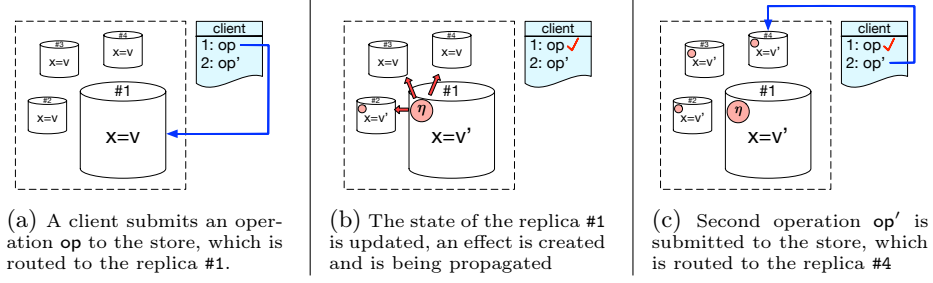


Fig. 1: system model of SYNCOPE

```

1 type Effect = String
2 type State = String
3
4 read :: State -> (String, Maybe Effect)
5 read s = (s, Nothing)
6
7 write :: String -> ((), Maybe Effect)
8 write comment = ((), Just comment)
9
10 apply :: State -> Effect -> State
11 apply s comment = s ++ comment

```

(a) A simple implementation

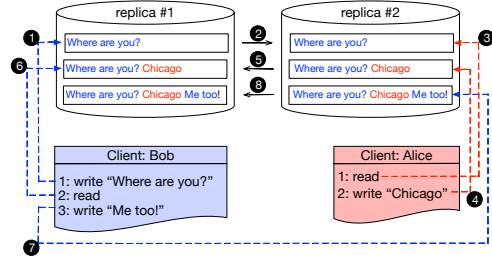


Fig. 2: A distributed application for comment section management

the data store may be concurrently accessed by a large number of clients, operations (even from the same session) might be routed to different replicas to improve latency (see Figs. 1a and 1c).

Lastly, we define two relations over effects created in the store. *Session order* ( $so$ ) is an irreflexive, transitive relation that relates an effect to all subsequent effects from the same session. *Visibility* ( $vis$ ) is an irreflexive and asymmetric relation that relates an effect to all others that are influenced by it (i.e., witnesses its update) at the time of their generation. For example, in Fig. 1c  $vis(\eta, \eta')$  holds, since  $\eta$  (the effect of  $op$ ) has already been delivered and applied to the replica #4, when  $op'$  is executed and thus has influenced generation of  $\eta'$ .

### 3 Motivation

#### 3.1 Replicated Data Types in ECDS

To motivate our approach, consider a highly available (low latency) application for managing comments on posts in a photo sharing web site. Fig. 2a presents a simple Haskell implementation of such an application cognizant of our system model.

In this implementation, **Effect** and **State** strings are respectively defined as the text of a single comment, and the concatenation of all visible comments

associated with a post. A new **Effect** is generated every time a user wants to comment on a post by calling the **write** function, and a **read** call simply returns the **State** of the object at the serving replica. The **apply** function, returns the updated state of the replica, which is the concatenation of the old state and the given effect. For perspicuity, we omit any conflict resolution strategy in the code; however, developers (using timestamps, roll-backs, etc.) can design the **apply** function to resolve conflicting concurrent updates as they desire, consistent with application invariants.

An example of how users interact with this application is presented in Fig.2b, where Alice and Bob invoke operations on an object (here, a photo of Alice in Chicago); the chronological order of events is given in black circles. At time ❶, Bob writes a comment, which is routed to replica #1, whose effect is then propagated and delivered to replica #2 at ❷; while Alice’s first read operation is routed to ❸. Alice and Bob then keep talking, generating more read and write events, while updates are propagated concurrently between the two replica.

As mentioned before, lost updates, is a well-known, often undesirable, behavior admitted by eventually consistent data stores (ECDS). An example of such anomaly can occur here if at time ❹, Bob is temporarily disconnected from both replicas in the figure, and his read operation is routed to another replica #3, that has not yet received any updates from #1 or #2. Consequently, Bob cannot see his first comment and would retry submitting it, assuming it failed the first time it was sent. This would result in multiple copies of the message eventually being displayed on each replica.

### 3.2 Ad-hoc Anomaly Prevention

One way to prevent the above anomaly is to tag each effect using a unique identifier as mentioned in Sec. 2. Using these tags, replicas will be able to track all locally available effects, and temporarily *block* operations, until all the preceding effects from the same session arrive at the replica. For example, the replica #3 that receives Bob’s read in the above undesired scenario, can simply postpone its execution until all prior effects upon which this operation depends reach this replica..

In order to reduce the overhead of tracking dependencies per operation, the above idea can be refined using another technique called *filtration*, which is based on separating the locally available effects at each replica that have not yet been applied to the state from those who have. In the above example each replica can maintain a *safe environment* for operations (e.g. using a soft-state cache), that contains an effect only if it also contains all the previous effects from the same session. This way, an operation can proceed, when the effect of its previous operation from the same session is already applied to the state (which transitively yields the presence of all dependencies).

We present a modified version of the running example in Appendix A, updated to tolerate the lost-update anomaly by implementing the blocking mechanism in the **read** function and incorporating filtration in the **apply** function

$ \begin{aligned} r &\in \text{rel.seed} := \text{vis} \mid \text{so} \mid r \cup r \\ R &\in \text{relation} := r \mid R; r \mid \text{null} \\ \pi &\in \text{prop} := \forall a. a \xrightarrow{R} \hat{\eta} \Rightarrow a \xrightarrow{\text{vis}} \hat{\eta} \\ \psi &\in \text{spec} := \pi \mid \pi \wedge \pi \end{aligned} $	<table border="1"> <thead> <tr> <th>Guarantee</th><th>Contract</th></tr> </thead> <tbody> <tr> <td>RMW</td><td><math>\forall a. a \xrightarrow{\text{so}} \hat{\eta} \Rightarrow a \xrightarrow{\text{vis}} \hat{\eta}</math></td></tr> <tr> <td>MW</td><td><math>\forall a. a \xrightarrow{\text{so}; \text{vis}} \hat{\eta} \Rightarrow a \xrightarrow{\text{vis}} \hat{\eta}</math></td></tr> <tr> <td>MR</td><td><math>\forall a. a \xrightarrow{\text{vis}; \text{so}} \hat{\eta} \Rightarrow a \xrightarrow{\text{vis}} \hat{\eta}</math></td></tr> <tr> <td>2VIS</td><td><math>\forall a. a \xrightarrow{\text{vis}; \text{vis}} \hat{\eta} \Rightarrow a \xrightarrow{\text{vis}} \hat{\eta}</math></td></tr> </tbody> </table>	Guarantee	Contract	RMW	$\forall a. a \xrightarrow{\text{so}} \hat{\eta} \Rightarrow a \xrightarrow{\text{vis}} \hat{\eta}$	MW	$\forall a. a \xrightarrow{\text{so}; \text{vis}} \hat{\eta} \Rightarrow a \xrightarrow{\text{vis}} \hat{\eta}$	MR	$\forall a. a \xrightarrow{\text{vis}; \text{so}} \hat{\eta} \Rightarrow a \xrightarrow{\text{vis}} \hat{\eta}$	2VIS	$\forall a. a \xrightarrow{\text{vis}; \text{vis}} \hat{\eta} \Rightarrow a \xrightarrow{\text{vis}} \hat{\eta}$
Guarantee	Contract										
RMW	$\forall a. a \xrightarrow{\text{so}} \hat{\eta} \Rightarrow a \xrightarrow{\text{vis}} \hat{\eta}$										
MW	$\forall a. a \xrightarrow{\text{so}; \text{vis}} \hat{\eta} \Rightarrow a \xrightarrow{\text{vis}} \hat{\eta}$										
MR	$\forall a. a \xrightarrow{\text{vis}; \text{so}} \hat{\eta} \Rightarrow a \xrightarrow{\text{vis}} \hat{\eta}$										
2VIS	$\forall a. a \xrightarrow{\text{vis}; \text{vis}} \hat{\eta} \Rightarrow a \xrightarrow{\text{vis}} \hat{\eta}$										
(a) syntax of contracts	(b) examples										

Fig. 4: SYNCOPE Specification Language

as explained above. Unfortunately, these modifications require fundamental and pervasive changes to the original code. Additionally, the changes are heavily tangled with application logic, complicating reasoning, hampering correctness arguments, and sacrificing composability and scalability.

### 3.3 Our Solution

SYNCOPE is a runtime enforcement mechanism that allows developers to define a consistency level for each operation *a priori*, delegating the responsibility for ensuring that constraints defined by this level are respected. Our technique generalizes blocking and filtration mechanisms, admits arbitrary user-defined dependency relations for each operation, and maintains a consistent *shim layer* on top of each ECDS replica.

The SYNCOPE shim layer maintains multiple safe environments ( $E_1, E_2, \dots$ ) by periodically (or on-demand) reading from the underlying ECDS database, and adding effects to each environment, only if its dependencies have already been added (Fig.3). SYNCOPE realizes this idea efficiently, using a simple tagging mechanism that represents effects in an environment via a tag associated with that environment. Each operation only witnesses effects from its associated environment, and is blocked by the runtime system if the necessary dependencies are not present.

Users can specify arbitrary consistency guarantees in a language that is seeded with **so** and **vis** relations. Constraints on read operations can be used to synthesize appropriate filtration and blocking mechanisms. For example, the following *contract*, eliminates the possibility of lost-update anomalies by establishing the appropriate conditions under which an effect may be witnessed by the current operation:

$$\psi : \forall a. \xrightarrow{\text{so}} \hat{\eta} \Rightarrow a \xrightarrow{\text{vis}} \hat{\eta}$$

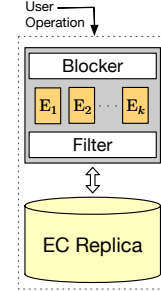


Fig. 3: SYNCOPE

## 4 Specification Language

The formal syntax of our specification (or contract) language, presented in Fig.4a, allows definitions of **prop**, a first-order formula that establishes dependency relations between effects, necessary to determine the effects an operation may witness, under a given consistency level. The language is seeded with **so** and

$\text{vis}$ , respectively representing session order and visibility relations over effects, and defines dependency **relation** as a sequence<sup>2</sup> of seeds, where  $(a \xrightarrow{\mathbf{r}_1; \dots; \mathbf{r}_k} b)$  is interpreted as  $\exists c. (a \xrightarrow{\mathbf{r}_1; \dots; \mathbf{r}_{k-1}} c \wedge c \xrightarrow{\mathbf{r}_k} b)$ .  $\text{null}$  is the empty relation. Additionally, the language allows conjunctions of propositions, **spec**, used to define a safe environment free from *multiple* inconsistencies. Our language is crafted to capture all fine-grained weak consistency levels, including well-known ones such as those explicated by Terry et al. [2] (see e.g., Fig.4b).

We provide two important classes of contracts, and explain how they can be satisfied with different enforcement techniques.

LB: A *lower bound* (LB) contract is one in which all defined dependency relations end with an **so**, i.e. are of the following form:  $(\forall a. a \xrightarrow{\mathbf{r}_1; \mathbf{r}_2; \dots; \mathbf{so}} \hat{\eta} \Rightarrow a \xrightarrow{\text{vis}} \hat{\eta})$ .

It specifies the smallest set of effects that any operation should witness to maintain consistency, e.g. RMW and MR in Fig.4b.

UB: Similarly, we define *upper bound* (UB) contracts as those whose dependency relations end with a **vis**. These contracts define constraints on the set of effects made visible to each operation; if an effect is in the set, certain dependencies of that effect must also be included, e.g. 2VIS and MW in Fig.4b.

Our consistency enforcement approach is based on blocking operations with LB contracts to make sure that they witness *all effects that they are supposed to*, and filtering for UB contracts to make sure that they do not witness *effects that they are not supposed to*.

## 5 Semantics

In this section, we present the consistency enforcement mechanism of SYNCOPE, abstracted as a formal operational semantics. Our approach is complete for the specification language defined in Sec.4. However for better comprehensibility, we present the semantics and the theorems parameterized over a contract consisting of a single proposition. Therefore, in the rest of this section, we will assume a given contract  $\psi$  of the following form:

$$\psi = \forall a. a \xrightarrow{\mathbf{r}_1; \mathbf{r}_2; \dots; \mathbf{r}_k} \hat{\eta} \Rightarrow a \xrightarrow{\text{vis}} \hat{\eta} \quad \mathbf{r}_i \in \{\text{vis}; \text{so}\}$$

The operational semantics defines a small-step relation over *execution states*, which are tuples of the form  $E = (A, \text{vis}, \text{so})$ . The *effect soup*  $A$  stands for the set of all effects produced in the system, and *primitive relations*  $\text{vis}, \text{so} \subseteq A \times A$ , respectively represent the visibility and session order among such effects. Figs. 5a and 5b present a simple execution state consisting of 9 effects with associated primitive relations<sup>3</sup>. We denote the subset of  $A$  consisting of effects that satisfy a certain condition as  $A_{(\text{condition})}$ .

Note that SYNCOPE's contracts are in fact constraints over execution states, where the domain of quantification is fixed to the effect soup  $A$ , and interpretation for **so** and **vis** relations (which occur free in the contract formulae) are also

<sup>2</sup> SYNCOPE also allows using closures of seeds, which is omitted here for simplicity.

<sup>3</sup> We omit drawing transitive **so** edges (e.g. between  $\eta_8$  and  $\eta_1$ ) for better readability.

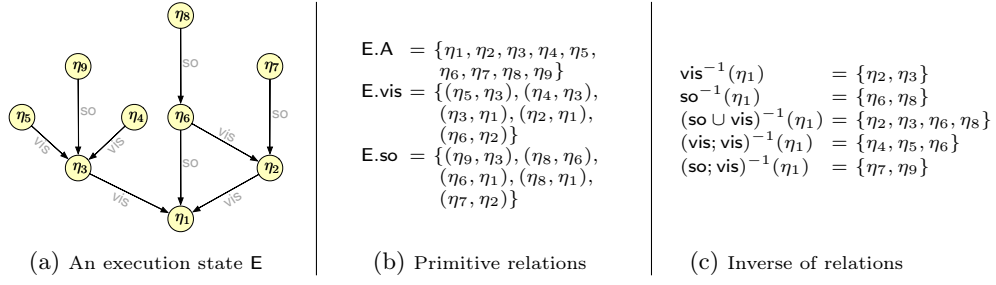


Fig. 5: A simple execution state

provided. Thus, execution states are potential models for any first-order formula expressible in the specification language. If an execution state  $E$  is a valid model for a contract  $\psi$ , we say that  $E$  satisfies  $\psi$  ( $E \models \psi$ ).

The reduction relation in our semantics is of the form  $(E, \text{op}_{<s,i>}) \xrightarrow{V} (E', \eta)$ , which can be interpreted as a transformation of the initial execution state  $E$ , caused by a replica with a local set of effects  $V$ , when it executes  $\text{op}$ , the  $i^{\text{th}}$  operation from the session  $s$ . During this reduction step, a new effect  $\eta$  is produced and added to the system, resulting in a new execution state  $E'$  composed of an updated effect soup and new primitive relations.

### 5.1 Preliminaries

Before presenting the operational semantics, we first introduce supporting definitions and notations. We start by defining the interpretation of an *inversed* dependency relation  $R^{-1}$  under an execution state  $E$ , which is utilized in the basis of our consistency enforcement mechanism. We previously mentioned our interpretation for  $\text{so}$  and  $\text{vis}$  between effects under  $E$ ; this can now be straightforwardly extended to their inverse as follows<sup>4</sup>:

$$\mathbf{r}^{-1}(S) = \bigcup_{b \in S} \{a \mid (a, b) \in E.\mathbf{r}\} \quad \mathbf{r} \in \{\text{so}, \text{vis}\} \quad (1)$$

Additionally, based on our interpretation of the sequences of seed relations given in Sec.4, we can extend the above definition:

$$b \in (R'; \mathbf{r})^{-1}(a) \iff \exists c. c \in \mathbf{r}^{-1}(a) \wedge b \in (R')^{-1}(c) \quad (2)$$

It might seem that we are ready to define any  $R^{-1}$  based on the two definitions above; however, note that definition (2) fails to capture the reality of our system model, where all computations are performed by replicas independently; at any given moment, a replica might have access to only a *subset of all produced effects* in the system. For example, consider  $(\text{so}; \text{vis})^{-1}(\eta_1)$  under the execution state presented in Fig.5. In order to compute this set, based on (2) we have:

$$b \in (\text{so}; \text{vis})^{-1}(\eta_1) \iff \exists c. c \in \text{vis}^{-1}(\eta_1) \wedge b \in (\text{so})^{-1}(c)$$

<sup>4</sup> Note that when the input of an inversed relation is a singleton  $\{\eta\}$ , we drop the brackets and simply write it as  $\mathbf{r}^{-1}(\eta)$



Now, since there exists *mid-level* effects  $c = \eta_2$  and  $c = \eta_3$ , that satisfy the above definition respectively for  $\eta_7$  and  $\eta_9$ , we can conclude:  $(\text{so}; \text{vis})^{-1}(\eta_1) = \{\eta_7, \eta_9\}$ . Consider a replica that contains  $\{\eta_1, \eta_6, \eta_7, \eta_9\}$  at the moment, and wants to check if the dependencies of  $\eta_1$  are locally present or not. Even though based on the above definition, the answer is affirmative (since the replica does contain  $\{\eta_7, \eta_9\}$ ), the replica has no way to verify it, since the mid-level effects  $\eta_2$  and  $\eta_3$  are not present at the replica yet.

To capture the above property, we redefine the inverse of  $R$ , *according to a set of available effects*  $V$ , that considers whether all required mid-level effects are present in  $V$ . The following definition is based on (1) and a more strict version of (2):

$$b \in R_V^{-1}(a) \iff \begin{cases} \perp & \text{if } R = \text{null} \\ b \in \mathbf{r}^{-1}(a) & \text{if } R = \mathbf{r} \\ \exists c. c \in \mathbf{r}^{-1}(a) \wedge b \in (R')_V^{-1}(c) \wedge \mathbf{r}^{-1}(a) \subseteq V & \text{if } R = R'; \mathbf{r} \end{cases} \quad (3)$$

For example, in Fig.5,  $(\eta_9 \in (\text{so}; \text{vis})_{\{\eta_1, \eta_3\}}^{-1}(\eta_1))$  holds, but  $(\eta_9 \notin (\text{so}; \text{vis})_{\{\eta_1\}}^{-1}(\eta_1))$ .

We define a set  $V$  to be *self-contained* for a given effect  $\eta$ , written as  $\mathbb{SC}_\eta^R(V)$ , if  $V$  contains all the required mid-level effects to compute  $R$  inverse of  $\eta$  in totality, i.e.

$$\mathbb{SC}_\eta^R(V) \iff R_V^{-1}(\eta) = R_{E.A}^{-1}(\eta) \quad (4)$$

For example in Fig.5,  $\mathbb{SC}_{\eta_1}^R(V)$  holds for an arbitrary  $R$  and for any  $V$  that is a superset of  $\{\eta_1, \eta_2, \eta_3, \eta_4, \eta_5\}$ .

We define  $\text{trunc}()$  as a function that given  $R \in \text{relation}$ , returns a new relation by removing the last element from the sequence in  $R$ :

$$\text{trunc}(R) = \begin{cases} \text{null} & \text{if } R = \mathbf{r} \text{ or } R = \text{null} \\ R' & \text{if } R = R'; \mathbf{r} \end{cases} \quad (5)$$

Finally, we define *closed subsets* of a given set  $V$ , as the subsets that are closed under  $(\text{trunc}(R))_V^{-1}$ , that also contain all the required mid-level effects to compute  $\text{trunc}(R)^{-1}$ . Moreover, we define the largest element among such subsets, as the *maximally closed subset* of  $V$  as follows<sup>5</sup>:

$$\begin{aligned} \text{closed subsets : } V' \in [V] & \iff V' \subseteq V \wedge (\text{trunc}(R))_V^{-1}(V') \subseteq V' \wedge \mathbb{SC}_\eta^{\text{trunc}(R)}(V') \\ \text{maximally closed subset : } V' = [V]_{\max} & \iff V' \in [V] \wedge \nexists V'' \in [V] . |V''| > |V'| \end{aligned}$$

## 5.2 Core Operational Semantics

Our operational semantics is defined as a set of reduction rules representing our consistency enforcement approach (see Fig.6). The small-step reduction relation  $(\rightarrow)$  is parametrized over a set  $V$ , which stands for the locally available set of effects at the replica taking the reduction step. Trivially,  $V$  must be a subset of all effects in the system at the initial execution state, however, there is no other

<sup>5</sup> We slightly abuse the previously defined notation in (3) and use a *set* of effects as the input of  $R^{-1}$ , which is defined as:  $x \in R_V^{-1}(S) \iff \exists (y \in S). x \in R_V^{-1}(y)$ .

### Auxiliary Definitions

$op \in \text{Oper. Name}$	$F_{op} \in \text{Op. Def.} := \mathcal{P}(\eta) \mapsto v$
$v \in \text{Ret. Val.}$	$A \in \text{Eff Soup} := \mathcal{P}(\eta)$
$s \in \text{Sess. ID}$	$\text{vis, so} \in \text{Relations} := \mathcal{P}((\eta, \eta))$
$\eta \in \text{Effect} := (s, op, v)$	$E \in \text{Exec State} := (A, \text{vis}, \text{so})$

### Auxiliary Reduction

$$S \vdash (E, op_{<s, i>}) \hookrightarrow (E', \eta)$$

[OPER]

$$\frac{S \subseteq A \quad F_{op}(S) = v \quad \eta \notin S \quad \eta = (s, op, v) \quad A' = A \cup \{\eta\} \quad \text{vis}' = \text{vis} \cup (S \times \{\eta\}) \quad \text{so}' = \text{so} \cup (A_{(\text{SessID}=s)} \times \{\eta\})}{S \vdash ((A, \text{vis}, \text{so}), op_{<s, i>}) \hookrightarrow ((A', \text{vis}', \text{so}'), \eta)}$$

### Operational Semantics

$$(E, op_{<s, i>}) \xrightarrow{V} (E', \eta)$$

[UB EXEC]

$$\frac{\mathbf{r}_k = \text{vis} \quad V \subseteq E.A \quad V' = [V]_{\max} \quad V' \vdash (E, op_{<s, i>}) \hookrightarrow (E', \eta)}{(E, op_{<s, i>}) \xrightarrow{V} (E', \eta)}$$

[LB EXEC]

$$\frac{\mathbf{r}_k = \text{so} \quad V \subseteq E.A \quad \mathbb{SC}_\eta^R(V) \quad R_V^{-1}(\eta) \subseteq V \quad V \vdash (E, op_{<s, i>}) \hookrightarrow (E', \eta)}{(E, op_{<s, i>}) \xrightarrow{V} (E', \eta)}$$

Fig. 6: Core Operational semantics of a replicated data store.

restrictions on  $V$ , since we only assume eventual consistency in the underlying store.

The rule [OPER] defines the abstract procedure of generating a new effect  $\eta$ , by witnessing a set of effects  $S$ , using a user-defined function  $F_{op}$ . We formally define an effect as a tuple  $\eta = (s, op, v)$ , representing the session  $s$ , operation name  $op$  whose execution created  $\eta$ , and the value  $v$  that the replica returns, responding to that operation. Moreover, the rule explains how the execution state changes after a new effect is produced. Specifically, in the new execution state, the effect soup  $A'$  contains the newly created effect  $\eta$ , the relation  $\text{vis}'$  captures the fact that all effects in the set  $S$  were made visible to  $\eta$ , and  $\text{so}'$  states that all effects from the same session as the current operation that are already present in the system, should be in session order with  $\eta$  in the final execution state.

Rule [UB EXEC], defines the execution of an operation in a replica under a UB contract. The rule requires operations to only witness  $V'$ , the maximally closed subset of  $V$ . Thus, the rule governs how replicas create safe environments for operations, by filtering out undesirable or unwanted effects.

Rule [LB EXEC] defines the step taken by a replica when an operation is executed under an LB contract. The precondition  $R_V^{-1}(\eta) \subseteq V$  in the rule ensures that the reduction happens only if the effects necessary to avoid the specified anomaly are present in  $V$ , assuming that  $V$  contains all the mid-level effects to determine dependencies of the newly created effect  $\eta$  (i.e. is a self contained set). Thus, the rule governs replicas to block execution of an operation under an LB contract, if the replica is unable to verify the presence of all necessary dependent effects.

### 5.3 Soundness and Optimality

In this section we present our meta-theoretic results on the desired properties for our consistency enforcement mechanism. Three theorems are presented, regarding the correctness of our approach, maximality of witnessed effects by each operation (i.e. minimum staleness) and the liveness guarantee of the system assuming the eventual delivery of all effects at all replicas. Detailed proofs of all theorems can be found in appendix B.

Before presenting the theorems, we define a  $\psi$ -consistent set of effects  $S$  under an execution state  $E$  as a set that is closed under  $(R = \mathbf{r}_1; \dots; \mathbf{r}_k)$ , i.e.

$$S \text{ is } \psi\text{-consistent} \iff \forall (\eta \in S). \forall (a \in E.A). R(a, \eta) \Rightarrow a \in S \quad (6)$$

**Theorem 1.** *For all reduction steps  $(E, op_{<s,i>}) \xrightarrow{V} (E', \eta)$ , the followings hold:*

- (i) *If  $V$  is  $\psi$ -consistent under  $E$ , then  $V \cup \{\eta\}$  is  $\psi$ -consistent under  $E'$*
- (ii)  *$E' \models \psi[\eta/\hat{\eta}]$*

The above theorem states the preservation of  $\psi$ -consistency at replicas, under reduction steps. Moreover, it states the correctness of the enforced consistency guarantee at the final execution state.

**Theorem 2.** *For all reduction steps  $(E, op_{<s,i>}) \xrightarrow{V} (E', \eta)$ , the set of effects made visible to  $\eta$  is maximal. i.e. for all  $a \in V$ , if  $\mathbb{SC}_a^{\text{trunc}(R)}(V)$ , then*

$$(a, \eta) \notin E'.\text{vis} \Rightarrow (E'.A, E'.\text{vis} \cup \{(a, \eta)\}, E'.so) \not\models \psi[\eta/\hat{\eta}]$$

**Theorem 3.** *For all execution states  $E$ , if there exists a set of effects  $S \subseteq E.A$ , such that:*

$$S \vdash (E, op_{<s,i>}) \hookrightarrow (E', \eta) \quad \wedge \quad (S \cup \{\eta\} \text{ is } \psi\text{-consistent under } E')$$

*then there exist  $E'', \eta'$  and  $V$  such that:  $((E, op_{<s,i>}) \xrightarrow{V} (E'', \eta'))$*

A trivial corollary of the above theorem is the liveness of our operational semantics, since at least one set  $S$  with the requested properties always exists<sup>6</sup> at any execution state.

## 6 Algorithm

While the semantics defines *what* subset of effects at a replica must be witnessed by every operation, it does not address *how* to realize efficient construction of that subset.

SYNCOPE maintains a consistent cache on top of each replica by periodically reading from the underlying ECDS, where an effect  $\eta$  is moved to the cache only if the cache already includes  $\text{trunc}(R)_V^{-1}(\eta)$ . Consequently, all operations under UB contracts can be immediately executed by witnessing the cache, which is a

<sup>6</sup>  $S = E.A$ . This requires the preservation of  $\psi$ -consistency under the reduction step, that is already shown in theorem 1.

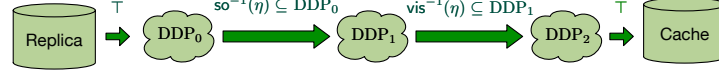


Fig. 7: Example of stepwise progress of effects before entering the cache

closed subset (not necessarily maximal) of  $V$ , the set of effects present at the replica. Moreover, LB contracts can also be satisfied, by blocking operations until effects of all previous operations from the same session enter the cache, in which case the current operation can proceed and witness *all* effects present at the replica.

Additionally, we implemented a simple memoization technique in SYNCOPe that extends the binary notion of dependency presence to the *degree of dependency presence* (DDP) representing the maximum *depth* (or size) of the dependencies of an effect, whose presence have been verified so far. Consequently, when verification of the presence of dependencies for an effect fails, the runtime system can avoid redundant computations the time it tries to verify the same property for the same effect. SYNCOPe's runtime, by performing periodic DDP refreshes, tries to assign larger DDP values to each effect when more dependencies arrive at the replica. Specifically, at each refresh, the DDP of an effect  $\eta$  is increased from  $i$  to  $i + 1$  if all effects in  $r_{i+1}^{-1}(\eta)$  already have DDP values at least equal to  $i$ .

For example, consider a contract with dependency relation  $R = \text{so}; \text{vis}; \text{so}$ , and a newly arrived effect  $\eta$  to the replica, whose DDP is initially set to 0. During the next refresh,  $\eta$  is given the value 1, if all effects in  $\text{so}^{-1}(\eta)$  have DDP equal to 0 (i.e. are present at the replica). Similarly,  $\eta$  is given the value 2, if all effects in  $\text{vis}^{-1}(\eta)$  have DDP value of at least 1, which means that  $(\text{so}; \text{vis})_V^{-1}(\eta)$  is now present at the replica and consequently,  $\eta$  can be safely added to the consistent cache (Fig.7). Using this technique, SYNCOPe avoid redundant computations of potentially large dependency relations.

## 7 Evaluation

In this section, we present an evaluation study of our implementation, including a report on benchmark applications that utilize fine-grained weak consistency requirements, expressible in SYNCOPE’s specification language. Fig.8 presents seven such programs, that include library definitions of individual replicated data types as well as larger programs consisting of multiple replicated types.

Each program offers various operations, each of which is assigned a potentially different consistency requirement, representing the need for a multi-consistent environment for efficient execution. We found 4 different kinds of consistency anomalies, in which 11 out of 38 (not requiring SC) operations defined in these programs were involved in, providing evidence for the need of a generic multi-consistent environment for efficient program execution. Surprisingly, we found no program intrinsically requiring causal consistency; all known consistency anomalies that operations may be involved in are expressible with simple fine-grained contracts composed of dependency relations of length 1 or 2, which differs from what was known in the context before, where all such operations were considered to require CC.

«««< HEAD Additionally, in many cases we found operations that may be involved in multiple anomalies, requiring simultaneous enforcement of different consistency guarantees, which shows the infeasibility of hand-writing such guarantees, considering the vast set of known consistency anomalies. For example, consider a bank account application, which offers `deposit`, `withdraw` and `get_balance` operations, where `withdraw` is a strongly consistent operation that succeeds only if there are sufficient funds in the account. There are two anomalous scenarios associated with `get_balance` in this program: (i) when a user performs a `deposit` that is not reflected in subsequent `get_balance` operations; (ii) when a `get_balance` witnesses a `withdraw` effect without witnessing all `deposit` effects visible to it, resulting in `get_balance` returning a potentially (incorrect) negative balance. As presented in Fig. 8, to preempt these anomalies, `get_balance` requires both RMW and 2VIS guarantees to be simultaneously satisfied.

We have deployed SYNCOPE on a cloud cluster, consisting of three fully replicated Cassandra replicas, running on separate machines within the same data-center. Each machine is instantiated with a SYNCOPE shim layer, that responds to clients, which are instantiated on a VM co-located with one of the replicas on a machine. We deploy the cluster on three `m4.xlarge` Amazon EC2 instances

Benchmark	Consistency	Description
Counter	MR	Monotonically increasing counter, e.g. YouTube’s watch count
DynamoDB	RMW	Integer register allowing various conditional puts and gets
Online Store	RMW	Online store with shopping carts and modifiable item prices
Bankaccount	2VIS $\wedge$ RMW	Offering deposit, withdraw and get balance operations
Shopping List	MW $\wedge$ RMW	A shopping list with concurrent adds and deletes functionality
Microblog	MW, RMW	A Twitter-like application modeled after Twissandra
Rubis	RMW, RMW $\wedge$ 2VIS	eBay-like application with browsing, supporting user wallet

Fig. 8: Fine-grained consistency requirement in benchmark programs

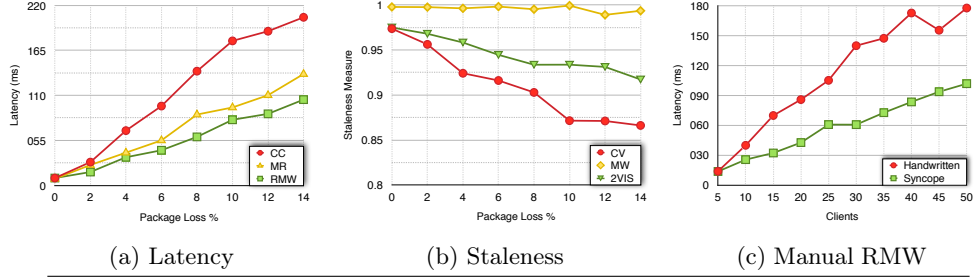


Fig. 9: A distributed application for comment section management

in the US-West (Oregon) region, with an inter-machine communication time of 5ms.

Inter-replica communication in Cassandra uses TCP connections, causing all messages to get delivered with no loss and reordering, which is in practice, far more consistent than EC, and masks out the performance gain from our fine-grained consistency guarantees. Consequently, to simulate a realistic EC environment, we injected artificial message losses in SYNCOPE’s shim layer, forcing random messages to be delayed for 1s, simulating messages losses in a network with roughly 400ms RTT.

Fig. 9(a) and 9(b) represent our experimental results, with a workload generated by 50 concurrent clients repeatedly running sessions, each composed of three operations, where operations uniformly choose from 5 objects, performed under a specified consistency level. We increase the percentage of delayed messages from 0 to 14. Each experiment ran for 100 repeated sessions per client. In addition to client perceived latency, we also measure the staleness of operations, which we define as the average ratio of the number of visible effects, to the number of all available effects, when executing an operation.

In the first set of experiments, we measure latency under three different LB contracts, all implemented in SYNCOPE. As expected, causal consistency and RMW experience respectively the highest and the lowest performance loss as the percentage of lost messages is increased<sup>7</sup>. With only a 4% percent message loss rate, we see 17% higher latency under an MR contract compared to RMW, and similarly 67% higher latency in CC compared to MR; with 10 percent message loss, the numbers are increased to 18% and 87%.

Similarly, we repeated the experiment with 3 UB contracts. Here, a *causal visibility* (CV) contract (i.e.  $\forall a.a \xrightarrow{(so \cup vis)^*; vis} \hat{a} \Rightarrow a \xrightarrow{vis} \hat{a}$ ), yields the most stale data when the percentage of lost messages is increased, whereas staleness in MW is the lowest and is barely effected. We report 3% (6%) difference between staleness of data under MW and 2VIS, and 4% (7%) difference between 2VIS and CV, at four (ten) percent message loss rate.

<sup>7</sup> In fact, they define the strongest and the weakest LB dependency relations expressible in our language:  $(\xrightarrow{so})$  and  $(\xrightarrow{(so \cup vis)^*})$

Finally, in order to provide evidence on the practicality of SYNCOPÉ, we implemented an ad-hoc mechanism to prevent the lost-updates anomaly, for a simple counter application. Fig. 9(c) shows the latency results of this application compared to the same in SYNCOPÉ, under the same setting as before (albeit with no message loss). We see 78% higher latency for the handwritten code compared to SYNCOPÉ with 50 concurrent clients. Beyond the performance numbers, we experienced many bookkeeping complications with the handwritten implementation, mainly because of the lack of meta-data queries in Cassandra which needs strongly consistent table alterations at the beginning and the end of each session.

## 8 Related Works

## 9 Conclusion

This paper presents QUELEA, a shallow Haskell extension for declarative programming over ECDS. The key idea underlying QUELEA’s design is the automatic classification of fine-grained consistency contracts on operations and distributed transactions with respect various consistency and isolation levels offered by the store. Our contract language is carefully crafted from a decidable subset of first-order logic, enabling the use of automated verification tools to discharge the proof obligations associated with contract classification. We realize an instantiation of QUELEA on top of an off-the-shelf distributed store, Cassandra, and illustrate the benefit of fine-grained contract classification by implementing and evaluating several scalable applications.

## References

1. KC Sivaramakrishnan, Gowtham Kaki, and Suresh Jagannathan. Declarative programming over eventually consistent data stores. *SIGPLAN Not.*, 50(6):413–424, June 2015.
2. Douglas B. Terry, Alan J. Demers, Karin Petersen, Mike J. Spreitzer, Marvin M. Theimer, and Brent B. Welch. Session guarantees for weakly consistent replicated data. pages 140–149, 1994.
3. Seth Gilbert and Nancy Lynch. Brewer’s conjecture and the feasibility of consistent, available, partition-tolerant web services. *SIGACT News*, 33(2):51–59, June 2002.
4. Mohsen Lesani, Christian J. Bell, and Adam Chlipala. Chapar: Certified causally consistent distributed key-value stores. *SIGPLAN Not.*, 51(1):357–370, January 2016.
5. James R. Wilcox, Doug Woos, Pavel Panchekha, Zachary Tatlock, Xi Wang, Michael D. Ernst, and Thomas Anderson. Verdi: A framework for implementing and formally verifying distributed systems. *SIGPLAN Not.*, 50(6):357–368, June 2015.
6. Peter Bailis, Ali Ghodsi, Joseph M. Hellerstein, and Ion Stoica. Bolt-on causal consistency. In *Proceedings of the 2013 ACM SIGMOD International Conference on Management of Data*, SIGMOD ’13, pages 761–772, New York, NY, USA, 2013. ACM.

7. Daniel J. Abadi. Consistency tradeoffs in modern distributed database system design: Cap is only part of the story. *IEEE Computer*, 45(2), 2012.
8. M.P. Herlihy and J.M. Wing. Linearizability: A Correctness Condition for Concurrent Objects. *ACM Transactions on Programming Languages and Systems*, 12(3):463–492, July 1990.
9. Christos H. Papadimitriou. The serializability of concurrent database updates. *J. ACM*, 26(4):631–653, 1979.
10. Avinash Lakshman and Prashant Malik. Cassandra: a decentralized structured storage system. *Operating Systems Review*, 44(2):35–40, 2010.
11. Marc Shapiro, Nuno Preguiça, Carlos Baquero, and Marek Zawirski. Conflict-free replicated data types. In *Proceedings of the 13th International Conference on Stabilization, Safety, and Security of Distributed Systems*, SSS’11, pages 386–400, Berlin, Heidelberg, 2011. Springer-Verlag.
12. Brian F. Cooper, Raghu Ramakrishnan, Utkarsh Srivastava, Adam Silberstein, Philip Bohannon, Hans-Arno Jacobsen, Nick Puz, Daniel Weaver, and Ramana Yerneni. Pnuts: Yahoo!’s hosted data serving platform. *Proc. VLDB Endow.*, 1(2):1277–1288, August 2008.
13. Giuseppe DeCandia, Deniz Hastorun, Madan Jampani, Gunavardhan Kakulapati, Avinash Lakshman, Alex Pilchin, Swaminathan Sivasubramanian, Peter Voss, and Werner Vogels. Dynamo: Amazon’s highly available key-value store. *SIGOPS Oper. Syst. Rev.*, 41(6):205–220, October 2007.
14. P. Mahajan, L. Alvisi, and M. Dahlin. Consistency, availability, convergence. Technical Report TR-11-22, Computer Science Department, University of Texas at Austin, May 2011.
15. Mustaque Ahamad, Gil Neiger, James E. Burns, Prince Kohli, and Phillip W. Hutto. Causal memory: definitions, implementation, and programming. *Distributed Computing*, 9(1):37–49, 1995.
16. Rivka Ladin, Barbara Liskov, Liuba Shrira, and Sanjay Ghemawat. Providing high availability using lazy replication. *ACM Trans. Comput. Syst.*, 10(4):360–391, November 1992.
17. Kenneth Birman, André Schiper, and Pat Stephenson. Lightweight causal and atomic group multicast. *ACM Trans. Comput. Syst.*, 9(3):272–314, August 1991.
18. Wyatt Lloyd, Michael J. Freedman, Michael Kaminsky, and David G. Andersen. Don’t settle for eventual: Scalable causal consistency for wide-area storage with cops. In *Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles*, SOSP ’11, pages 401–416, New York, NY, USA, 2011. ACM.



## A Modified Haskell Program

```

1 data Sess = Bob | Alice
2 type ID = (Sess,Int)
3 type Effect = (ID,String)
4 type State = (String,Int,Int)
5
6 read :: ID -> State -> String
7 read (sess,seq) (st,sq1,sq2) =
8   case sess of
9     Bob -> if (seq==sq1+1) then st
10            else read (sess,seq) (st,sq1,sq2)
11     Alice -> if (seq==sq2+1) then st
12              else read (sess,seq) (st,sq1,sq2)
13
14 apply :: State -> Effect -> State
15 apply (st,sq1,sq2) ((sess,seq),cm) =
16   case sess of
17     Bob -> if (sq1==seq-1)
18            then (st++cm,sq1+1,sq2)
19            else (st,sq1,sq2)
20     Alice -> if (sq2==seq-1)
21              then (st++cm,sq1,sq2+1)
22              else (st,sq1,sq2)

```

Fig. 10: Guarded Application to Prevent Lost-updates Anomaly When Serving Bob and Alice

## B Proofs

Here, we present the detailed proofs of the theorems of the paper. Let's first present a useful lemma:

**Lemma 1.** *For all relations  $R$  and execution steps:*

$$(\mathbf{E}, op_{<s, i>}) \xrightarrow{V} (\mathbf{E}', \eta)$$

*interpretatin of  $R$  under  $E$  and  $E'$  only differs considering  $\eta$ , i.e.  $a, b \neq \eta \Rightarrow (R'(a, b) \Leftrightarrow R(a, b))$*

*Proof.* We only prove  $\Rightarrow$ , the other part can be done similarly. We have the following goal and hypotheses:

$$\begin{aligned} H_0 &: (\mathbf{E}, op_{<s, i>}) \xrightarrow{V} (\mathbf{E}', \eta) \\ H_1 &: a, b \neq \eta \\ H_2 &: R'(a, b) \\ G_0 &: R(a, b) \end{aligned}$$

Now by destructing  $R$  we have the followings from new hypothesis and goal:

$$\begin{aligned} H_3 &: (\text{trunc}(R); r)'(a, b) \\ G_1 &: (\text{trunc}(R); r)(a, b) \end{aligned}$$

which can be rewritten by the definition to get that  $y$  exists s.t.

$$\begin{aligned} H_4 &: (\text{trunc}(R))'(a, y) \\ H_5 &: r'(y, b) \\ G_1 &: \exists x. (\text{trunc}(R))(a, x) \wedge (r)(x, b) \end{aligned}$$

Now we instantiate the goal with  $y$  itself and by using induction on the length of  $R$ , the first conjunct is proved, and we are left with the following:

$$\begin{aligned} H_6 &: r'(y, b) \\ G_1 &: r(y, b) \end{aligned}$$

Now by inversion on  $H_0$  we get two cases, at both of which the following can be derived. (In one case  $V$  should be replaced by  $V'$  but has no effect on the proof):

$$\begin{aligned} H_7 &: \text{vis}' = \text{vis} \cup V \times \{\eta\} \\ H_8 &: \text{so}' = \text{so}' = \text{so} \cup \{(\eta', \eta) \mid \eta' \in \mathbf{A}_{(\text{SessID}=s)}\} \end{aligned}$$

Now, because of  $H_1$  (and the fact that  $y \neq \eta$ ) it is easy to get the following from  $H_7$  and  $H_8$ :

$$\begin{aligned} H_9 &: \text{vis}(y, b) \Rightarrow \text{vis}(y, b) = \\ H_{10} &: \text{so}(y, b) \Rightarrow \text{so}(y, b) = \end{aligned}$$

Which directly prove the goal, after destructing  $r$ .

### B.1 Proof of Theorem 1

(Part i) We have the following two hypotheses and the goal:

$$\frac{H_0 : (\mathbf{E}, op_{<s, i>}) \xrightarrow{V} (\mathbf{E}', \eta) \quad H_1 : V \text{ is } \psi\text{-consistent under } \mathbf{E}}{G_0 : V \cup \{\eta\} \text{ is } \psi\text{-consistent under } \mathbf{E}'}$$

Rewriting the definition in  $G_0$  results in the following. We denote the interpretation of  $R$  under  $E'$  as  $R'$ :

$$G_1 : \forall(b \in V \cup \{\eta\}). \forall(a \in E'.A). R'(a, b) \Rightarrow a \in V \cup \{\eta\}$$

By intros we have:

$$\frac{H_2 : b \in V \cup \{\eta\} \quad H_3 : a \in E'.A \quad H_4 : R'(a, b)}{G_2 : a \in V \cup \{\eta\}}$$

by inversion on  $H_0$ , there is two cases, in case one (UB reduction) we have the following:

$$T_1 : V' \vdash (\mathbf{E}, op_{<s, i>}) \hookrightarrow (\mathbf{E}', \eta)$$

by inversion on  $T_1$  we will have the following:

$$T_2 : E'.A = E.A \cup \{\eta\}$$

Since the other case (LB reduction) also includes similar premises which yields  $T_2$ , we can add it to the hypothesis:

$$H_5 : E'.A = E.A \cup \{\eta\}$$

by rewriting  $H_5$  in  $H_3$  and by inversion, we get two cases:  $a = \eta$  and  $a \in E.A$ . The first case immediatly proves  $G_2$ , so we only consider the second case where we have:

$$H_6 : a \in E.A$$

Now, by inversion on  $H_2$ , we have two cases:

– **Case 1:**

$$b \in V$$

by inversion in  $H_1$  we have:

$$H_7 : \forall(x \in V). \forall(y \in E.A). R(y, x) \Rightarrow y \in V$$

by instantiation with a and b:

$$H_8 : R(a, b) \Rightarrow a \in V$$

Now by applying the lemma 1 on  $H_4$  we get that  $R(a, b)$  holds (since  $a, b \neq \eta$ ), which can be applied on  $H_8$  to get  $a \in V$  which proves the goal  $G_2$ .

– **Case 2:**

$$\begin{array}{l} H_9 : b = \eta \\ \text{(by rewriting } H_9 \text{ in } H_4) \quad H_{10} : R'(a, \eta) \end{array}$$

Now we use inversion on  $H_0$  and get two cases: (LB exec) and (UB exec)

– **SCase (LB exec):** we have  $H_{11}$  and  $H_{12}$  from the reduction rule premises:

$$\begin{array}{l} H_{11} : R_V^{-1}(\eta) = R_{E'.A}^{-1}(\eta) \\ H_{12} : R_V^{-1}(\eta) \subseteq V \end{array}$$

now from  $H_{10}$  we have  $H_{13}$  which can be rewritten by  $H_{11}$  to get  $H_{H14}$ :

$$\begin{aligned} H_{13} &: a \in R_{E'.A}^{-1}(\eta) \\ H_{14} &: a \in R_V^{-1}(\eta) \end{aligned}$$

The goal  $G_2$  is now proved from  $H_{12}$  and  $H_{14}$ .

– **SCase (UB exec)**: We have the following from the premises:

$$\begin{aligned} H_{15} &: V' = \lfloor V \rfloor_{\max} \\ H_{16} &: V' \subseteq V \end{aligned}$$

now destruct  $R$ , the only non-trivial cases are  $(R = \text{trunc}(R); \text{vis})$  and  $(R = \text{vis})$ :

**SSCase**  $(R = \text{trunc}(R); \text{vis})$ :

From  $H_{10}$  we get  $H_{17}$  which based on the definition, yields that there exists  $c$  such that  $H_{18}$ ,  $H_{19}$  and  $H_{20}$  hold:

$$\begin{aligned} H_{17} &: a \in (\text{trunc}(R)'; \text{vis}')_{E'.A}^{-1}(\eta) \\ H_{18} &: c \in \text{vis}'^{-1}(\eta) \\ H_{19} &: a \in \text{trunc}(R)'^{-1}(c) \\ H_{20} &: \text{vis}'^{-1}(\eta) \subseteq E'.A \end{aligned}$$

from  $H_{15}$  we have:

$$H_{21} : (\text{trunc}(R))_V^{-1}(V') \subseteq V'$$

Now from  $H_{18}$  is straightforward to get:

$$H_{22} : c \in V'$$

which after appying the lemma 1 on  $H_{19}$ , and by  $H_{21}$  yields the following, which proves the goal  $G_2$ :

$$H_{23} : a \in V'$$

**SSCase**  $(R = \text{vis})$ : From  $H_{10}$  we get that  $\text{vis}'(a, \eta)$ , which -with a similar argument to the previous subcase- yields the following and the goal is proved:

$$H_{24} : a \in V'$$

QED.

### (Part ii)

For this part we have the following hypothesis and the goal:

$$\begin{aligned} H_0 &: (\mathbf{E}, \text{op}_{<s, i>}) \xrightarrow{V} (\mathbf{E}', \eta) \\ G_0 &: E' \models [\eta/\hat{\eta}] \end{aligned}$$

By inversion on  $H_0$ , we have two cases:

**Case1** (UB exec):

$$\begin{aligned} H_1 &: r_k = \text{vis} \\ H_2 &: V \subseteq E.A \\ H_3 &: V' = \lfloor V \rfloor_{\max} \\ H_4 &: V' \vdash (\mathbf{E}, \text{op}_{<s, i>}) \hookrightarrow (\mathbf{E}', \eta) \end{aligned}$$

The goal  $G_0$  can be rewritten as:

$$G_1 : E' \models \forall a. a \xrightarrow{R} \eta \Rightarrow a \xrightarrow{\text{vis}} \eta$$

Since the  $E'.A$  gives the interpretation for the universe of quantification:

$$G_2 : \forall (a \in E'.A). E' \models a \xrightarrow{R} \eta \Rightarrow a \xrightarrow{vis} \eta$$

by intros:

$$\begin{aligned} H_5 &: a \in E'.A \\ G_3 &: E' \models a \xrightarrow{R} \eta \Rightarrow a \xrightarrow{vis} \eta \end{aligned}$$

Now since  $((\mathcal{M} \models A \Rightarrow B) \Leftrightarrow (\mathcal{M} \models A \Rightarrow \mathcal{M} \models B))$  we can rewrite  $G_3$  as:

$$G_4 : (E' \models a \xrightarrow{R} \eta) \Rightarrow (E' \models a \xrightarrow{vis} \eta)$$

intros:

$$\begin{aligned} H_6 &: E' \models a \xrightarrow{R} \eta \\ G_5 &: E' \models a \xrightarrow{vis} \eta \end{aligned}$$

Now we use the interpretation given by  $E'$ , to rewrite the relations as follows. Note that we denote the interpretation of  $R$  under  $E'$  as  $R'$  and  $E.vis$  as  $vis'$ .

$$\begin{aligned} H_7 &: R'(a, \eta) \\ G_6 &: vis'(a, \eta) \end{aligned}$$

by inversion on  $H_4$ :

$$H_8 : vis' = vis \cup V' \times \{\eta\}$$

Now since  $\eta$  is a fresh effect, we get that  $a \in V' \Rightarrow vis'(a, \eta)$  which can be applied to  $G_6$  to get the following:

$$G_7 : a \in V'$$

Now, destructing  $R$  yields multiple cases, only one of which is non-trivial:  $R = \text{trunc}(R); vis$ , which can be rewritten in  $H_7$  to get:

$$H_9 : (\text{trunc}(R); vis)'(a, \eta)$$

Now we can rewrite the definition in  $H_9$ , and derive that there exists  $b$  such that:

$$\begin{aligned} H_{10} &: \text{trunc}(R)'(a, b) \\ H_{11} &: vis'(b, \eta) \end{aligned}$$

Now using a similar argument, from  $H_8$  and  $H_{11}$  we get:

$$H_{12} : b \in V'$$

Now by applying the lemma 1 on  $H_{10}$  we get:

$$H_{13} : \text{trunc}(R)(a, b)$$

since we have  $V' \in [V]$ , we get the following:

$$H_{14} : \forall (x \in V'). (\text{trunc}(R))_{E.A}^{-1}(V') \Rightarrow x \in V'$$

which yields the following from  $H_{12}$  and  $H_{13}$ :

$$H_{15} : a \in V'$$

which proves the goal  $G_7$ .

**Case2** (LB exec):

We prove this case by induction on the length of the given relation  $R$ . We have the followings, from the premises of the reduction rule:

$$\begin{aligned} H_1 &: r_k = \text{so} \\ H_2 &: V \subseteq E.A \\ H_3 &: R_V^{-1}(\eta) = R_{E.A}^{-1}(\eta) \\ H_4 &: R_V^{-1}(\eta) \subseteq V \\ H_5 &: V \vdash (\mathbf{E}, op_{<s,i>}) \hookrightarrow (\mathbf{E}', \eta) \end{aligned}$$

Using the same argument as the previous section, we get the following new goal and hypotheses:

$$\begin{aligned} H_6 &: a \in E'.A \\ H_7 &: R'(a, \eta) \\ G_1 &: \text{vis}'(a, \eta) \end{aligned}$$

We now destruct  $R$  to get  $H_8$  from  $H_7$ , and rewrite the definition in it to get the next two hypotheses. Note that by destructing  $R$ , there are only two non-trivial cases  $R = \text{trunc}(R); \text{so}$  and  $R = \text{so}$ , which we are only considering the former, since the latter can be proved similarly.

$$\begin{aligned} H_8 &: (\text{trunc}(R); \text{so})'(a, \eta) \\ H_9 &: \text{trunc}(R)'(a, b) \\ H_{10} &: \text{so}'(b, \eta) \end{aligned}$$

Now, from the previous section we know that  $(\text{so}')^{-1}(\eta) \subseteq V$  which yields the following from  $H_{10}$ :

$$H_{11} : b \in V$$

The goal is proved by the induction hypothesis,  $H_9$  and  $H_{11}$ .

QED.

## B.2 Proof of Theorem 2

We prove the theorem by contradiction:

$$\begin{aligned} H_0 &: (\mathbf{E}, op_{<s,i>}) \xrightarrow{V} (\mathbf{E}', \eta) \\ H_1 &: a \in V \\ H_2 &: (a, \eta) \notin E'.\text{vis} \\ H_3 &: (E'.A, E'.\text{vis} \cup \{(a, \eta)\}, E'.\text{so}) \models \psi[\eta/\hat{\eta}] \\ H_4 &: (\text{trunc}(R)_V^{-1}(a) = \text{trunc}(R)_{E.A}^{-1}(a)) \\ G_0 &: \perp \end{aligned}$$

Now we call  $(E'.A, E'.\text{vis} \cup \{(a, \eta)\}, E'.\text{so})$  as  $E''$  and derive the following from  $H_3$ :

$$H_5 : E'' \models \forall x.x \xrightarrow{R} \eta \Rightarrow x \xrightarrow{\text{vis}} \eta$$

because  $E''$  defines the universe of quantification (and since  $E''.A = E'.A$ ), we get the following:

$$H_6 : \forall (x \in E'.A). E'' \models x \xrightarrow{R} \eta \Rightarrow x \xrightarrow{\text{vis}} \eta$$

and is rewritten as the following:

$$H_7 : \forall (x \in E'.A). (E'' \models x \xrightarrow{R} \eta) \Rightarrow (E'' \models x \xrightarrow{\text{vis}} \eta)$$

Now by inversion on  $H_0$  we get two cases, one of which is trivial. We skip the formal proof for it but it is easy to see that in [LB exec] case, ALL effects in  $V$  are made

visible to  $\eta$ , so the set is trivially maximal, i.e.  $H_1$  and  $H_2$  yield  $\perp$ . For the other case (UB exec), we get the following:

$$\begin{aligned} H_8 : V' &= \lfloor V \rfloor_{\max} \\ H_9 : V' &\vdash (\mathbf{E}, op_{<s, i>}) \hookrightarrow (\mathbf{E}', \eta) \end{aligned}$$

by inversion on  $H_9$  we get  $H_{10}$  and from that and from  $H_2$ , following a similar argument from the proof of theorem 1, we get  $H_{11}$ :

$$\begin{aligned} H_{10} : \mathbf{vis}' &= \mathbf{vis} \cup V' \times \{\eta\} \\ H_{11} : a &\notin V' \end{aligned}$$

Now by denoting the interpretation of  $R$  under  $E''$  as  $R''$ ,  $H_7$  can be rewritten as follows:

$$H_{12} : \forall (x \in E'.A). R''(x, \eta) \Rightarrow \mathbf{vis}''(x, \eta)$$

Now by inversion on  $H_8$ , we get the following:

$$\begin{aligned} H_{13} : V' &\in \lfloor V \rfloor \\ H_{14} : \exists V'' \in \lfloor V \rfloor. |V''| &> |V'| \\ (\text{from } H_{13}) \quad H_{15} : V' &\subseteq V \wedge (\text{trunc}(R))_V^{-1}(V') \subseteq V' \wedge \\ &(\text{trunc}(R))_V^{-1}(V') = (\text{trunc}(R))_{E.A}^{-1}(V') \end{aligned}$$

Now we can destruct  $R$ , where we get multiple cases, only two of which are non-trivial, ( $R = \mathbf{vis}$ ) and ( $R = \text{trunc}(R); \mathbf{vis}$ )

- **Case1**( $R = \mathbf{vis}$ ):  
 $\text{trunc}(R) = \mathbf{null}$ , thus  $V$  itself satisfies the requirements in  $H_{15}$  and we get that ( $V = \lfloor V \rfloor_{\max}$ ) and the following holds:

$$H_{16} : V = V'$$

which results in contradiction from  $H_1$  and  $H_{11}$ .

- **Case2**( $R = \text{trunc}(R); \mathbf{vis}$ ):  
 Since  $|V' \cup \{a\}| > |V'|$  we have the following:

$$H_{17} : (V' \cup \{a\}) \notin \lfloor V \rfloor$$

which based on the definition yields that the conditions for holding the above relation are not true, i.e.

$$\begin{aligned} H_{18} : \neg((V' \cup \{a\}) &\subseteq V \wedge (\text{trunc}(R))_V^{-1}(V' \cup \{a\}) \subseteq (V' \cup \{a\}) \wedge \\ &(\text{trunc}(R))_V^{-1}(V' \cup \{a\}) = (\text{trunc}(R))_{E.A}^{-1}(V' \cup \{a\})) \end{aligned}$$

or equally:

$$\begin{aligned} H_{19} : (V' \cup \{a\}) &\not\subseteq V \vee \\ &(\text{trunc}(R))_V^{-1}(V' \cup \{a\}) \not\subseteq (V' \cup \{a\}) \vee \\ &(\text{trunc}(R))_V^{-1}(V' \cup \{a\}) \neq (\text{trunc}(R))_{E.A}^{-1}(V' \cup \{a\}) \end{aligned}$$

By inversion on the above, we get three cases, two of which are trivial. The last conjunct can't hold because of  $H_4$  and the first one also contradicts with  $H_1$  and  $H_{15}$ . Thus, we are left with only one case:

$$H_{20} : (\text{trunc}(R))_V^{-1}(V' \cup \{a\}) \not\subseteq (V' \cup \{a\})$$

Now, from the second conjunct in  $H_{15}$  we know that it should be the case that:

$$(\text{from } H_{15} : (\text{trunc}(R))_V^{-1}(V') \subseteq V') \quad H_{21} : ((\text{trunc}(R))_V^{-1}(a) \not\subseteq (V' \cup \{a\}))$$

The above hypothesis yields the existence of  $c \neq a$  such that:

$$\begin{aligned} H_{22} &: c \in (\text{trunc}(R))_V^{-1}(a) \\ H_{23} &: c \notin V' \end{aligned}$$

Now, by rewriting  $(R = \text{trunc}(R); \text{vis})$  in  $H_{12}$  we get  $H_{24}$ , which can be rewritten again into  $H_{25}$  from the definition:

$$\begin{aligned} H_{24} &: \forall(x \in E'.A).((\text{trunc}(R); \text{vis})''(x, \eta) \Rightarrow \text{vis}''(x, \eta)) \\ H_{25} &: \forall(x \in E'.A).(\exists b. \text{trunc}(R)''(x, b) \wedge \\ &\quad \text{vis}''(b, \eta) \Rightarrow \text{vis}''(x, \eta)) \end{aligned}$$

Now, we instantiate  $H_{25}$  with  $x = c$ :

$$H_{26} : \exists b. \text{trunc}(R)''(c, b) \wedge \text{vis}''(b, \eta) \Rightarrow \text{vis}''(c, \eta)$$

we can replace  $\text{trunc}(R)''$  with  $\text{trunc}(R)'$  in above definition, since from  $H_3$ , the only difference in interpretation under  $E'$  and  $E''$  is the extra element  $(a, \eta)$  in  $E''.\text{vis}$  which does not effect  $\text{trunc}(R)''(c, b)$ :

$$H_{27} : \exists b. \text{trunc}(R)'(c, b) \wedge \text{vis}''(b, \eta) \Rightarrow \text{vis}''(c, \eta)$$

Moreover, since  $c \neq a$ , we can replace  $\text{vis}''(c, \eta)$  with  $\text{vis}'(c, \eta)$ :

$$H_{28} : \exists b. \text{trunc}(R)'(c, b) \wedge \text{vis}''(b, \eta) \Rightarrow \text{vis}'(c, \eta)$$

From  $H_{15}$  and  $H_{22}$  we get  $H_{29}$ , and  $H_{30}$  also holds trivially from  $H_3$ :

$$\begin{aligned} H_{29} &: \text{trunc}(R)'(c, a) \\ H_{30} &: \text{vis}''(a, \eta) \end{aligned}$$

which can be used in instantiation of  $H_{28}$  with  $b = a$  and derive the following:

$$H_{31} : \text{vis}'(c, \eta)$$

However, we know -from the previously explained argument- that  $H_{31}$  results in  $H_{32}$ , which results in contradiction with  $H_{23}$ .

$$H_{32} : c \in V'$$

QED.

### B.3 Proof of Theorem 3

Before proving the theorem, we first present and prove a useful lemma and then we will present a new definition, regarding sets of effects.

---

**Lemma 2.** *Under an execution state  $E$  and for a given set  $S \subseteq E.A$ , if  $S$  is  $\psi$ -consistent under  $E$ , then  $\forall(x \in S).R_S^{-1}(x) \subseteq S$  under  $E$ .*

*Proof.*

$$\begin{aligned} H_0 &: \text{Sis}\psi\text{-consistent} \\ G_0 &: \forall(x \in S).R_S^{-1}(x) \subseteq S \end{aligned}$$

after intros:

$$\begin{aligned} H_1 &: x \in S \\ G_1 &: R_S^{-1}(x) \subseteq S \end{aligned}$$



inversion on  $H_0$  gives the following:

$$H_2 : \forall(\eta \in S). \forall(a \in E.A). R(a, \eta) \Rightarrow a \in S$$

which can be rewritten to:

$$H_3 : \forall(\eta \in S). R^{-1}(\eta) \subseteq S$$

however, since  $S \subseteq E.A$  then<sup>8</sup>:

$$H_4 : \forall(a \in E.A). R_S^{-1}(a) \subseteq R^{-1}(a)$$

Now we can instantiate  $H_3$  and  $H_4$  into:

$$\begin{aligned} H_5 : R^{-1}(x) &\subseteq S \\ H_6 : R_S^{-1}(x) &\subseteq R^{-1}(x) \end{aligned}$$

which trivially yields  $G_1$  and the proof is completed.

QED.

**Definition 1.** We define the complement of a given set of effects  $S$  (under an execution state  $E$ ) as the super set of  $S$ , containing ALL the mid-level effects required to determine ALL the dependencies of the effects in  $S$ , i.e.

$$S' \in [S] \iff R_{S'}^{-1}(S) = R_{E.A}^{-1}(S)$$

Now, using the above theorem and lemma, we present the proof of the theorem 3, which starts by listing the following hypotheses and the goal:

$$\begin{aligned} H_0 : S &\vdash (\mathbf{E}, op_{<s,i>}) \hookrightarrow (\mathbf{E}', \eta) \\ H_1 : S \cup \{\eta\} &\text{ is } \psi\text{-consistent} \\ G_0 : \exists E'' . \exists \eta' . \exists V . ((\mathbf{E}, op_{<s,i>}) &\xrightarrow{V} (\mathbf{E}'', \eta')) \end{aligned}$$

Now, by destructing  $R$  we get two non-trivial cases:

– **Case1**( $R = \text{trunc}(R); \text{vis}$ ):

In this case<sup>9</sup>, we generate the premises of the  $[\text{UB EXEC}]$  to achieve the goal as follows. Firstly, we define  $S'$  and present  $\eta'$ :

$$\begin{aligned} H_3 : S' &= \lfloor S \rfloor_{\max} \\ H_4 : \eta' &= (s, op, F_{op}(S')) \end{aligned}$$

Moreover, we will define the followings, which will be used when presenting  $E''$ :

$$\begin{aligned} H_5 : \text{so}'' &= \text{so} \cup A_{(\text{sessID}=s)} \times \{\eta'\} \\ H_6 : \text{vis}'' &= \text{vis} \cup S' \times \{\eta'\} \\ H_7 : A'' &= E.A \cup \{\eta'\} \end{aligned}$$

Now we present  $V$  and  $E''$  as follows and rewrite the goal:

$$\begin{aligned} H_8 : V &= S \\ H_9 : E'' &= (A'', \text{so}'', \text{vis}'') \\ G_1 : (\mathbf{E}, op_{<s,i>}) &\xrightarrow{V} (\mathbf{E}'', \eta') \end{aligned}$$

<sup>8</sup> we skip the formal proof of this claim, however, since the only difference in the definitions of  $R^{-1}$  and  $R_S^{-1}$  is the extra requirement about mid-level effects in the latter, it should be a subset of the former.

<sup>9</sup> Note that in this case the goal  $G_0$ , trivially holds. That is because the contract in this case is  $[\text{UB}]$ , which represents executions without blocking or waiting, that can always make progress by showing *some* set of effects to the operations

by applying [UB EXEC] on  $G_1$  we get the following new goals (after rewriting  $H_9$  and  $H_3$ ):

$$\begin{aligned} G_2 &: r_k = \text{vis} \\ G_3 &: S \subseteq E.A \\ G_4 &: S' = \lfloor S \rfloor \\ G_5 &: S' \vdash (\mathbf{E}, op_{<s,i>}) \hookrightarrow (\mathbf{E}'', \eta') \end{aligned}$$

first three goals are proved via the assumptions, and the last one can be easily shown to hold by applying [OPER] and deriving the following new goals:

$$\begin{aligned} G_6 &: S' \subseteq E.A \\ G_7 &: F_{op}(S') = v \\ G_8 &: \eta' = (s, op, v) \\ G_9 &: \eta \notin S' \\ G_{10} &: E''.A = E.A \cup \{\eta'\} \\ G_{11} &: E''.\text{vis} = E.\text{vis} \cup S' \times \{\eta\} \\ G_{12} &: E''.\text{so} = E.\text{so} \cup (A_{(\text{sessID}=s)}) \times \{\eta\} \end{aligned}$$

all the above goals have already been shown in the assumptions and the case is proved.

– **Case2**( $R = \text{trunc}(R); \text{so}$ ):

Similarly in this case we define the following:

$$H_{13} : V = \lceil S \cup \{\eta\} \rceil$$

which yields:

$$H_{14} : \forall (x \in S \cup \{\eta\}). R_V^{-1}(x) = R_{E'.A}^{-1}(x)$$

and also:

$$H_{15} : R_V^{-1}(\eta) = R_{E'.A}^{-1}(\eta)$$

Similar to the previous case, we now define the followings:

$$\begin{aligned} H_{16} &: \eta' = (s, op, F_{op}(V)) \\ H_{17} &: \text{so}'' = \text{so} \cup A_{(\text{sessID}=s)} \times \{\eta'\} \\ H_{18} &: \text{vis}'' = \text{vis} \cup V \times \{\eta'\} \end{aligned}$$

Now we present  $E''$  as follows and rewrite the goal:

$$\begin{aligned} H_{19} &: E'' = (A'', \text{so}'', \text{vis}'') \\ G_1 &: (\mathbf{E}, op_{<s,i>}) \xrightarrow{V} (\mathbf{E}'', \eta') \end{aligned}$$

by applying [LB EXEC] on  $G_1$  we get the following new goals

$$\begin{aligned} G_2 &: r_k = \text{so} \\ G_3 &: V \subseteq E.A \\ G_4 &: R_V^{-1}(\eta') = R_{E''.A}^{-1}(\eta') \\ G_5 &: R_V^{-1}(\eta') \subseteq V \\ G_6 &: V \vdash (\mathbf{E}, op_{<s,i>}) \hookrightarrow (\mathbf{E}'', \eta') \end{aligned}$$

Now,  $G_2$  and  $G_3$  are trivially proved from the assumptions, and  $G_6$  also can be easily proved following the argument from the previous case. We prove  $G_4$  and  $G_5$ , by a new claim that  $R_{E'.A}^{-1}(\eta) = R_{E''.A}^{-1}(\eta')$  which will be proved separately. Thus, we can rewrite the goals and add the new claim:

$$\begin{aligned} G_7 &: R^{-1}(\eta) = R_{E'.A}^{-1}(\eta) \\ G_8 &: R^{-1}(\eta) \subseteq V \\ G_9 &: R_{E'.A}^{-1}(\eta) = R_{E''.A}^{-1}(\eta') \end{aligned}$$

Now  $G_7$  is equal to the assumption  $H_{15}$ , and  $G_8$  is the direct result of applying the lemma 2 on  $H_1$ . Now by rewriting  $R = \text{trunc}(R); \text{so}$  in  $G_9$  we have the following:

$$G_{10} : (\text{trunc}(R); \text{so})_{E'.A}^{-1}(\eta) = (\text{trunc}(R); \text{so})_{E''.A}^{-1}(\eta')$$

Now, note that the only difference in  $E'$  and  $E''$  is in how the update the vis relation from  $E$ , the former makes the set  $S$  visible to the operation and the latter the set  $[S \cup \{\eta\}]$ . Now since the given relation  $R$  ends with an **so** relation, it is straightforward to show that  $G_{10}$  holds and thus the case (and the theorem) is proved.

QED.