Abstraction for Concurrent Objects*

Ivana Filipović, Peter O'Hearn, Noam Rinetzky, and Hongseok Yang

Queen Mary, University of London, UK

Abstract. Concurrent data structures are usually designed to satisfy correctness conditions such as sequential consistency and linearizability. In this paper, we consider the following fundamental question: what guarantees are provided by these conditions for client application programs? We formally show that these conditions can be *characterized* in terms of observational refinement. Our study also provides a new understanding of sequential consistency and linearizability in terms of the abstraction of dependency between computation steps of client programs.

1 Introduction

The design and implementation of correct efficient concurrent programs is a challenging problem. Thus, it is not surprising that programmers prefer to develop concurrent software mainly by utilizing highly-optimized concurrent data structures that have been implemented by experts.

Unfortunately, there is a gap in our theoretical understanding, which can have a serious consequence on the correctness of client programs of those concurrent data structures. Usually, programmers expect that the behavior of their program does not change whether they use experts' data structures or less-optimized but obviously-correct data structures. In the programming language community, this expectation has been formalized as observational refinement [4, 8, 11]. On the other hand, concurrent data structures are designed with different correctness conditions proposed by the concurrent-algorithm community, such as *sequential consistency* [9] and *linearizability* [6]. Can these correctness conditions meet programmers' expectation? In other words, what are the relationships between these conditions and observational refinement? As far as we know, no systematic studies have been done to answer this question.

The goal of this paper is to close the aforementioned gap. We show that (1) linearizability coincides with observational refinement, and (2) as long as the threads are non-interfering (except through experts' concurrent data structures), sequential consistency is equivalent to observational refinement. Our results pinpoint when it is possible to replace a concurrent data structure by another sequentially consistent or linearizable data structure in (client) programs, while preserving observable properties of the programs. One part of this connection (e.g., that linearizability implies observational refinement) has been a folklore among the concurrent-algorithm researchers, and our

* We would like to thank anonymous referees, Viktor Vafeiadis and Matthew Parkinson for useful comments. This work was supported by EPSRC.

results provide the first formal confirmation of this folklore. On the other hand, we believe that the other part (e.g., that observational refinement implies linearizability) is a new result that has not been conceived even informally.

Programs, Object Systems, and Histories. A concurrent data structure provides a set of procedures, which may be invoked by concurrently executing threads of the client program using the data structure. Thus, procedure invocations may overlap. (In our setting, a data structure can neither create threads nor call to a procedure of the client.) We refer to a collection of concurrent data structures as an *object system*.

In this paper, we are not interested in the implementation of an object system; we are only interested in the possible interactions between the client program and the object system. Thus, we assume that an object system is represented by a set of *histories*. Every history records a possible interaction between the client application program and the object system. The interaction is given in the form of sequences of procedure invocations made by the client and the responses which it receives. A program can use an object system only by interacting with it according to one of the object system's histories.

Example 1. The history $H_0 = (t_1, \mathit{call}\ q.enq(1)); (t_1, ret()\ q.enq); (t_2, \mathit{call}\ q.deq()); (t_2, ret(1)\ q.deq)$ records an interaction in which thread t_1 enqueues 1 into queue q followed by a dequeue by thread t_2. The histories

$$H_1 = (t_1, \mathit{call}\ q.enq(1))(t_1, ret()\ q.enq)(t_2, \mathit{call}\ q.enq(2))(t_2, ret()\ q.enq)$$
$$H_2 = (t_2, \mathit{call}\ q.enq(2))(t_2, ret()\ q.enq)(t_1, \mathit{call}\ q.enq(1))(t_1, ret()\ q.enq)$$
$$H_3 = (t_1, \mathit{call}\ q.enq(1))(t_2, \mathit{call}\ q.enq(2))(t_1, ret()\ q.enq)(t_2, ret()\ q.enq)$$

record interactions in which thread t_1 enqueues 1 into the queue and thread t_2 enqueues 2. In H_1, the invocation made by t_1 happens before that of t_2 (i.e., t_1 gets a response before t_2 invokes its own procedure). In H_2, it is the other way around. In H_3, the two invocations overlap.

Sequential Consistency and Linearizability. Informally, an object system OS_C is *sequentially consistent* wrt. an object system OS_A if for every history H_C in OS_C, there exists a history H_A in OS_A that is just another interleaving of threads' actions in H_C: in both H_C and H_A, the same threads invoke the same sequences of operations (i.e., procedure invocations) and receive the same sequences of responses. We say that such H_C and H_A are *weakly equivalent*. (We use the term *weak* equivalence to emphasis that the only relation between H_C and H_A is that they are different interleavings of the same sequential threads.) OS_C is *linearizable* wrt. OS_A, if for every history H_C in OS_C, there is some H_A in OS_A such that (1) H_C and H_A are weakly equivalent and (2) the global order of non-overlapping invocations of H_C is preserved in H_A.[1] In the context of this paper, the main difference between sequential consistency and

[1] It is common to require that OS_A be comprised of sequential histories, i.e., ones in which invocations do not overlap. (In this setting, linearizability intuitively means that every operation appears to happen atomically between its invocation and its response.) However, this requirement is not essential for our results.

linearizability is, intuitively, that the former preserves only the happens-before relation between operations of the *same* thread while the latter preserves this relation between the operations of *all* threads.

Example 2. The histories H_1, H_2, and H_3 are weakly equivalent. None of them is weakly equivalent to H_0. The history H_3 is linearizable wrt. H_1 as well as H_2, because H_3 does not have non-overlapping invocations. On the other hand, H_1 is not linearizable with respect to H_2; in H_1, the enqueue of t_1 is completed before that of t_2 even starts, but this global order on these two enqueues is reversed in H_2.

Observational Refinement. Our notion of observational refinement is based on observing the initial and final values of variables of the client program. (One can think of the program as having a final command "print all variables".) We say that an object system OS_C observationally refines an object system OS_A if every program P with OS_A, replacing OS_A by OS_C does not generate new behaviors: for every initial state s, the execution of P with OS_C at s produces only those output states that can already be obtained by running P with OS_A at s.

The main results of this paper is the following characterization of sequential consistency and linearizability in terms of observational refinement:

1. OS_C observationally refines OS_A iff OS_C is sequential consistent with respect to OS_A, assuming client operations (e.g., assignments to variables) of each thread access thread-local variables (or resources) only.
2. OS_C observationally refines OS_A iff OS_C is linearizable with respect to OS_A, assuming that client operations may use at least one shared global variable.

We start the paper by defining a programming language and giving its semantics together with the formal definition of observational refinement (Sections 2, 3, 4 and 5). Then, we describe a generic technique for proving observational refinement in Section 6, and use this technique to prove the connection between observational refinement and linearizability or sequential consistency in Section 7. The next section revisits the definitions of sequential consistency and linearizability, and provides the analysis of them in terms of the dependency between computation steps. Finally, we conclude the paper in Section 9.

2 Programming Language

We assume that we are given a fixed collection O of objects, with method calls $o.f(n)$. For simplicity, all methods will take one integer argument and return an integer value. We will denote method calls by $x{:=}o.f(e)$.

The syntax of sequential commands C and complete programs P is given below:

$$C \ ::= \ \mathtt{c} \mid x{:=}o.f(e) \mid C;C \mid C + C \mid C^\star \qquad\qquad P \ ::= \ C_1 \parallel \cdots \parallel C_n$$

Here, $\mathtt{c}$ ranges over an unspecified collection PComm of primitive commands, $+$ is nondeterministic choice, ; is sequential composition, and $(\cdot)^\star$ is Kleene-star (iterated ;). We use $+$ and $(\cdot)^\star$ instead of conditionals and while loops for theoretical simplicity:

given appropriate primitive actions the conditionals and loops can be encoded. In this paper, we assume that the primitive commands include assume statements $\texttt{assume}(b)$ and assignments $x{:=}e$ not involving method calls.[2]

3 Action Trace Model

Following Brookes [2], we will define the semantics of our language in two stages. In the first there will be a trace model, where the traces are built from atomic actions. This model resolves all concurrency by interleaving. In the second stage, which is shown in Section 5, we will define the evaluation of these action traces with initial states.

Definition 1. *An* **atomic action** *(in short, action) φ is a client operation or a call or return action: $\varphi ::= (t, a) \mid (t, \mathit{call}\, o.f(n)) \mid (t, \mathit{ret}(n)\, o.f)$. Here, t is a thread-id (i.e., a natural number), a in (t, a) is an atomic client operation taken from an unspecified set Cop_t (parameterized by the thread-id t), and n is an integer. An* **action trace** *(in short, trace) τ is a finite sequential composition of actions (i.e., $\tau ::= \varphi; \cdots; \varphi$).*

We identify a special class of traces where calls to object methods run sequentially.

Definition 2. *A trace τ is* **sequential** *when all calls in τ are immediately followed by matching returns, that is, τ belongs to the set*

$$\Big(\bigcup_{t,a,o,f,n,m} \{\, (t,a),\quad (t, \mathit{call}\, o.f(n)); (t, \mathit{ret}(m)\, o.f) \,\}\Big)^* \Big(\bigcup_{t,o,f,n} \{\, \epsilon,\quad (t, \mathit{call}\, o.f(n)) \,\}\Big).$$

Intuitively, the sequentiality means that all method calls to objects run atomically. Note that the sequentiality also ensures that method calls and returns are properly matched (possibly except the last call), so that, for instance, no sequential traces start with a return action, such as $(t, \mathit{ret}(3)\, o.f)$.

The execution of a program in this paper generates only well-formed traces.

Definition 3. *A trace τ is* **well-formed** *iff for all thread-ids t, the projection of τ to the t-thread, $\tau|_t$, is sequential.*

The well-formedness formalizes two properties of traces. Firstly, it ensures that all the returns should have corresponding method calls. Secondly, it formalizes the intuition that each thread is a sequential program, if it is considered in isolation. Thus, when the thread calls a method $o.f$, it has to wait until the method returns, before doing anything else. We denote the set of all well-formed traces by $WTraces$.

Our trace model $T(-)$ defines the meaning of sequential commands and programs in terms of traces, and it is shown in Figure 1. In our model, a sequential command C means a set $T(C)t$ of well-formed traces, which is parametrized by the id t of a thread running the command. The semantics of a complete program (a parallel composition) P, on the other hand, is a non-parametrized set $T(P)$ of well-formed traces; instead of taking thread-ids as parameters, $T(P)$ creates thread-ids.

[2] The $\texttt{assume}(b)$ statement acts as skip when the input state satisfies b. If b does not hold in the input state, the statement deadlocks and does not produce any output states.

$$T(\mathtt{c})t = \{\ (t,a_1);(t,a_2);\ldots;(t,a_k)\ \mid\ a_1;a_2;\ldots;a_k \in [\![\mathtt{c}]\!]_t\ \}$$

$$T(x{:=}o.f(e))t = \{\ \tau;(t,\mathit{call}\ o.f(n));(t,\mathit{ret}(n')\ o.f);\tau'\ \mid\ n,n' \in \mathit{Integers}\ \wedge\ \tau \in T(\mathtt{assume}(e{=}n))t\ \wedge\ \tau' \in T(x{:=}n')t\ \}$$

$$T(C_1;C_2)t = \{\,\tau_1;\tau_2 \mid \tau_i \in T(C_i)t\,\} \quad T(C_1{+}C_2)t = T(C_1)t \cup T(C_2)t \quad T(C^\star)t = (T(C)t)^\star$$

$$T(C_1 \parallel \cdots \parallel C_n) \ = \ \bigcup\{\ \ \mathit{interleave}(\tau_1,\ldots,\tau_n)\ \ \mid\ \ \tau_i \in T(C_i)i\ \wedge\ 1 \le i \le n\ \ \}$$

Fig. 1. Action Trace Model. Here $\tau \in \mathit{interleave}(\tau_1,\ldots,\tau_n)$ iff every action in τ is done by a thread $1 \le i \le n$ and $\tau|_i = \tau_i$ for every such thread i.

Two cases of our semantics are slightly unusual and need further explanations. The first case is the primitive commands $\mathtt{c}$. In this case, the semantics assumes that we are given an interpretation $[\![\mathtt{c}]\!]_t$ of $\mathtt{c}$, where $\mathtt{c}$ means finite sequences of atomic client operations (i.e., $[\![\mathtt{c}]\!]_t \subseteq \mathit{Cop}_t^+$). By allowing sequences of length 2 or more, this assumed interpretation allows the possibility that $\mathtt{c}$ is not atomic, but implemented by a sequence of atomic operations. The second case is method calls. Here the semantics distinguishes calls and returns to objects, to be able to account for concurrency (overlapping operations). Given $x{:=}o.f(e)$, the semantics non-deterministically chooses two integers n, n', and uses them to describe a call with input n and a return with result n'. In order to ensure that the argument e evaluates to n, the semantics inserts the assume statement $\mathtt{assume}(e{=}n)$ before the call action, and to ensure that x gets the return value n', it adds the assignment $x{:=}n'$ after the return action. Note that some of the choices here might not be feasible; for instance, the chosen n may not be the value of the parameter expression e when the call action is invoked, or the concurrent object never returns n' when called with n. The next evaluation stage of our semantics will filter out all these infeasible call/return pairs.

Lemma 1. *For all sequential commands C, programs P and thread-ids t, both $T(C)t$ and $T(P)$ contain only well-formed traces.*

4 Object Systems

The semantics of objects is given using histories, which are sequences of calls and returns to objects. We first define precisely what the individual elements in the histories are.

Definition 4. *An* **object action** *is a call or return: $\psi ::= (t, \mathit{call}\ o.f(n)) \mid (t, \mathit{ret}(n)\ o.f)$. A* **history** *$H$ is a finite sequence of object actions (i.e., $H ::= \psi;\psi;\ldots;\psi$). If a history H is well-formed when viewed as a trace, we say that H is* **well-formed**.

Note that in contrast to traces, histories do not include atomic client operations (t, a). We will use $\mathcal{A}$ for the set of all actions, $\mathcal{A}_o$ for the set of all object actions, and $\mathcal{A}_c$ for $\mathcal{A} - \mathcal{A}_o$, i.e., the set of all client operations.

We follow Herlihy and Wing's approach [6], and define object systems.

Definition 5. *An* **object system** OS *is a set of well-formed histories.*

Notice that OS is a collective notion, defined for all objects together rather than for them independently. Sometimes, the traces of a system satisfy special properties.

Definition 6. *Let OS be an object system. We say that*

- OS *is* **sequential** *iff it contains only sequential traces;*
- OS *is* **local** *iff for any well-formed history H, $H \in OS \iff (\forall o.\, H|_o \in OS)$.*

A local object system is one in which the set of histories for all the objects together is determined by the set of histories for each object individually. Intuitively, locality means that objects can be specified in isolation. Sequential and local object systems are commonly used as specifications for concurrent objects in the work on concurrent algorithms. (See, e.g., [5]).

5 Semantics of Programs

We move on to the second stage of our semantics, which defines the evaluation of traces. Suppose we are given a trace τ and an initial state s, which is a function from variables $x, y, z, \ldots$ to integers.[3] The second stage is the evaluation of the trace τ with s, and it is formally described by the evaluation function eval below:

$$\begin{array}{c} \mathsf{eval} \;:\; States \times WTraces \to \mathcal{P}(States) \\ \mathsf{eval}(s, (t, call\, o.f(n)); \tau) = \mathsf{eval}(s, \tau) \qquad \mathsf{eval}(s, (t, ret(n)\, o.f); \tau) = \mathsf{eval}(s, \tau) \\ \mathsf{eval}(s, (t, a); \tau) = \bigcup_{(s,s') \in [\![a]\!]} \mathsf{eval}(s', \tau) \qquad \mathsf{eval}(s, \epsilon) = \{s\} \end{array}$$

The semantic clause for atomic client operations (t, a) assumes that we already have an interpretation $[\![a]\!]$ where a means a binary relation on $States$. Note that a state s does not change during method calls and returns. This is because firstly, in the evaluation map, a state describes the values of client variables only, not the internal status of objects and secondly, the assignment of a return value n to a variable x in $x{:=}o.f(e)$ is handled by a separate client operation; see the definition of $T(x{:=}o.f(e))$ in Figure 1.

Now we combine the two stages, and give the semantics of programs P. Given a specific object system OS, the formal semantics $[\![P]\!](OS)$ is defined as follows:

$$\begin{array}{rcl} [\![P]\!](OS) & : & States \to \mathcal{P}(States) \\ [\![P]\!](OS)(s) & = & \bigcup \{\, \mathsf{eval}(s, \tau) \;\mid\; \tau \in T(P) \wedge \mathsf{getHistory}(\tau) \in OS \,\} \end{array}$$

Here $\mathsf{getHistory}(\tau)$ is the projection of τ to object actions. The semantics first calculates all traces $T(P)$ for τ, and then selects only those traces whose interactions with objects can be implemented by OS. Finally, the semantics runs all the selected traces with the initial state s.

Our semantics observes the initial and final values of variables in threads, and ignores the object histories. One can think of the program as having a final command "print all variables", which gives us our observable. We use this notion of observation and compare two different object systems OS_A and OS_C.

[3] All the results of the paper except the completeness can be developed without assuming any specific form of s. Here we do not take this general approach, to avoid being too abstract.

Definition 7. *Let OS_A and OS_C be object systems. We say that*

- OS_C **observationally refines** $OS_A \iff \forall P, s.\, [\![P]\!](OS_C)(s) \subseteq [\![P]\!](OS_A)(s)$;
- OS_C *is* **observationally equivalent** *to* $OS_A \iff \forall P.\, [\![P]\!](OS_C) = [\![P]\!](OS_A)$.

Usually, OS_A is a sequential local object system that serves as a specification, and OS_C is a concurrent object system representing the implementation. The observational refinement means that we can replace OS_A by OS_C in any programs without introducing new behaviors of those programs, and gives a sense that OS_C is a correct implementation of OS_A.

In the remainder of this paper, we will focus on answering the question: how do correctness conditions on concurrent objects, such as linearizability, relate to observational refinements?

6 Simulation Relations on Histories

We start by describing a general method for proving observational refinements. Later in Section 7, we will show that both linearizability and sequential consistency can be understood as specific instances of this method.

Roughly speaking, our method works as follows. Suppose that we want to prove that OS_C observationally refines OS_A. According to our method, we first need to choose a binary relation $\mathcal{R}$ on histories. This relation has to be a *simulation*, i.e., a relation that satisfies a specific requirement, which we will describe shortly. Next, we should prove that every history H in OS_C is $\mathcal{R}$-related to some history H' in OS_A. Once we finish both steps, the soundness theorem of our method lets us infer that OS_C is an observational refinement of OS_A.

The key part of the method, of course, lies in the requirement that the chosen binary relation $\mathcal{R}$ be a simulation. If we were allowed to use any relation for $\mathcal{R}$, we could pick the relation that relates all two histories, and this would lead to the incorrect conclusion that every OS_C observationally refines OS_A, as long as OS_A is nonempty.

To describe our requirement on $\mathcal{R}$ and its consequence precisely, we need to formalize the dependency between actions in a single trace and define trace equivalence based on this formalization.

Definition 8 (Independent Actions). *An action φ* **is independent of** *an action φ', denoted $\varphi \# \varphi'$, iff (1) $\mathsf{getTid}(\varphi) \neq \mathsf{getTid}(\varphi')$ and (2) for all $s \in States$, $\mathsf{eval}(s, \varphi\varphi') = \mathsf{eval}(s, \varphi'\varphi)$. Here, $\mathsf{getTid}(\varphi)$ is the thread-id (i.e., the first component) of φ.*

Definition 9 (Dependency Relations). *For each trace τ, we define the* **immediate dependency relation** $<_\tau$ *to be the following relation on actions in τ:*[4]

$$\tau_i <_\tau \tau_j \iff i < j \wedge \neg(\tau_i \# \tau_j).$$

The **dependency relation** $<_\tau^+$ *on τ is the transitive closure of $<_\tau$.*

[4] Strictly speaking, $<_\tau$ is a relation on the indices $\{1, \ldots, |\tau|\}$ of τ so that we should have written $i <_\tau j$. In this paper, we use a rather informal notation $\tau_i <_\tau \tau_j$ instead, since we found this notation easier to understand.

Definition 10 (Trace Equivalence). *Traces τ, τ' are* **equivalent***, denoted $\tau \sim \tau'$, iff there exists a bijection $\pi : \{1, \ldots, |\tau|\} \to \{1, \ldots, |\tau'|\}$ such that*

$$(\forall i.\ \tau_i = \tau'_{\pi(i)}) \ \wedge \ (\forall i, j.\ \tau_i <^+_\tau \tau_j \iff \tau'_{\pi(i)} <^+_{\tau'} \tau'_{\pi(j)}).$$

Intuitively, $\tau \sim \tau'$ means that τ' can be obtained by swapping independent actions in τ. Since we swap only independent actions, we expect that τ' and τ essentially mean the same computation. The lemma below justifies this expectation, by showing that our semantics cannot observe the difference between equivalent traces.

Lemma 2. *For all well-formed traces τ, τ', if $\tau \sim \tau'$, we have that*

$$(\forall P.\ \tau \in T(P) \iff \tau' \in T(P)) \ \wedge \ (\forall s.\ \mathsf{eval}(s, \tau) = \mathsf{eval}(s, \tau')).$$

We are now ready to give the definition of simulation, which encapsulates our requirement on relations on histories, and to prove the soundness of our proof method based on simulation.

Definition 11 (Simulation). *A binary relation $\mathcal{R}$ on histories is a* **simulation** *iff for all well-formed histories H and H' such that $(H, H') \in \mathcal{R}$,*

$$\forall \tau \in \mathit{WTraces}.\ \mathsf{getHistory}(\tau) = H \implies \exists \tau' \in \mathit{WTraces}.\ \tau \sim \tau' \wedge \mathsf{getHistory}(\tau') = H'.$$

One way to understand this definition is to read a history H as a representation of the trace set $\mathsf{means}(H) = \{\tau \in \mathit{WTraces} \mid \mathsf{getHistory}(\tau) = H\}$. Intuitively, this set consists of the well-formed traces whose interactions with objects are precisely H. According to this reading, the requirement in the definition of simulation simply means that $\mathsf{means}(H)$ is a subset of $\mathsf{means}(H')$ modulo trace equivalence $\sim$. For every relation $\mathcal{R}$ on histories, we define its lifting to a relation $\lhd_{\mathcal{R}}$ on object systems by

$$\mathit{OS}_C \lhd_{\mathcal{R}} \mathit{OS}_A \iff \forall H \in \mathit{OS}_C.\ \exists H' \in \mathit{OS}_A.\ (H, H') \in \mathcal{R}.$$

Theorem 1. *If $\mathit{OS}_C \lhd_{\mathcal{R}} \mathit{OS}_A$ and $\mathcal{R}$ is a simulation, OS_C observationally refines OS_A.*

Proof. Consider a program P and states s, s' such that $s' \in [\![P]\!](\mathit{OS}_C)(s)$. Then, by the definition of $[\![P]\!]$, there exist a well-formed trace $\tau \in T(P)$ and a history $H \in \mathit{OS}_C$ such that $\mathsf{getHistory}(\tau) = H$ and $s' \in \mathsf{eval}(s, \tau)$. Since $H \in \mathit{OS}_C$ and $\mathit{OS}_C \lhd_{\mathcal{R}} \mathit{OS}_A$ by our assumption, there exists $H' \in \mathit{OS}_A$ with $(H, H') \in \mathcal{R}$. Furthermore, H and H' are well-formed, because object systems contain only well-formed histories. Now, since $\mathcal{R}$ is a simulation, τ is well-formed and $\mathsf{getHistory}(\tau) = H$, there exists a well-formed trace τ' such that (1) $\tau \sim \tau'$ and (2) $\mathsf{getHistory}(\tau') = H'$. Note that because of Lemma 2, the first conjunct here implies that $\tau' \in T(P)$ and $s' \in \mathsf{eval}(s, \tau')$. This and the second conjunct $\mathsf{getHistory}(\tau') = H'$ together imply the desired $s' \in [\![P]\!](\mathit{OS}_A)(s)$. □

7 Sequential Consistency, Linearizability and Refinement

Now we explain the first two main results of this paper:

1. Linearizability implies observational refinement.

2. Sequential consistency implies observational refinement if client operations of each thread access thread-local variables (or resources) only.

It is not difficult to obtain high-level understanding about why our results hold. Both linearizability and sequential consistency define certain relationships between two object systems, one of which is normally assumed sequential and local. Interestingly, in both cases, we can prove that these relationships are generated by lifting some *simulation* relations. From this observation follow our results, because Theorem 1 says that all such simulation-generated relationships on object systems imply observational refinements.

In the rest of this section, we will spell out the details of the high-level proof sketches just given. For this, we need to review the relations on histories used by sequential consistency and linearizability [6].

Definition 12 (Weakly Equivalent Histories). *Two histories are* **weakly equivalent***, denoted $H \equiv H'$, iff their projections to threads are equal.*[5]

$$H \equiv H' \iff \forall t.\ H|_t = H'|_t.$$

As its name indicates, the weak equivalence is indeed a weak notion. It only says that the two traces are both interleavings of the same sequential threads (but they could be different interleavings).

Definition 13 (Happen-Before Order). *For each history H, the* **happen-before order** *$\prec_H$ is a binary relation on object actions in H defined by*

$$\begin{aligned} H_i \prec_H H_j \iff \exists i', j'.\ & i \le i' < j' \le j \ \wedge \\ & \mathsf{getTid}(H_i) = \mathsf{getTid}(H_{i'}) \ \wedge\ \mathsf{getTid}(H_{j'}) = \mathsf{getTid}(H_j) \ \wedge \\ & \mathsf{retAct}(H_{i'}) \ \wedge\ \mathsf{callAct}(H_{j'}). \end{aligned}$$

Here $\mathsf{retAct}(\psi)$ *holds when ψ is a return and* $\mathsf{callAct}(\psi)$ *holds when ψ is a call.*

This definition is intended to express that in the history H, the method call for H_i is completed before the call for H_j starts. To see this intention, assume that H is well-formed. One important consequence of this assumption is that if an object action ψ of some thread t is followed by some return action ψ' of the same thread in the history H (i.e., $H = ...\psi...\psi'...$), then the return for ψ itself appears before ψ' or it is ψ'. Thus, the existence of $H_{i'}$ in the definition ensures that the return action for H_i appears before or at $H_{i'}$ in the history H. By a similar argument, we can see that the call for H_j appears after or at $H_{j'}$. Since $i' < j'$, these two observations mean that the return for H_i appears before the call for H_j, which is the intended meaning of the definition. Using this happen-before order, we define the linearizability relation $\sqsubseteq$:

Definition 14 (Linearizability Relation). *The linearizability relation is a binary relation $\sqsubseteq$ on histories defined as follows: $H \sqsubseteq H'$ iff (1) $H \equiv H'$ and (2) there is a bijection $\pi : \{1, \ldots, |H|\} \to \{1, \ldots, |H'|\}$ such that* [6]

$$(\forall i.\ H_i = H'_{\pi(i)}) \ \wedge\ (\forall i, j.\ H_i \prec_H H_j \Longrightarrow H'_{\pi(i)} \prec_{H'} H'_{\pi(j)}).$$

[5] For the same definition, Herlihy and Wing use the terminology "equivalence".

[6] In this paper, we consider only those histories that arise from complete terminating computations; see the definition of $[\![P]\!]$ in Section 5. Consequently, we do not have to worry about completing or removing pending calls in histories, unlike Herlihy and Wing's definition.

Recall that for each relation $\mathcal{R}$ on histories, its lifting $\lhd_{\mathcal{R}}$ to the relation on object systems is defined by: $OS \lhd_{\mathcal{R}} OS' \iff \forall H \in OS.\, \exists H' \in OS'.\, (H, H') \in \mathcal{R}$. Using this lifting, we formally specify sequential consistency and linearizability.

Definition 15. *Let OS_A and OS_C be object systems. We say that*

- *OS_C is* **sequentially consistent** *wrt. OS_A iff $OS_C \lhd_{\equiv} OS_A$;*
- *OS_C is* **linearizable** *wrt. OS_A iff $OS_C \lhd_{\sqsubseteq} OS_A$.*

Note that this definition does not assume the sequentiality and locality of OS_A, unlike Herlihy and Wing's definitions. We use this more general definition here in order to emphasize that the core ideas of sequential consistency and linearizability lie in relations $\equiv$ and $\sqsubseteq$ on histories, not in the use of a sequential local object system (as a specification).

We first prove the theorem that connects linearizability and observational refinement. Our proof uses the lemma below:

Lemma 3. *Let H be a well-formed history and let i, j be indices in $\{1, \ldots, |H|\}$. Then,*

$$\begin{array}{l}(\exists \tau \in \mathit{WTraces}.\ \mathsf{getHistory}(\tau) = H \ \ \wedge \ \ H_i <_\tau^+ H_j) \\ \quad \Longrightarrow \ \ (i < j) \ \wedge \ (\mathsf{getTid}(H_i) = \mathsf{getTid}(H_j) \ \vee \ H_i \prec_H H_j).\end{array}$$

Proof. Consider a well-formed history H, indices i, j of H and a well-formed trace τ such that the assumptions of this lemma hold. Then, we have indices $i_1 < i_2 < \ldots < i_n$ of τ such that

$$H_i \ = \ \tau_{i_1} \ <_\tau \ \tau_{i_2} \ <_\tau \ \ldots \ <_\tau \ \tau_{i_{n-1}} \ <_\tau \ \tau_{i_n} \ = \ H_j. \quad (1)$$

One conclusion $i < j$ of this lemma follows from this, because $\mathsf{getHistory}(\tau) = H$ means that the order of object actions in H are maintained in τ. To obtain the other conclusion of the lemma, let $t = \mathsf{getTid}(H_i)$ and $t' = \mathsf{getTid}(H_j)$. Suppose that $t \neq t'$. We will prove that for some $i_k, i_l \in \{i_1, \ldots, i_n\}$,

$$i_k < i_l \ \wedge \ t = \mathsf{getTid}(\tau_{i_k}) \ \ \wedge \ t' = \mathsf{getTid}(\tau_{i_l}) \ \wedge \ \mathsf{retAct}(\tau_{i_k}) \ \wedge \ \mathsf{callAct}(\tau_{i_l}). \quad (2)$$

Note that this gives the conclusion we are looking for, because all object actions in τ are from H and their relative positions in τ are the same as those in H. In the rest of the proof, we focus on showing (2) for some i_k, i_l. By the definition of $\#$, an object action ψ can depend on another action φ, only when both actions are done by the same thread. Now note that the first and last actions in the chain in (1) are *object* actions by *different* threads t and t'. Thus, the chain in (1) must contain *client* operations τ_{i_x} and τ_{i_y} such that $\mathsf{getTid}(\tau_{i_x}) = t$ and $\mathsf{getTid}(\tau_{i_y}) = t'$. Let τ_{i_a} be the first client operation by the thread t in the chain and let τ_{i_b} be the last client operation by t'. Then, $i_a < i_b$. This is because otherwise, the sequence $\tau_{i_a} \ \tau_{i_a+1} \ \ldots \ \tau_{i_n}$ does not have any client operation of the thread t', while τ_{i_a} is an action of the thread t and τ_{i_n} is an action of the different thread t'; these facts make it impossible to have $\tau_{i_a} <_\tau \tau_{i_a+1} <_\tau \ldots <_\tau \tau_{i_n}$. Since τ_{i_1} is an object action by the thread t and τ_{i_a} is a client operation by the same thread, by the well-formedness of τ, there should exist some i_k between i_1 (including) and i_a such that τ_{i_k} is a return object action by the thread t. By a symmetric argument, there should be some i_l between i_b and i_n (including) such that τ_{i_l} is a call object action by t'. We have just shown that i_k and i_l satisfy (2), as desired. $\square$

Theorem 2. *The linearizability relation $\sqsubseteq$ is a simulation.*

Proof. For an action φ and a trace τ, define $\varphi\#\tau$ to mean that $\varphi\#\tau_j$ for all $j \in \{1, \ldots, |\tau|\}$. In this proof, we will use this $\varphi\#\tau$ predicate and the following facts:

Fact 1. Trace equivalence $\sim$ is symmetric and transitive.
Fact 2. If $\tau \sim \tau'$ and τ is well-formed, τ' is also well-formed.
Fact 3. If $\tau\tau'$ is well-formed, its prefix τ is also well-formed.
Fact 4. If $\varphi\#\tau'$, we have that $\tau\varphi\tau' \sim \tau\tau'\varphi$.
Fact 5. If $\tau \sim \tau'$, we have that $\tau\varphi \sim \tau'\varphi$.

Consider well-formed histories H, S and a well-formed trace τ such that $H \sqsubseteq S$ and $\mathsf{getHistory}(\tau) = H$. We will prove the existence of a trace σ such that $\tau \sim \sigma$ and $\mathsf{getHistory}(\sigma) = S$. This gives the desired conclusion of this theorem; the only missing requirement for proving that $\sqsubseteq$ is a simulation is the well-formedness of σ, but it can be inferred from $\tau \sim \sigma$ and the well-formedness of τ by Fact 2.

Our proof is by induction on the length of S. If $|S| = 0$, H has to the empty sequence as well. Thus, we can choose τ as the required σ in this case. Now suppose that $|S| \neq 0$. That is, $S = S'\psi$ for some history S' and object action ψ. Note that since the well-formed traces are closed under prefix (Fact 3), S' is also a well-formed history. During the proof, we will use this fact, especially when applying induction on S'.

Let δ be the projection of τ to client operations (i.e., $\delta = \tau|_{\mathcal{A}_c}$). The starting point of our proof is to split τ, H, δ. By assumption, $H \sqsubseteq S'\psi$. By the definition of $\sqsubseteq$, this means that

$$\begin{aligned}\exists H', H''.\ & H = H'\psi H'' \ \wedge\ H'H'' \sqsubseteq S' \\ & \wedge\ \big(\forall j \in \{1, \ldots, |H''|\}.\ \neg(\psi \prec_H H''_j) \ \wedge\ \mathsf{getTid}(\psi) \neq \mathsf{getTid}(H''_j)\big).\end{aligned} \tag{3}$$

Here we use the bijection between indices of H and $S'\psi$, which exists by the definition of $H \sqsubseteq S'\psi$. The action ψ in $H'\psi H''$ is what is mapped to the last action in $S'\psi$ by this bijection. The last conjunct of (3) says that the thread-id of every action of H'' is different from $\mathsf{getTid}(\psi)$. Thus, $\psi\#H''$ (because an *object* action is independent of all actions by *different* threads). From this independence and the well-formedness of H, we can drive that $H'H''\psi$ is well-formed (Facts 2 and 4), and that its prefix $H'H''$ is also well-formed (Fact 3). Another important consequence of (3) is that since $\tau \in \mathit{interleave}(\delta, H)$, the splitting $H'\psi H''$ of H induces splittings of τ and δ as follows: there exist $\tau', \tau'', \delta', \delta''$ such that

$$\tau = \tau'\psi\tau'' \ \wedge\ \delta = \delta'\delta'' \ \wedge\ \tau' \in \mathit{interleave}(\delta', H') \ \wedge\ \tau'' \in \mathit{interleave}(\delta'', H''). \tag{4}$$

The next step of our proof is to identify one short-cut for showing this theorem. The short-cut is to prove $\psi\#\tau''$. To see why this short-cut is sound, suppose that $\psi\#\tau''$. Then, by Fact 4,

$$\tau \ =\ \tau'\psi\tau'' \ \sim\ \tau'\tau''\psi. \tag{5}$$

Since τ is well-formed, this implies that $\tau'\tau''\psi$ and its prefix $\tau'\tau''$ are well-formed traces as well (Facts 2 and 3). Furthermore, $\mathsf{getHistory}(\tau'\tau'') = H'H''$, because of the last two conjuncts of (4). Thus, we can apply the induction hypothesis to $\tau'\tau'', H'H'', S'$,

and obtain σ with the property: $\tau'\tau'' \sim \sigma \ \wedge \ \mathsf{getHistory}(\sigma) = S'$. From this and Fact 5, it follows that

$$\tau'\tau''\psi \sim \sigma\psi \quad \wedge \quad \mathsf{getHistory}(\sigma\psi) = \mathsf{getHistory}(\sigma)\psi = S'\psi. \tag{6}$$

Now, the formulas (5) and (6) and the transitivity of $\sim$ (Fact 1) imply that $\sigma\psi$ is the required trace by this theorem. In the remainder of the proof, we will use this short-cut, without explicitly mentioning it.

The final step is to do the case analysis on δ''. Specifically, we use the nested induction on the length of δ''. Suppose that $|\delta''| = 0$. Then, $\tau'' = H''$, and by the last conjunct of (3) (the universal formula), we have that $\psi \# \tau''$; since ψ is an object action, it is independent of actions by different threads. The theorem follows from this. Now consider the inductive case of this nested induction: $|\delta''| > 0$. Note that if $\psi \# \delta''$, then $\psi \# \tau''$, which implies the theorem. So, we are going to assume that $\neg(\psi \# \delta'')$. Pick the greatest index i of τ'' such that $\psi <^+_\tau \tau''_i$. Let $\varphi = \tau''_i$. Because of the last conjunct of (3) and Lemma 3, τ''_i comes from δ, not H''. In particular, this ensures that there are following further splittings of δ'', τ'' and H'': for some traces $\gamma, \gamma', \kappa, \kappa', T, T'$,

$$\begin{array}{l} \delta'' \ = \ \gamma\varphi\gamma' \ \wedge \ \tau'' \ = \ \kappa\varphi\kappa' \ \wedge \ H'' \ = \ TT' \ \wedge \\ \kappa \ \in \ \mathit{interleave}(\gamma, T) \ \wedge \ \kappa' \ \in \ \mathit{interleave}(\gamma', T') \ \wedge \ \varphi\#\kappa'. \end{array}$$

Here the last conjunct $\varphi\#\kappa'$ comes from the fact that φ is the last element of τ'' with $\psi <^+_\tau \varphi$. Since γ' is a subsequence of κ', the last conjunct $\varphi\#\kappa'$ implies that $\varphi\#\gamma'$. Also, $\tau'\psi\kappa\varphi\kappa' \sim \tau'\psi\kappa\kappa'\varphi$ by Fact 4. Now, since $\tau = \tau'\psi\kappa\varphi\kappa'$ is well-formed, the equivalent trace $\tau'\psi\kappa\kappa'\varphi$ and its prefix $\tau'\psi\kappa\kappa'$ both are well-formed as well (Facts 2 and 3). Furthermore, $\tau'\psi\kappa\kappa' \in \mathit{interleave}(\delta'\gamma\gamma', H'\psi H'')$. Since the length of $\gamma\gamma'$ is shorter than δ'', we can apply the induction hypothesis of the nested induction, and get

$$\exists\sigma. \quad \tau'\psi\kappa\kappa' \sim \sigma \quad \wedge \quad \mathsf{getHistory}(\sigma) = S'\psi. \tag{7}$$

We will prove that $\sigma\varphi$ is the trace desired for this theorem. Because of $\varphi\#\kappa'$ and Fact 4, $\tau = \tau'\psi\kappa\varphi\kappa' \sim \tau'\psi\kappa\kappa'\varphi$. Also, because of Fact 5 and the first conjunct of (7), $\tau'\psi\kappa\kappa'\varphi \ \sim \ \sigma\varphi$. Thus, $\tau \sim \sigma\varphi$ by the transitivity of $\sim$. Furthermore, since φ is not an object action, the second conjunct of (7) implies that $\mathsf{getHistory}(\sigma\varphi) = \mathsf{getHistory}(\sigma) = S'\psi$. We have just shown that $\sigma\varphi$ is the desired trace. □

Corollary 1. *If OS_C is linearizable wrt. OS_A, then OS_C observationally refines OS_A.*

Proof. Suppose that OS_C is linearizable wrt. OS_A. Then, $OS_C \lhd_\sqsubseteq OS_A$. Furthermore, $\sqsubseteq$ is a simulation by Theorem 2. From these and Theorem 1 follows this corollary. □

Next, we consider sequential consistency. For sequential consistency to imply observational refinement, we need to restrict programs such that threads can access local variables only in their client operations: $\forall t, t', a, a'.\, (t{\neq}t' \wedge a \ \in \ \mathit{Cop}_t \wedge a' \in \mathit{Cop}_{t'}) \implies a \,\#\, a'$.

Lemma 4. *Suppose that all threads can access local variables only in their client operations. Then, for all well-formed histories H and indices i, j in $\{1, \ldots, |H|\}$,*

$$(\exists \tau{\in}\mathit{WTraces}.\, \mathsf{getHistory}(\tau){=}H \wedge H_i{<}^+_\tau H_j) \implies i{<}j \wedge \mathsf{getTid}(H_i){=}\mathsf{getTid}(H_j).$$

Proof. Consider a well-formed history H, indices i, j and a well-formed trace τ satisfying the assumptions of this lemma. Then, for some indices $i_1 < ... < i_n$ of τ,

$$H_i \quad = \quad \tau_{i_1} \quad <_\tau \quad \tau_{i_2} \quad <_\tau \quad \ldots \quad <_\tau \quad \tau_{i_{n-1}} \quad <_\tau \quad \tau_{i_n} \quad = \quad H_j. \qquad (8)$$

One conclusion $i < j$ of this lemma follows from this; the assumption $\mathsf{getHistory}(\tau) = H$ of this lemma means that the order of object actions in H are maintained in τ. To obtain the other conclusion of the lemma, we point out one important property of $\#$: under the assumption of this lemma, $\neg(\varphi\#\varphi')$ only when $\mathsf{getTid}(\varphi) = \mathsf{getTid}(\varphi')$. (Here φ, φ' are not necessarily object actions.) To see why this property holds, we assume $\neg(\varphi\#\varphi')$ and consider all possible cases of φ and φ'. If one of φ and φ' is an object action, the definition of $\#$ implies that φ and φ' have to be actions by the same thread. Otherwise, both φ and φ' are atomic client operations. By our assumption, all threads access only local variables in their client operations, so that two client operations are independent if they are performed by different threads. This implies that φ and φ' should be actions by the same thread. Now, note that $\tau_k <_\tau \tau_l$ implies $\neg(\tau_k\#\tau_l)$, which in turn entails $\mathsf{getTid}(\tau_k) = \mathsf{getTid}(\tau_l)$ by what we have just shown. Thus, we can derive the following desired equality from (8):

$$\mathsf{getTid}(H_i) = \mathsf{getTid}(\tau_{i_1}) = \mathsf{getTid}(\tau_{i_2}) = \ldots = \mathsf{getTid}(\tau_{i_n}) = \mathsf{getTid}(H_j). \quad \square$$

Theorem 3. *If all threads access local variables only in their client actions, the weak equivalence $\equiv$ is a simulation.*

Proof. The proof is similar to the one for Theorem 2. Instead of repeating the common parts between these two proofs, we will explain what we need to change in the proof of Theorem 2, so as to obtain the proof of this theorem. Firstly, we should replace linearizability relation $\sqsubseteq$ by weak equivalence $\equiv$. Secondly, we need to change the formula (3) to

$$\exists H'H''.\ H = H'\psi H'' \wedge H'H'' \equiv S' \wedge \forall j \in \{1, ..., |H''|\}.\ \mathsf{getTid}(\psi) \neq \mathsf{getTid}(H''_j).$$

Finally, we should use Lemma 4 instead of Lemma 3. After these three changes have been made, the result becomes the proof of this theorem. $\square$

Corollary 2. *If OS_C is sequentially consistent wrt. OS_A and all threads access local variables only in their client actions, OS_C is an observational refinement of OS_A.*

Proof. This corollary follows from Theorems 1 and 3. $\square$

Completeness Under suitable assumptions on programming languages and object systems, we can obtain the converse of Corollaries 1 and 2: observational refinement implies linearizability and sequential consistency. First, we assume that object systems OS contain only those histories all of whose calls have matching returns. This assumption is necessary, because observational refinement considers only terminating, completed computations. Next, we assume that threads' primitive commands include the `skip` statement. Finally, we consider specific assumptions for sequential consistency and linearizability, which will be described shortly.

For sequential consistency, we suppose that the programming language contains atomic assignments $x{:=}n$ of constants n to thread-local variable x and has atomic assume statements of the form $\texttt{assume}(x{=}n)$ with thread-local variable x.[7] Note that this supposition does not require the use of any global variables, so that it is consistent with the assumption of Corollary 2. Under this supposition, observational refinement implies sequential consistency.

Theorem 4. *If OS_C observationally refines OS_A then $OS_C \lhd_{\equiv} OS_A$.*

The main idea of the proof is to create for every history $H \in OS_C$ a program P_H that records the interaction of every thread t with the object system using t's local variables. This program lets us use the assumed observational refinement and find a history $H' \in OS_A$ required by this theorem. The detailed proof is given in Appendix A.

For linearizability, we further suppose that there is a single global variable g shared by all threads. That is, threads can assign constants to g atomically, or they can run the statement $\texttt{assume}(g{=}n)$ for some constant n. Under this supposition, observational refinement implies linearizability.

Theorem 5. *If OS_C observationally refines OS_A, then $OS_C \lhd_{\sqsubseteq} OS_A$.*

The core idea of the proof is, again, to create for every history $H \in OS_C$ one specific program P_H. This program uses a single global variable and satisfies that for every (terminating) execution τ of P_H, the object history of τ always has the same happen-before relation as H. We then instantiate the assumed observational refinement with P_H, and this instantiation leads to a desired history H' in OS_A by this theorem. The detailed proof appears in Appendix A.

8 Abstract Dependency

Although our results on observational refinements give complete characterization of sequential consistency and linearizability, they still do not explain where the relations $\equiv$ and $\sqsubseteq$ in sequential consistency and linearizability come from. In this section, we will answer this question using the dependency between actions.

The result of this section is based on one reading of a well-formed history H. In this reading, the history H means not the single trace H itself but the set of all the well-formed traces whose object actions are described by H. Formally, we let $\mathit{WHistories}$ be the set of all the well-formed histories, and define the function means as follows:

$$\begin{array}{rcl} \mathsf{means} & : & \mathit{WHistories} \to \mathcal{P}(\mathit{WTraces}) \\ \mathsf{means}(H) & = & \{\tau \in \mathit{WTraces} \mid \mathsf{getHistory}(\tau) = H\}. \end{array}$$

Using means, we define a new relation on well-formed histories, which compare possible dependencies between actions in the histories.

[7] Technically, this assumption also means that $T(x{:=}n)t$ and $T(\texttt{assume}(x{=}n))t$ are singleton traces (t, a) and (t, b), where $[\![b]\!](s) \equiv \mathsf{if}\ (s(x){=}n)\ \mathsf{then}\ \{s\}\ \mathsf{else}\ \{\}$ and $[\![a]\!](s) \equiv \{s[x{\mapsto}n]\}$.

Definition 16 (Abstract Dependency). *For each well-formed history H, the* **abstract dependency** $<_H^{\#}$ *for H is the binary relation on actions in H determined by*

$$H_i <_H^{\#} H_j \iff i < j \ \wedge \ \exists \tau \in \mathsf{means}(H).\ H_i <_\tau^{+} H_j.$$

The RHS formula of the equivalence here means that in some concrete trace τ of H, there is a chain of dependencies from H_i to H_j. Note that using this formula, the definition ensures that $<_H^{\#}$ overapproximates all such dependency chains.

Definition 17 (Causal Complexity Relation). *The* **causal complexity relation** $\sqsubseteq^{\#}$ *is a binary relation on well-formed histories, such that $H \sqsubseteq^{\#} S$ iff there exists a bijection $\pi : \{1, \ldots, |H|\} \to \{1, \ldots, |S|\}$ satisfying*

$$\forall i, j \in \{1, \ldots, |H|\}. \quad H_i = S_{\pi(i)} \ \wedge \ (H_i <_H^{\#} H_j \implies S_{\pi(i)} <_S^{\#} S_{\pi(j)}).$$

Intuitively, $H \sqsubseteq^{\#} S$ means that S is a rearrangement of actions in H that preserves all the abstract causal dependencies in H. Note that S might contain abstract causal dependencies that are not present in H.

We now present the main results of this section, the identification of the cases where sequential consistency or linearizability coincides with causal complexity relation. The proofs of these theorems appear in Appendix B.

Theorem 6. *If all threads access only local variables in their client operations, then $\forall H, S \in \mathit{WHistories}.\ H \equiv S \iff H \sqsubseteq^{\#} S$.*

Theorem 7. *Assume that for every pair (t, t') of thread-ids with $t \neq t'$, there exist client operations $a \in \mathit{Cop}_t$ and $a' \in \mathit{Cop}_{t'}$ with $\neg(a \# a')$. Under this assumption, we have the following equivalence: $\forall H, S \in \mathit{WHistories}.\ H \sqsubseteq S \iff H \sqsubseteq^{\#} S$.*

9 Conclusions

Developing a theory of data abstraction in the presence of concurrency has been a long-standing open question in the programming language community. In this paper, we have shown that this open question can be attacked from a new perspective, by carefully studying correctness conditions proposed by the concurrent-algorithm community, using the tools of programming languages. We prove that linearizability is a sound method for proving observational refinements for concurrent objects, which becomes complete when threads are allowed to access shared global variables. When threads access only thread-local variables, we have shown that sequential consistency becomes a sound and complete proof method for observational refinements. We hope that our new understanding on concurrent objects can facilitate the long-delayed transfer of the rich existing theories of data-abstraction [7, 8, 13, 10, 12] from sequential programs to concurrent ones.

In the paper, we used a standard assumption on a programming language from the concurrent-algorithm community. We assumed that a programming language did not allow callbacks from concurrent objects to client programs, that all the concurrent objects were properly encapsulated [1], and that programs were running under "sequentially consistent" memory models. Although widely used by the concurrent-algorithm

experts, these assumptions limit the applicability of our results. In fact, they also limit the use of linearizability in the design of concurrent data structures. Removing these assumptions and extending our results is what we plan to do next.

References

1. A. Banerjee and D. A. Naumann. Representation independence, confinement and access control. In *POPL'02*, 2002.
2. S. D. Brookes. A semantics for concurrent separation logic. In *CONCUR'04*, 2004.
3. J. He, C. A. R. Hoare, and J. W. Sanders. Data refinement refined. In *ESOP'86*, 1986.
4. M. Herlihy and N. Shavit. *The Art of Multiprocessor Programming*. Morgan Kaufmann, 2008.
5. M. Herlihy and J. M. Wing. Linearizability: A correctness condition for concurrent objects. *ACM TOPLAS*, 12(3):463–492, 1990.
6. C. A. R. Hoare. Proof of correctness of data representations. *Acta Inf.*, 1:271–281, 1972.
7. C. A. R. Hoare, J. He, and J. W. Sanders. Prespecification in data refinement. *Inf. Proc. Letter*, 25(2):71–76, May 1987.
8. L. Lamport. How to make a multiprocessor computer that correctly executes multiprocess programs. *IEEE Trans. Computers*, 28(9):690–691, 1979.
9. J. Mitchell and G. Plotkin. Abstract types have existential types. *ACM TOPLAS*, 10(3):470–502, 1988.
10. G. Plotkin. LCF considered as a programming language. *TCS*, 5:223–255, 1977.
11. G. Plotkin and M. Abadi. A logic for parametric polymorphism. In *TLCA'93*, 1993.
12. J. C. Reynolds. Types, abstraction and parametric polymorphism. In R. E. A. Mason, editor, *Information Processing '83*, pages 513–523. North-Holland, Amsterdam, 1983.

A Proofs of Theorems 4 and 5

Call a history H *completed* if all calls in H have matching returns. Also, throughout this appendix, we assume that the programming language includes `skip`.

Theorem 4. *Suppose that programs can have atomic assignments $x{:=}n$ and atomic assume statements* `assume`$(x{=}n)$ *for thread-local variables x and constant n. If OS_C contain only completed histories and OS_C observationally refines OS_A, then $OS_C \lhd_{\equiv} OS_A$.*

Proof. The plan of the proof is to construct for every history $H \in OS_C$ a program P_H that records the interactions of every thread with the object system from the point of view of every thread. The goal is to make it possible to record this interaction at every final state s' of P_H and thus be able to read $H|_t$ from s'.

Let H be a history in OS_C. Let $H|_t$ be the projection of H on the object actions executed by thread t. H, when viewed as a trace, is well-formed. Thus, $H|_t$, is a sequential trace. In particular, $H|_t$ is comprised of a sequence of pairs of call and return object actions. (By our assumption, $H|_t$ is comprised only of matching pairs of calls and returns.)

For every thread t that has an action in H, we construct a straight-line command $P_H^t = C_1^t; C_2^t; \ldots; C_{k_t}^t$, where $k_t = |(H|_t)|/2$ is the number of pairs of call and return actions executed by thread t. Here C_i^t is a sequence of atomic commands, and it is constructed according to the i-th pair of object actions in $H|_t$. The definition of C_i^t goes as follows. For $i = 1, \ldots, k$, let $(H|_t)_{2i-1} = (t, call\, o.f(n_i^t))$ and $(H|_t)_{2i} = (t, ret(m_i^t)\, o.f)$. The composed command that we construct for this pair is

$$C_i^t \quad = \quad x_i^t{:=}n_i^t;\ y_i^t{:=}o.f(x_i^t);\ \texttt{assume}(y_i^t{=}m_i^t).$$

Note that the composed command is constructed according to the values in H: C_i^t invokes operation f on object o passing n_i^t as the argument and expects that the return value be m_i^t. Furthermore, note that the argument to the command is recorded in x_i^t and the return value is recorded in y_i^t. Both of these variables are local to thread t and are never rewritten. Thus, starting from any state, the only trace $\tau_i^t \in T(C_i^t)t$ that can be executed until completion for some initial state is

$$\begin{array}{rcl} \tau^t_{n_i^t, m_i^t} & = & (t, x_i^t := n_i^t); (t, assume(x_i^t = n_i^t)); \\ & & (t, call\, o.f(n_i^t)); (t, ret(m_i^t)); \\ & & (t, y_i^t := m_i^t); (t, assume(y_i^t = m_i^t)) \end{array}$$

Here we overload $x := n$ and $assume(x{=}n)$ to mean not primitive commands but atomic client operations in Cop_t, with standard meanings. Let τ^t be $\tau^t_{n_1^t, m_1^t}; \tau^t_{n_2^t, m_2^t}; \ldots$.

The following claims are immediate:

Claim 1. For every trace τ, if $\tau|_t \in T(P_H^t)t$ and τ can be evaluated until completion for some initial state, then $\tau|_t = \tau^t$. Furthermore, if $\tau|_t = \tau^t$ for all threads t in τ, the evaluation of τ can be evaluated until completion for all states.

Claim 2. Since x_i^t and y_i^t are thread-local variables and they are never rewritten by their owner thread, we have that $x_i^t = n_i^t$ and $y_i^t = m_i^t$ at every final state in $\mathsf{eval}(s, \tau)$, as long as $\tau|_t \in T(P_H^t)t$.

Claim 3. $H|_t = \mathsf{getHistory}(\tau^t)$.

We construct a program P_H which corresponds to history H by a parallel composition of the commands for every thread: $P_H = P_H^1 || \ldots || P_H^{t_{max}}$, where t_{max} is the maximal thread identifier in H. For technical reasons, in case $1 \leq t < t_{max}$ does not appear in H, we define $P_H^t = \texttt{skip}$. (Recall that H is a finite sequence, thus there is a finite number of threads executing in H. Specifically, there is a finite number of such commands).

Let τ_H be an interleaving of $\tau^{t_1}, \ldots, \tau^{t_{max}}$ such that $\mathsf{getHistory}(\tau_H) = H$. Such a τ_H exists because of Claim 3 above and $H \in \mathit{interleave}(H|_{t_1}, \ldots, H|_{t_{max}})$. Furthermore, $\tau_H \in T(P_H)$ because $\tau^{t_i} \in T(P_H^{t_i})t_i$ for every $t_i = t_1, \ldots, t_{max}$.

Let n_0 be a value that does not appear in H. Let s_0 be a state where all (local) variables x_i^t's and y_i^t's are initialized to n_0. Let s' be the state where $s'(x_i^t) = n_i^t$ and $s'(y_i^t) = m_i^t$. Because $\mathsf{getHistory}(\tau_H) = H \in OS_C$, the combination of Claims 1 and 2 and the definition of eval implies that $s' \in [\![P_H]\!](OS_C)(s_0)$.

Now, we have $s' \in [\![P_H]\!](OS_A)(s_0)$, because OS_C observationally refines OS_A. Thus, there exists a trace $\tau_A \in T(P_H)$ and history $H_A \in OS_A$ such that $s' \in \mathsf{eval}(\tau_A, s_0)$ and $\mathsf{getHistory}(\tau_A) = H_A$. Since $\tau_A \in T(P_H)$, we have that $(\tau_A)|_t \in T(P_H^t)$. By Claim 1, this means that for every thread t, $\tau_A|_t = \tau^t$. By Claim 3, we get that $H_A \equiv H$, which implies that OS_C is sequentially consistent wrt. OS_A. □

Theorem 5. *Suppose that programs can have atomic assignments $x{:=}n$ and atomic assume statements $\texttt{assume}(x{=}n)$ for thread-local variables x and constant n. Suppose further that threads have atomic constant assignments and assume statements to one shared global variable. If OS_C contains only completed histories and OS_C observationally refines OS_A, then $OS_C \lhd_\sqsubseteq OS_A$.*

Proof. The plan of the proof is similar to that for Theorem 4. We construct, for every history $H \in OS_C$, a program P_H that records the interactions of of every thread with the object system. This recoding remains in the final state of P_H and thus allows us to see every step of $H|_t$. We use a global variable g to enforce that every (terminating) execution of the program has the same happen-before order between object operations.

Let H be a history in OS_C. Let $H|_t$ be the projection of H to object operations executed by thread t. Using the same argument as in the proof of Theorem 4, we construct, for every thread t which has an action in H, a straight-line composite command

$$PL_H^t \quad = \quad CL_1^t;\ CL_2^t;\ \ldots;\ CL_{k_t}^t,$$

where $k_t = |(H|_t)|/2$ is the number of pairs of call and return actions executed by thread t, as a sequence of composed commands and CL_i^t is constructed according to the i-th pair of object actions in H done by thread t. The construction of CL_i^t goes as follows. For $i = 1, \ldots, k_t$, let $(H|_t)_{2i-1} = (t, \mathit{call}\, o.f(n_i^t))$ and $(H|_t)_{2i} = (t, \mathit{ret}(m_i^t)\, o.f)$. Let i_c and i_r be the indices of these actions in H, i.e., $H_{i_c} = (H|_t)_{2i-1}$ and $H_{i_r} = (H|_t)_{2i}$. The corresponding command CL_i^t is

$$CL_i^t \quad = \quad \texttt{assume}(g{=}i_c);\ g{:=}i_c{+}1;\ C_i^t;\ \texttt{assume}(g{=}i_r);\ g{:=}i_r{+}1\ ,$$

where C_i^t is defined as in the proof of Theorem 4, i.e.,

$$C_i^t \quad = \quad x_i^t{:=}n_i^t;\ y_i^t{:=}o.f(x_i^t);\ \texttt{assume}(y_i^t{=}m_i^t)\ .$$

Note that the command C_i^t in CL_i^t can be executed only when $g = i_c$, and that if so, CL_i^t increments g by 1 before running C_i^t. Similarly, after C_i^t terminates, the computation of t can continue only when $g = i_r$, and then again g is incremented.

By the same reason discussed in the proof of Theorem 4, the only trace $\alpha_i^t \in T(CL_i^t)t$ that can be executed until completion is

$$\begin{array}{rcl} \alpha^t_{n_i^t,m_i^t} & = & (t, assume(g{=}i_c));\ (t, g := i_c{+}1); \\ & & \tau^t_{n_i^t,m_i^t}; \\ & & (t, assume(g{=}i_r));\ (t, g := i_r{+}1) \end{array}$$

where $\tau^t_{n_i^t,m_i^t}$ is defined as in the proof of Theorem 4:

$$\begin{array}{rcl} \tau^t_{n_i^t,m_i^t} & = & (t, x_i^t{:=}n_i^t);\ (t, assume(x_i^t{=}n_i^t)); \\ & & (t, call\ o.f(n_i^t));\ (t, ret(m_i^t)); \\ & & (t, y_i^t{:=}m_i^t);\ (t, assume(y_i^t{=}m_i^t)) \end{array}$$

We construct a program P_H^L, which corresponds to history H, by a parallel composition of the command for each thread:

$$P_H^L \quad = \quad PL_H^1 || \ldots || PL_H^{t_{max}},$$

where t_{max} is the maximal thread identifier in H. For technical reasons, in case that some t with $1 \leq t < t_{max}$ does not appear in H, we define $PL_H^t = \texttt{skip}$.

Let α_H be an interleaving of $\alpha^1, \ldots, \alpha^{t_{max}}$ such that $\mathsf{getHistory}(\alpha_H) = H$ that can be evaluated until completion. Again, such an α_H exists for the same reason discussed in the proof of Theorem 4. Furthermore, assume that α_H is an interleaving of action sequence fragments of the following two forms:

$$(t, assume(g{=}i_c)); (t, g{:=}i_c{+}1); (t, x_i^t{:=}n_i^t); (t, assume(x_i^t{=}n_i^t)); (t, call\ o.f(n_i^t))\ ,$$

$$(t, ret(m_i^t)); (t, y_i^t{:=}m_i^t); (t, assume(y_i^t{=}m_i^t)); (t, assume(g{=}i_r)); (t, g{:=}i_r{+}1)\ .$$

Thus, once a thread runs $assume(g{=}i_c)$ in α_H, it continues without being intervened by different threads at least until it invokes the i-th (call) object action. Similarly, once a thread runs the i-th (return) object action, it continues without being interrupted at least until it assigns $i_r{+}1$ to g. Note that in α, g is incremented and tested in the same order as the object actions occur in H.

Let n_0 be a value that does not appear in H. Let s_0 be a state where all (local) variables x_i^t's and y_i^t's are initialized to n_0 and g is initialized to 1. Note that our construction of α_H ensures that the trace α_H can run until completion from the initial state s_0. Furthermore, since OS_C observationally refines OS_A, by the same arguments as in the proof of Theorem 4, we can infer that there exists a history $S \in OS_A$ such that $S \equiv H$, and also that there exists $\alpha \in T(P_H^L)$ with $\mathsf{getHistory}(\alpha) = S \wedge \mathsf{eval}(s_0, \alpha) \neq \emptyset$. Using α, we will show that the bijection π implicit in $H \equiv S$ preserves the happen-before order. Let H_i be a return action in H and let H_j be a call action. Let $\bar{i}$ and $\bar{j}$ be the indices of H_i and H_j in S, respectively. By the choice of π, it is sufficient to prove that if $i < j$, then $\bar{i} < \bar{j}$. Suppose that $i < j$. Then, $i_r < j_c$. Since α can run until completion,

the definition of P_H^L implies that the assume statement for g following the return of $S_{\bar{i}}$ should be run before the assume statement that comes before the call of $S_{\bar{j}}$. This means that $S_{\bar{i}}$ occurs before $S_{\bar{j}}$ in α. Since $\mathsf{getHistory}(\alpha) = S$, we should have that $\bar{i} < \bar{j}$ as desired. What we have shown implies that π preserves the happen-before order. This in turn means $H \sqsubseteq H_A^L$. That is, OS_C is linearizable wrt. OS_A. □

B Proofs of Theorems 6 and 7

Theorem 6. *If all threads access only local variables in their client operations, then*

$$\forall H, S \in \mathit{WHistories}.\quad H \equiv S \iff H \sqsubseteq^{\#} S.$$

Proof. For each well-formed history H, define a relation $<'_H$ on actions of H by

$$H_i <'_H H_j \quad \iff \quad (i < j \ \wedge \ \mathsf{getTid}(H_i) = \mathsf{getTid}(H_j)).$$

We will prove this theorem by showing two lemmas on well-formed histories. The first lemma is that $H \equiv S$ iff there exists a bijection π such that

$$\forall i, j \in \{1, \ldots, |H|\}.\quad H_i = S_{\pi(i)} \quad \wedge \quad (H_i <'_H H_j \Longrightarrow S_{\pi(i)} <'_S S_{\pi(j)}). \quad (9)$$

The second lemma is that for all well-formed histories H, the two relations $<'_H$ and $<_H^{\#}$ coincide. Note that the second lemma allows us to replace $<'_H$ and $<'_S$ in (9) by $<_H^{\#}$ and $<_S^{\#}$. This replacement would change the first lemma to the equivalence claimed in this theorem. Thus, it is sufficient to prove these two lemmas.

To show the only-if direction of the first lemma, suppose that $H \equiv S$. Then, $|H| = |S|$ and $H|_t = S|_t$ for all thread-ids t. Thus, we can define a bijection $\pi : \{1, \ldots, |H|\} \to \{1, \ldots, |S|\}$ by setting $\pi(i)$ to j where both H_i and S_j are the same k-th action in $H|_t$ $(= S|_t)$ for some k and t. It is straightforward to show that π is the required bijection in the first lemma. For the if direction, suppose that π is a bijection satisfying (9). Choose an arbitrary thread-id t. We need to show that $H|_t = S|_t$. Since S is a rearrangement of actions in H, we have $|H|_t| = |S|_t|$. Pick an index k of $H|_t$. It suffices to show that $(H|_t)_k = (S|_t)_k$. Let i be the index of H such that H_i is the k-th element of $H|_t$. Then, in the history H, exactly $(k-1)$-many actions by the thread t appear before i, and $(|H|_t| - k)$-many actions by t appear after i. Now, by the implication in (9), in the history S, at least $k-1$ actions by the thread t should appear before $\pi(i)$, and at least $|H|_t| - k$ actions by t should appear after $\pi(i)$. But, $|S|_t| = |H|_t|$. Thus, $\pi(i)$ is the k-th action by the thread t in S. Note that by the equality in (9), $H_i = S_{\pi(i)}$, so that the k-th action of $H|_t$ is the same as the k-th action of $S|_t$.

Now, we move on to the second lemma: $<_H^{\#} = <'_H$. Note that that the inclusion $<_H^{\#} \subseteq <'_H$ is already proved in Lemma 4. To prove the other inclusion, suppose that $H_i <'_H H_j$. Then, $i < j$ and $\neg(H_i \# H_j)$. Thus, $H_i <_H^{+} H_j$. Furthermore, since H is well-formed, it belongs to $\mathsf{means}(H)$. By combining $H_i <_H^{+} H_j$ and $H \in \mathsf{means}(H)$, we can obtain $H_i <_H^{\#} H_j$ as desired. □

Theorem 7. *Assume that for every pair (t, t') of thread-ids with $t \neq t'$, there exist client operations $a \in Cop_t$ and $a' \in Cop_{t'}$ with $\neg(a \# a')$. Under this assumption, we have the following equivalence:*

$$\forall H, S \in \mathit{WHistories}.\ \ H \sqsubseteq S \iff H \sqsubseteq^{\#} S.$$

Proof. For each well-formed history H, define a relation $<''_H$ on actions of H by

$$H_i <''_H H_j \iff (i < j \ \wedge\ (\mathsf{getTid}(H_i) = \mathsf{getTid}(H_j) \ \vee\ H_i \prec_H H_j)). \quad (10)$$

As in the proof of Theorem 6, we will prove this theorem by showing two lemmas on well-formed histories. The first lemma is that $H \sqsubseteq S$ iff there is a bijection π on $\{1, \ldots, |H|\}$ such that

$$\forall i, j \in \{1, \ldots, |H|\}.\ \ H_i = S_{\pi(i)} \ \wedge\ (H_i <''_H H_j \Longrightarrow S_{\pi(i)} <''_S S_{\pi(j)}). \quad (11)$$

The second lemma is that for all well-formed histories H, the two relations $<''_H$ and $<^{\#}_H$ coincide. To see how the conclusion of the theorem follows these lemmas, note that the second lemma allows us to replace $<''_H$ and $<''_S$ in (11) by $<^{\#}_H$ and $<^{\#}_S$. This replacement would give the desired equivalence for this theorem. In the remainder of the proof, we will show these two lemmas.

To show the only-if direction of the first lemma, suppose that $H \sqsubseteq S$. Then, there is a bijection π such that

$$\forall i, j \in \{1, \ldots, |H|\}.\ \ H_i = S_{\pi(i)} \ \wedge\ (H_i \prec_H H_j \Longrightarrow S_{\pi(i)} \prec_S S_{\pi(j)}). \quad (12)$$

We will show that π satisfies (11). Suppose that $H_i <''_H H_j$ for some i, j. Then, $i < j$. Let $t = \mathsf{getTid}(H_i)$ and $t' = \mathsf{getTid}(H_j)$. We do the case analysis on $H_i \prec_H H_j$. If $H_i \prec_H H_j$, (12) implies that $S_{\pi(i)} \prec_S S_{\pi(j)}$, which in turn entails that $\pi(i) < \pi(j)$ (by the definition of $\prec_S$). Thus, in this case, we have $S_{\pi(i)} <''_S S_{\pi(j)}$ as desired. If $\neg(H_i \prec_H H_j)$, we should have that $t = t'$, because $H_i <''_H H_j$. Thus,

$$\mathsf{getTid}(S_{\pi(i)}) = \mathsf{getTid}(H_i) = t = t' = \mathsf{getTid}(H_j) = \mathsf{getTid}(S_{\pi(j)}).$$

This means that we can complete the only-if direction by showing that $\pi(i) < \pi(j)$. Note that H_i and H_j should be the call and return actions of the same method call, respectively; otherwise, due to the well-formedness of H, we can find a return for H_i and a call for H_j between H_i and H_j, which entails that $H_i \prec_H H_j$, contradicting our assumption $\neg(H_i \prec_H H_j)$. Another fact to note is that since H is well-formed and H_j is the return for H_i,

$$\forall k.\ \mathsf{getTid}(H_k) = t \Longrightarrow (k < i \Longrightarrow H_k \prec_H H_i) \wedge (j < k \Longrightarrow H_i \prec_H H_k).$$

By (12) and the definition of $\prec_S$,

$$\forall k.\ \mathsf{getTid}(H_k) = t \Longrightarrow (k < i \Longrightarrow \pi(k) < \pi(i)) \wedge (j < k \Longrightarrow \pi(i) < \pi(k)). \quad (13)$$

Let m be the number of t's actions in H that appears before i and let n be the number of t's actions in H that occurs after j. Then, by what we have just shown, the number of t's

actions in H is $n+m+2$. For the sake of contradiction, suppose that $\pi(j) < \pi(i)$. (They cannot be the same because π is bijective.) Then, because of (13) and this supposition, at least $(m+1)$-many actions by t occur before $S_{\pi(i)}$ in S. But, among these $m+1$ actions, there are $m/2+1$ return actions, because $H_j = S_{\pi(j)}$ is a return action and the half of the remaining m actions are return actions. Now, due to the well-formedness of S, all these return actions should have matching call actions in S before them, so that we can infer that there are $(m+2)$ actions by t in S before $\pi(i)$. Since n-many actions of t appear in H after j, (13) implies that there are at least n-many t's actions after $\pi(i)$ in S. By collecting all these numbers, we can infer that S has at least $(m+2)+1+n$ actions by t (where 1 comes from $\pi(i)$). Note that this number is greater than $m+n+2$, the number of t's actions in H. This is contradictory, because $H|_t = S|_t$.

For the if direction of the first lemma, suppose that π is a bijection satisfying (11). To show that $H \equiv S$, we reuse the proof of Theorem 6. The key observation here is that by the definitions of $<'_H$ and $<''_H$, (11) implies (9). Furthermore, while proving Theorem 6, we already showed that (9) implies $H \equiv S$. Thus, $H \equiv S$ holds here as well. We now show that π satisfies the requirement in the definition of linearizability. Suppose that $H_i \prec_H H_j$. Then, $H_i <''_H H_j$ by (10), and $S_{\pi(i)} <''_S S_{\pi(j)}$ by (11). Let $t = \mathsf{getTid}(S_{\pi(i)})$ and $t' = \mathsf{getTid}(S_{\pi(j)})$. We do the case analysis on $t = t'$. Suppose that $t \neq t'$. Then, by (10), $S_{\pi(i)} \prec_S S_{\pi(j)}$, as desired. Now, suppose $t = t'$. In this case, we only need to show that $S_{\pi(j)}$ is not a return for $S_{\pi(i)}$, because that is the only case that $\neg(S_{\pi(i)} \prec_S S_{\pi(j)})$. Since $t = t'$,

$$\mathsf{getTid}(H_i) = \mathsf{getTid}(S_{\pi(i)}) = t = t' = \mathsf{getTid}(S_{\pi(j)}) = \mathsf{getTid}(H_j).$$

Furthermore, $H_i \prec_H H_j$ by the choice of i, j. Thus, H_j is not a return for H_i. This means that H_i is a return and H_j is a call, or there is some action by the thread t between H_i and H_j. In both cases, (11) implies that $S_{\pi(j)}$ is not a return for $S_{\pi(i)}$, as desired.

Now, we move on to the second lemma: $<^{\#}_H = <''_H$. The inclusion $<^{\#}_H \subseteq <''_H$ is already proved in Lemma 3. To prove the other inclusion, suppose that $H_i <''_H H_j$. Then, $i < j$. Let $t = \mathsf{getTid}(H_i)$ and $t' = \mathsf{getTid}(H_j)$. If $t = t'$, we have $\neg(H_i \# H_j)$. This implies that $H_i <^{\#}_H H_j$, because H is well-formed so that it is in $\mathsf{means}(H)$. Now, consider the other case that $t \neq t'$. Then, $H_i \prec_H H_j$. This means that for some indices k, l of H,

$$(i \leq k < l \leq j) \wedge \mathsf{getTid}(H_k) = t \wedge \mathsf{getTid}(H_l) = t' \wedge \mathsf{retAct}(H_k) \wedge \mathsf{callAct}(H_l).$$

We use the assumption of this theorem, and get client operations $a \in \mathit{Cop}_t$ and $a' \in \mathit{Cop}_{t'}$ with $\neg(a \# a')$. Using these a, a', we define τ to be

$$H_1;\ H_2;\ \ldots\ H_k;\ (t, a);\ H_{k+1};\ \ldots\ H_{l-1};\ (t', a');\ H_l;\ \ldots\ H_{|H|}.$$

Since H is well-formed, H_k is a return by t and H_l is a call by t', the trace τ is well-formed as well. Furthermore,

$$H_i \ <_\tau \ H_k \ <_\tau \ (t, a) \ <_\tau \ (t', a') \ <_\tau \ H_l \ <_\tau \ H_j.$$

This shows that $H_i <^{+}_\tau H_j$. From this follows the desired conclusion: $H_i <^{\#}_H H_j$. $\square$