

# Liveness-Preserving Atomicity Abstraction\*

Alexey Gotsman and Hongseok Yang

<sup>1</sup> IMDEA Software Institute

<sup>2</sup> University of Oxford

**Abstract.** Modern concurrent algorithms are usually encapsulated in libraries, and complex algorithms are often constructed using libraries of simpler ones. We present the first theorem that allows harnessing this structure to give compositional liveness proofs to concurrent algorithms and their clients. We show that, while proving a liveness property of a client using a concurrent library, we can soundly replace the library by another one related to the original library by a generalisation of a well-known notion of linearizability. We apply this result to show formally that lock-freedom, an often-used liveness property of non-blocking algorithms, is compositional for linearizable libraries, and provide an example illustrating our proof technique.

## 1 Introduction

Concurrent systems are usually expected to satisfy *liveness* properties [1], which, informally, guarantee that certain good events eventually happen. Reasoning about liveness in modern concurrent programs is difficult. Fortunately, the task can be simplified using reasoning methods that are able to exploit program structure. For example, concurrent algorithms are usually encapsulated in libraries and complex algorithms are often constructed using libraries of simpler ones. Thus, in reasoning about liveness of client code of a concurrent library, we would like to abstract from the details of a particular library implementation. This requires a notion of library abstraction that is able to specify the relevant liveness properties of the library.

Sound abstractions of concurrent libraries are commonly formalised by the notion of *linearizability* [10], which fixes a certain correspondence between the library and its abstract specification (the latter usually sequential, with its methods implemented atomically). However, linearizability is not suitable for liveness. It takes into account finite computations only and does not restrict the termination behaviour of library methods when relating them to methods of an abstract specification. As a result, the linearizing specification loses most of the liveness properties of the library. For example, no linearizing specifications can specify that library methods always terminate or a method meant to acquire a resource may not always return a value signifying that the resource is busy. In this paper we propose a generalisation of linearizability that lifts the above limitations and allows specifying such properties (§3).

Building on our generalized notion of linearizability, we present a theorem that allows giving liveness proofs to concurrent algorithms that are compositional in their structure (Theorem 4, §4). Namely, we show that, while proving a liveness property of

---

\* We would like to thank Anindya Banerjee, Aleks Nanevski, Matthew Parkinson and Viktor Vafeiadis for helpful comments and suggestions. Yang was supported by EPSRC.

a client of a concurrent library, we can soundly replace the library by a simpler one related to the original library by our generalisation of linearizability. To our knowledge, this is the first result, both for safety and liveness, that allows exploiting linearizability in verifying concurrent programs. In particular, it enables liveness-preserving *atomicity abstraction*. When proving a liveness property of a client using a concurrent library, we can replace the library by its atomic abstract specification, and prove the liveness of the client with respect to this specification instead.

We further show that we can use existing tools for proving classical linearizability (e.g., [15, 2]) to establish our generalisation. To this end, we identify a class of *linearization-closed* properties that, when satisfied by a library, are also satisfied by any other library linearizing it. This allows us to perform atomicity abstraction in two stages. We first use existing tools to establish the linearizability of a library to a coarse specification, sufficient only for proving safety properties of a client. We can then strengthen the specification for free with any linearization-closed liveness properties proved of the library implementation (Corollary 7, §5).

Finally, we demonstrate how our results can be used to give compositional proofs of *lock-freedom*, a liveness property often required of modern concurrent algorithms. In particular, we show that lock-freedom is a compositional property for linearizable libraries (Theorem 9, §6): when proving it of an algorithm using a linearizable lock-free library, we can replace library methods by their atomic always-terminating specifications. Our formalisation also highlights a (perhaps surprising) fact that compositionality does not hold for a variant of lock-freedom that assumes fair scheduling. We demonstrate the resulting proof technique on a non-blocking stack by Hendler et al. [8] (§7).

Proofs of our theorems can be found in § B and § C.

## 2 Preliminaries

**Programming language.** We consider a simple language for heap-manipulating concurrent programs, where a program consists of a library implementing several methods and its client, given by a parallel composition of threads. Let  $\text{Var}$  be a set of variables, ranged over by  $x, y, \dots$ , and  $\text{Method}$  a set of method names, ranged over by  $m$ . For simplicity, all methods take one argument. The syntax of the language is given below:

$$\begin{aligned} E & ::= \mathbb{Z} \mid x \mid E + E \mid -E \mid \dots & C & ::= c \mid m(E) \mid C; C \mid C + C \mid C^\circ \\ D & ::= C; \text{return}(E) & & \text{(where } C \text{ does not include method calls } m(E)) \\ A & ::= \{m = D, \dots, m = D\} \\ C(A) & ::= \text{let } A \text{ in } C \parallel \dots \parallel C & & \text{(where all the methods called are defined in } A) \end{aligned}$$

The language includes primitive commands  $c$ , method call  $m(E)$ , sequential composition  $C; C'$ , nondeterministic choice  $C + C'$ , and iteration  $C^\circ$ . We use a notation  $C^\circ$  here (instead of the usual Kleene star  $C^*$ ), so as to emphasise that  $C^\circ$  describes not just finite, but also infinite iterations of  $C$ . Both primitive commands and method calls  $m(E)$  are assumed atomic. The primitive commands form the set  $\text{PComm}$ , and they include standard instructions, such as skip, variable assignment  $x = E$ , the update  $[E] = E'$  of the heap cell  $E$  by  $E'$ , the read  $x = [E]$  of the heap cell  $E$  into the variable  $x$ , and the assume statement  $\text{assume}(E)$ , filtering out states making  $E = 0$ . We point out that the standard constructs, such as loops and conditionals, can be defined in our language as syntactic sugar, with conditions translated using  $\text{assume}$  (see also §A).

Let us fix a program  $C(A) = \text{let } A \text{ in } C_1 \parallel \dots \parallel C_n$  with the library definition  $A = \{m = D_m \mid m \in M\}$ . We let the signature of the library  $A$  be the set of the implemented methods:  $\text{sig}(A) = M$ . In the following we index threads in programs using the set of identifiers  $\text{ThreadID} = \mathbb{N}$ .

We restrict programs to ensure that the state of the client is disjoint from that of the library, and that this state separation is respected by client operations and library routines. We note that this restriction is assumed by the standard notion of linearizability [10]; we intend to relax it in our future work. Technically, we assume  $\text{PComm} = \text{ClientPComm} \uplus \text{LibPComm}$  for some sets  $\text{ClientPComm}$  and  $\text{LibPComm}$  and require that all primitive commands in the client be from  $\text{ClientPComm}$  and those in the library from  $\text{LibPComm}$ . As formalised below, the commands in  $\text{ClientPComm}$  and  $\text{LibPComm}$  can access only variables and heap locations belonging to the client and the library, respectively.

We also assume special variables  $\text{retval}_t \in \text{Var}$  for each thread  $t$  and  $\text{param} \in \text{Var}$ . The variable  $\text{retval}_t$  contains the result of the most recent method call by thread  $t$  and is implicitly updated by the return command. No commands in the program are allowed to modify  $\text{retval}_t$  explicitly, and the variable can only be read by  $C_t$ . The variable  $\text{param}$  keeps the values of parameters passed upon method calls and is implicitly updated by the call command. We assume that the variables occurring in the expression  $E$  of a call command  $m(E)$  are accessed only by the thread executing the command.

**State model.** Let  $\text{CLoc}$  and  $\text{LLoc}$  be disjoint sets representing heap locations that belong to the address spaces of the client and the library, respectively. We also assume  $\text{Var} = \text{CVar} \uplus \text{LVar}$  for some sets  $\text{CVar}$  and  $\text{LVar}$  representing variables that belong to the client and the library, respectively. Let  $\text{param} \in \text{LVar}$  and  $\text{retval}_t \in \text{CVar}$ ,  $t = 1..n$ . We then define the set of program states  $\text{State}$  as follows:

$$\begin{aligned} \text{Loc} &= \text{CLoc} \uplus \text{LLoc} & \text{Val} &= \mathbb{Z} \uplus \text{Loc} \\ \text{Stack} &= \text{Var} \rightarrow \text{Val} & \text{Heap} &= \text{Loc} \rightarrow \text{Val} & \text{State} &= \text{Stack} \times \text{Heap} \end{aligned}$$

A state in this model consists of a stack and a heap, both of which are total maps from variables or locations to values. Every location or variable is owned either by the library or by the client. We make this ownership explicit by defining two sets,  $\text{CState}$  for client states and  $\text{LState}$  for library states:  $\text{CState} = (\text{CVar} \rightarrow \text{Val}) \times (\text{CLoc} \rightarrow \text{Val})$  and  $\text{LState} = (\text{LVar} \rightarrow \text{Val}) \times (\text{LLoc} \rightarrow \text{Val})$ . Also, we define three operations relating these sets to  $\text{State}$ :  $\text{client} : \text{State} \rightarrow \text{CState}$ ,  $\text{lib} : \text{State} \rightarrow \text{LState}$  and  $\circ : \text{CState} \times \text{LState} \rightarrow \text{State}$ . The first two project states to client and library states by restricting the domains of the stack and the heap: e.g., for  $(s, h) \in \text{State}$  we have  $\text{lib}(s, h) = (s|_{\text{LVar}}, h|_{\text{LLoc}})$ . The  $\circ$  operator combines client and library states into program states:  $(s_1, h_1) \circ (s_2, h_2) = (s_1 \uplus s_2, h_1 \uplus h_2)$ . We lift  $\circ$  to sets of states pointwise.

**Control-flow graphs.** In the definition of program semantics, it is technically convenient for us to abstract from a particular syntax of programming language and represent commands by their *control-flow graphs*. A control-flow graph (CFG) is a tuple  $(N, T, \text{start}, \text{end})$ , consisting of the set of program positions  $N$ , the control-flow relation  $T \subseteq N \times \text{Comm} \times N$ , and the initial and final positions  $\text{start}, \text{end} \in N$ . The edges are annotated with commands from  $\text{Comm}$ , which are primitive commands, calls  $m(E)$  or returns  $\text{return}(E)$ . Every command  $C$  in our language can be translated to a CFG in a standard manner (§A). Hence, we can represent a program  $C(A)$  by a collection of CFGs: the client command  $C_t$  for a thread  $t$  is represented by  $(N_t, T_t, \text{start}_t, \text{end}_t)$ , and

the body  $D_m$  of a method  $m$  by  $(N_m, T_m, \text{start}_m, \text{end}_m)$ . We often view this collection of CFGs for  $C(A)$  as a single graph consisting of two node sets  $\text{CNode} = \biguplus_{t=1}^n N_t$  and  $\text{LNode} = \biguplus_{m \in \text{sig}(A)} N_m$ , and the edge set  $T = \biguplus_{t=1}^n T_t \uplus \biguplus_{m \in \text{sig}(A)} T_m$ . Finally, we define  $\text{method} : \text{LNode} \rightarrow M$  as follows:  $\text{method}(v) = m$  if and only if  $v \in N_m$ .

**Program semantics.** Programs in our semantics denote sets of *traces*, which are finite or infinite sequences of actions of the form

$$\varphi \in \text{Act} ::= (t, \text{Client}(c)) \mid (t, \text{Lib}(c)) \mid (t, \text{call } m(k)) \mid (t, \text{ret } m(k))$$

where  $t \in \text{ThreadID}$ ,  $c \in \text{PComm}$ ,  $k \in \text{Val}$  and  $m \in \text{Method}$ . Each action corresponds to a primitive command  $c$  executed by the client or the library (in which case we tag  $c$  with *Client* or *Lib*), a call to or a return from the library. We denote the sets of each kind of actions with *ClientAct*, *LibAct*, *CallAct* and *RetAct*, respectively, and let  $\text{CallRetAct} = \text{CallAct} \cup \text{RetAct}$ . Also, we write *Trace* for the set of all traces and adopt the standard notation:  $\varepsilon$  is the empty trace,  $\tau(i)$  is the  $i$ -th action in the trace  $\tau$ , and  $|\tau|$  is the length of the trace  $\tau$  ( $|\tau| = \omega$  if  $\tau$  is infinite).

Our semantics assumes an interpretation of every primitive command  $c$  as a transformer  $f_c$  of type  $\text{LState} \rightarrow \mathcal{P}(\text{LState})$ , if  $c \in \text{LibPComm}$ , or of type  $\text{CState} \rightarrow \mathcal{P}(\text{CState})$ , if  $c \in \text{ClientPComm}$ . In both cases, we lift it to a function  $f_c : \text{State} \rightarrow \mathcal{P}(\text{State})$  by transforming only the client or the library part of the input state:

$$\forall \theta \in \text{State}. f_c(\theta) \stackrel{\text{def}}{=} \begin{cases} \{\text{client}(\theta)\} \circ f_c(\text{lib}(\theta)), & \text{if } c \in \text{LibPComm}; \\ f_c(\text{client}(\theta)) \circ \{\text{lib}(\theta)\}, & \text{if } c \in \text{ClientPComm}. \end{cases}$$

For the transformers of sample primitive commands see §A.

Let the set of *thread positions* be defined as follows:  $\text{Pos} = \text{CNode} \cup (\text{Val} \times \text{CNode} \times \text{LNode})$ . Elements in *Pos* describe the runtime status of a thread. A node  $v \in \text{CNode}$  indicates that the thread is about to execute the client code coming right after the node  $v$  in its CFG. A triple  $\langle u, v, v' \rangle$  means that the thread is at the program point  $v'$  in the code of a library method,  $u$  is the current value of the param variable for this method and  $v$  the return program point in the client code.

The semantics of the program  $C(A)$  with threads  $\{1, \dots, n\}$  is defined using a transition relation  $\longrightarrow_{C(A)} : \text{Config} \times \text{Act} \times \text{Config}$ , which transforms program configurations  $\text{Config} = (\{1, \dots, n\} \rightarrow \text{Pos}) \times \text{State}$ . The configurations are pairs of program counters and states, where a program counter defines the position of each thread in the program. The relation is defined by the rules in Figure 1. Note that, upon a method call, the actual parameter and the return point are saved as components in the new program position, and the method starts executing from the corresponding starting node of its CFG. The saved actual parameter is accessed whenever the library code reads the variable *param*, as modelled in the third rule for the library action. Upon a return, the return point is read from the current program counter, and the return value is written into the  $\text{retval}_t$  variable for the thread  $t$  executing the return command.

Our operational semantics induces a trace interpretation of programs  $C(A)$ . For a finite trace  $\tau$  and  $\sigma, \sigma' \in \text{Config}$  we write  $\sigma \xrightarrow{\tau}_{C(A)}^* \sigma'$  if there exists a corresponding derivation of  $\tau$  using  $\longrightarrow$ . Similarly, for an infinite trace  $\tau$  and  $\sigma \in \text{Config}$  we write  $\sigma \xrightarrow{\tau}_{C(A)}^\omega$  to mean the existence of infinite  $\tau$ -labelled computation from  $\sigma$  according to our semantics. Let us denote with  $\text{pc}_0$  the initial program counter  $[1 : \text{start}_1, \dots, n : \text{start}_n]$ . The trace semantics of  $C(A)$  is defined as follows:

$$\llbracket C(A) \rrbracket = \{\tau \mid \exists \theta \in \text{State}. (\text{pc}_0, \theta) \xrightarrow{\tau}_{C(A)}^\omega \vee \exists \sigma \in \text{Config}. (\text{pc}_0, \theta) \xrightarrow{\tau}_{C(A)}^* \sigma\}.$$

$$\begin{array}{c}
\frac{(v, c, v') \in T \quad \theta' \in f_c(\theta)}{\text{pc}[t : v], \theta \xrightarrow{(t, \text{Client}(c))}_{C(A)} \text{pc}[t : v'], \theta'} \quad \frac{(v, m(E), v') \in T \quad \llbracket E \rrbracket s = u}{\text{pc}[t : v], \theta \xrightarrow{(t, \text{call } m(u))}_{C(A)} \text{pc}[t : \langle u, v', \text{start}_m \rangle], \theta} \\
\frac{(v, c, v') \in T \quad (s', h') \in f_c(s[\text{param} : u], h)}{\text{pc}[t : \langle u, v_0, v \rangle], (s, h) \xrightarrow{(t, \text{Lib}(c))}_{C(A)} \text{pc}[t : \langle s'(\text{param}), v_0, v' \rangle], (s', h')} \\
\frac{(v, \text{return}(E), v') \in T \quad \llbracket E \rrbracket (s[\text{param} : u]) = u'}{\text{pc}[t : \langle u, v_0, v \rangle], (s, h) \xrightarrow{(t, \text{ret } (\text{method}(v))(u'))}_{C(A)} \text{pc}[t : v_0], (s[\text{retval}_t : u'], h)}
\end{array}$$

**Fig. 1.** Operational semantics of programs.  $\llbracket E \rrbracket s \in \text{Val}$  is the value of the expression  $E$  in the stack  $s$ . We denote with  $g[x : y]$  the function that has the same value as  $g$  everywhere except  $x$ , where it has the value  $y$ . We remind the reader that  $T$  is the control-flow relation of  $C(A)$ .

Note that  $\llbracket C(A) \rrbracket$  includes all finite or infinite traces (including non-maximal ones).

**Client and library traces.** In this paper we consider two special kinds of traces: *client traces*, which include only actions from  $\text{CallRetAct} \cup \text{ClientAct}$ , and *library traces*, which include only actions from  $\text{CallRetAct} \cup \text{LibAct}$ . Given a trace  $\tau \in \text{Trace}$ , we can obtain the corresponding client  $\text{client}(\tau)$  and library  $\text{lib}(\tau)$  traces by projecting  $\tau$  to the appropriate subsets of actions. We consider two further projections:  $\text{visible}(\tau)$  projects  $\tau$  to actions in  $\text{ClientAct}$ , and  $\tau|_t$  to actions of thread  $t$ . We let  $\text{CTrace}$  be the set of all client traces and  $\text{LTrace}$  the set of all library traces.

**Histories.** We record interactions between the client and the library using *histories*, which are sequences of actions from  $\text{CallRetAct} \cup \text{BlockAct}$ , where  $\text{BlockAct} = \{(t, \text{starve}) \mid t \in \text{ThreadID}\}$ . An action  $(t, \text{starve})$  means that thread  $t$  is suspended by the scheduler and is never scheduled again (is ‘starved’). We record  $\text{starve}$  events because the liveness properties we are dealing with in this paper, such as lock-freedom (§6), need to distinguish between method non-termination due to divergence and the one due to being starved by the scheduler. Let  $\text{History}$  be the set of all histories.

Given a trace  $\tau \in \text{Trace}$ , we can construct a corresponding history  $\text{history}(\tau)$  in two steps. First, for every thread  $t$ , if the last action of the thread in  $\tau$  exists and is an action in  $\text{CallAct} \cup \text{LibAct}$ , we insert  $(t, \text{starve})$  right after this action in  $\tau$ , obtaining a sequence of actions  $\tau'$ . The history  $\text{history}(\tau)$  is then obtained by projecting  $\tau'$  to actions in  $\text{CallRetAct} \cup \text{BlockAct}$ .

### 3 Concurrent Library Semantics and Linearizability

The correctness of concurrent libraries is usually defined using the notion of linearizability [10], which fixes a particular correspondence between the implementation and the specification of a library. We now define an analogue of this notion in our setting.

**Definition 1.** *The linearizability relation is a binary relation  $\sqsubseteq$  on histories defined as follows:  $H \sqsubseteq H'$  if  $\forall t \in \text{ThreadID}. H|_t = H'|_t$  and there is a bijection  $\pi : \{1, \dots, |H|\} \rightarrow \{1, \dots, |H'|\}$  such that  $\forall i. H(i) = H'(\pi(i))$  and*

$$\forall i, j. (i < j \wedge H(i) \in \text{RetAct} \wedge H(j) \in \text{CallAct}) \Rightarrow \pi(i) < \pi(j).$$

That is, the history  $H'$  linearizes the history  $H$  when it is a permutation of the latter preserving the order of actions within threads and non-overlapping method invocations. The duration of a method invocation is defined by the interval from the method call action to the corresponding return action (or to infinity if there is none). Our definition allows  $H$  and  $H'$  to be infinite, in contrast to the standard notion of linearizability which considers only finite histories (we provide a more detailed comparison below).

To check if one library linearizes another, we need to define the set of histories a library can generate. We do this using the *most general client* of the library. As we show in Lemma 10(1), §B, the client we define here is indeed most general in the sense that its semantics includes all library behaviours generated by any other client in our programming language. Formally, consider a library  $A = \{m = D_m \mid m \in M\}$ . For a given  $n$ , the most general client  $\text{MGC}_n(A)$  is the combination of CFGs for the library  $A$  and those for the client with  $n$  threads that repeatedly invoke library methods in any order and with all possible parameters: the CFG for thread  $t$  is  $(N_t, T_t, v_{\text{mgc}}^t, v_{\text{mgc}}^t)$  with  $N_t = \{v_{\text{mgc}}^t\}$  and  $T_t = \{(v_{\text{mgc}}^t, m(u), v_{\text{mgc}}^t) \mid m \in \text{sig}(A), u \in \text{Val}\}$ . One can understand  $\text{MGC}_n(A)$  as “let  $A$  in  $C_{\text{mgc}}^1 \parallel \dots \parallel C_{\text{mgc}}^n$ ” where  $C_{\text{mgc}}^t$  repeatedly makes all possible method calls. Let  $N_{\text{mgc}} = \bigsqcup_{t=1}^n N_t$ .

We define the denotation of  $\text{MGC}_n(A)$  in a *library-local semantics*, where the program executes only on the library part of state. Namely, we consider a relation  $\rightarrow_{\text{MGC}_n(A)}: \text{LConfig} \times \text{Act} \times \text{LConfig}$  transforming configurations  $\text{LConfig} = (\{1, \dots, n\} \rightarrow \text{LPos}) \times \text{LState}$ , where  $\text{LPos} = N_{\text{mgc}} \cup (\text{Val} \times N_{\text{mgc}} \times \text{LNode})$ . The relation is defined as in Figure 1, but with the rule for return commands replaced by the one that does not write the return value into  $\text{retval}_t$  (since this variable is not part of library states in  $\text{LState}$ ):

$$\frac{(v, \text{return}(E), v') \in T \quad \llbracket E \rrbracket(s[\text{param} : u]) = u'}{\text{pc}[t : \langle u, v_0, v \rangle], (s, h) \xrightarrow{(t, \text{ret}(\text{method}(v))(u'))}_{\text{MGC}_n(A)} \text{pc}[t : v_0], (s, h)}$$

Let  $\llbracket \text{MGC}_n(A) \rrbracket_{\text{lib}} \subseteq \text{LTrace}$  be the set of all traces generated by the program  $\text{MGC}_n(A)$  in this semantics from any initial state in  $\text{LState}$ . We then define the set of all possible behaviours of the library  $A$  as the set of its traces  $\llbracket A \rrbracket = \bigcup_{n \geq 1} \llbracket \text{MGC}_n(A) \rrbracket_{\text{lib}}$ . This lets us lift the notion of linearizability to libraries as follows.

**Definition 2.** For libraries  $A_1$  and  $A_2$  with  $\text{sig}(A_1) = \text{sig}(A_2)$  we say that  $A_2$  *linearizes*  $A_1$ , written  $A_1 \sqsubseteq A_2$ , if  $\forall H_1 \in \text{history}(\llbracket A_1 \rrbracket), \exists H_2 \in \text{history}(\llbracket A_2 \rrbracket), H_1 \sqsubseteq H_2$ .

Thus,  $A_2$  linearizes  $A_1$  if every behaviour of the latter under the most general client may be reproduced in a linearized form by the former.

It is instructive to compare our definition of linearizability with the classical one [10]. The original definition of linearizability between an implementation  $A_1$  of a concurrent library and its specification  $A_2$  considers only finite histories without starve actions. It assumes that the specification  $A_2$  is sequential, meaning that every method in it is implemented by an atomic terminating command. To deal with non-terminating method calls in  $A_1$  when comparing the sets of histories generated by the two libraries, the original definition *completes* the histories of  $A_1$  before the comparison: for every call action in the history without a corresponding return action, either the action is discarded or a corresponding return action with an arbitrary return value is added in the history. Such an arbitrary completion of pending calls does not allow making any statements about the termination behaviour of the library in its specification. Furthermore,

the fact that the definition considers only finite histories makes it impossible to specify trace-based liveness properties satisfied by the library, e.g., that a method meant to acquire a resource may not always return a value signifying that the resource is busy.

Our definition lifts these limitations in a bid to enable compositional reasoning about liveness properties of concurrent libraries. Definitions 1 and 2 take into account infinite computations and do not require the specification  $A_2$  to be sequential. Thus, they allow method calls in  $A_2$  to diverge and the execution of such methods to overlap with the executions of others. Our definitions require any method divergence in the implementation to be reproducible in the specification. As we show in §5, by restricting the set of histories of the specification with fairness constraints, we can specify trace-based liveness properties. As we discuss in §8, our definition is more flexible than previous attempts at generalising linearizability to deal with method non-termination.

The classical notion of linearizability can also be expressed in our setting. We use this in §5 to harness existing linearizability checkers in reasoning about liveness properties. The linearizability of concurrent libraries according to the classical definition can be established using several logics and tools, e.g., based on separation logic [15, 14] or TVLA [2]. These logics and tools reduce showing linearizability to proving an invariant relating the states of the implementation and the sequential specification. They establish the validity of the invariant both on finite and infinite computations. Hence, it can be shown that they also establish linearizability in the sense of Definition 1. More precisely, assume a specification of the effect of every method  $m$  in a library  $A_1$  given as a command  $c_m; \text{return}(E_m)$  for some  $c_m \in \text{PComm}$ . Then the tools in [15, 14, 2] establish  $A_1 \sqsubseteq A_2$ , where  $A_2 = \{m = (\text{skip}^\circ; c_m; \text{skip}^\circ; \text{return}(E_m)) \mid m \in \text{sig}(A_1)\}$ . It is easy to show that this linearizability relation, when restricted to finite histories, is equivalent to the classical notion of linearizability [10].

Since the classical notion of linearizability does not specify the termination behaviour of the library, methods in the library  $A_2$  above may diverge. The divergence can happen either before the method makes a change to the library state using  $c_m$  or after, as modelled by the two  $\text{skip}^\circ$  statements. In fact, both of these cases are exhibited by practical concurrent algorithms. For example, the classical Treiber’s stack [13] and its variations [8] do not modify the state in the case of divergence, but Harris’s non-blocking linked list [7] does. History completion in the classical definition of linearizability corresponds to divergence at one of the  $\text{skip}^\circ$  statements in our formalisation: discarding a pending call models the divergence at the first one, and completing a pending call with an arbitrary return the divergence at the second. We are able to express the classical notion of linearizability in a uniform way because the specification  $A_2$  above is not sequential. Namely, we allow non-terminating method invocations to overlap with others in the specification and, hence, do not need to complete them.

## 4 Atomicity Abstraction

We now show how our notion of linearizability can be used to abstract an implementation of a library while reasoning about liveness properties of its client. Namely, we prove that replacing a library used by a client with its linearization leaves all the original client behaviours reproducible modulo the following notion of trace equivalence:

**Definition 3.** *Client traces  $\tau, \tau' \in \text{CTrace}$  are **equivalent**, written  $\tau \sim \tau'$ , if  $\forall t \in \text{ThreadID}. \tau|_t = \tau'|_t$  and there exists a bijection  $\pi : \{1, \dots, |\tau|\} \rightarrow \{1, \dots, |\tau'|\}$  such*

that  $\forall i. \tau(i) = \tau'(\pi(i))$  and

$$\forall i, j. (i < j \wedge \tau(i), \tau(j) \in \text{ClientAct}) \Rightarrow \pi(i) < \pi(j)$$

Two traces are equivalent if they are permutations of each other preserving the order of actions within threads and all client actions. Note that  $\text{visible}(\tau) = \text{visible}(\tau')$  when  $\tau \sim \tau'$ . Hence, trace equivalence preserves any linear-time temporal property over trace projections to client actions. The following theorem states the desired abstraction result.

**Theorem 4 (Abstraction).** *Consider  $C(A_1)$  and  $C(A_2)$  such that  $A_1 \sqsubseteq A_2$ . Then*

$$\forall \tau_1 \in \llbracket C(A_1) \rrbracket. \exists \tau_2 \in \llbracket C(A_2) \rrbracket. \text{client}(\tau_1) \sim \text{client}(\tau_2) \wedge \text{history}(\tau_1) \sqsubseteq \text{history}(\tau_2).$$

**Corollary 5.** *If  $A_1 \sqsubseteq A_2$ , then  $\text{visible}(\llbracket C(A_1) \rrbracket) \subseteq \text{visible}(\llbracket C(A_2) \rrbracket)$ .*

According to Corollary 5, while reasoning about a client  $C(A_1)$  of a library  $A_1$ , we can soundly replace  $A_1$  with a simpler library  $A_2$  linearizing  $A_1$ : if a linear-time liveness property over client actions holds over  $C(A_2)$ , it will also hold over  $C(A_1)$ . In practice, we are usually interested in **atomicity abstraction** (see, e.g., [11]), a special case of the above transformation when methods in  $A_2$  are implemented using atomic commands. In §6 we apply this technique to proving liveness properties of modern concurrent algorithms. Before this, however, we need to explain how to establish the required linearizability relation  $A_1 \sqsubseteq A_2$ . This is the subject of the next section.

## 5 Linearization-Closed Properties

As we explained in §3, existing tools can only prove linearizability relations  $A_1 \sqsubseteq A_2$  such that  $A_2$  has the form  $\{m = (\text{skip}^\circ; c_m; \text{skip}^\circ; \text{return}(E_m)) \mid m \in \text{sig}(A_1)\}$  for some atomic commands  $c_m$  and expressions  $E_m$ . The specification  $A_2$  of the library  $A_1$  is too coarse to prove a non-trivial liveness property of a client, as it allows methods to diverge and does not permit specifying liveness properties. If the library  $A_1$  satisfies some liveness property (e.g., its method invocations not starved by the scheduler always terminate), we would like to carry it over to  $A_2$  to use in the proof of the client. This is, in fact, possible for a certain class of properties.

**Definition 6.** *A property  $P \subseteq \text{History}$  over histories is **linearization-closed** if  $\forall H, H'. (H \in P \wedge H \sqsubseteq H') \Rightarrow H' \in P$ .*

Intuitively, linearization-closed properties should be formulated in terms of pairs of call and return actions and not in terms of individual actions, as the latter can be rearranged during linearization. For example, the property “methods that are not starved by the scheduler always terminate” is linearization-closed. In contrast, the property “a  $(t, \text{ret } m(0))$  action is always followed by a  $(t', \text{ret } m(1))$  action” is not.

**Corollary 7.** *Let  $P \subseteq \text{History}$  be linearization-closed,  $A_1 \sqsubseteq A_2$ , and  $\text{history}(\llbracket A_1 \rrbracket) \subseteq P$ . Then  $\text{visible}(\llbracket C(A_1) \rrbracket) \subseteq \text{visible}(\llbracket C(A_2) \rrbracket) \cap \{\tau \mid \text{history}(\tau) \in P\}$ .*

This corollary of Theorem 4, improving on Corollary 5, allows us to perform atomicity abstraction in two stages. We start with the coarse refinement  $A_1 \sqsubseteq A_2$  established by tools for classical linearizability. If a liveness property  $P$  over histories holds of the implementation  $A_1$  and is linearization-closed, the trace set of the specification  $A_2$  can

be shrunk by removing those violating  $P$ . To convert  $C(A_2)$  into a program with the trace set  $\llbracket C(A_2) \rrbracket \cap \{\tau \mid \text{history}(\tau) \in P\}$  we can use standard automata-theoretic techniques from model checking: we represent  $P$  by an automaton and construct a synchronous product of  $C(A_2)$  and the automaton. See [16, 4, 6] for more details.

## 6 Compositional Liveness Proofs for Concurrent Algorithms

**Lock-freedom.** We now illustrate how Corollary 7 can be used to perform compositional proofs of liveness properties of *non-blocking* concurrent algorithms [9]. These complicated algorithms employ synchronisation techniques alternative to the usual lock-based mutual exclusion and typically provide high-performance concurrent implementations of data structures, such as stacks, queues, linked lists and hash tables (see, for example, the `java.util.concurrent` library).

Out of all properties used to formulate progress guarantees for such algorithms, we concentrate on *lock-freedom*, as the one most often used and most difficult to prove. Informally, an algorithm implementing operations on a concurrent data structure is considered lock-free if from any point in a program’s execution, some thread is guaranteed to complete its operation. Thus, lock-freedom ensures the absence of livelock, but not starvation. The formal definition is as follows.

**Definition 8.** *A library  $A$  is **lock-free** if for any  $t \in \text{ThreadID}$ , the set of its histories  $\text{history}(\llbracket A \rrbracket)$  satisfies  $\text{LF} = \Box \Diamond (\_, \text{ret } \_) \vee \Box ((t, \text{call } \_) \Rightarrow \Diamond ((t, \text{starve}) \vee (t, \text{ret } \_)))$ .*

Here we use linear temporal logic (LTL) over histories, with predicates over actions as atomic propositions;  $\Box$  and  $\Diamond$  are the standard operators “always” and “eventually” and  $\_$  stands for an irrelevant existentially quantified value. The property formalises the informal condition that some operation always complete by requiring that either some operation return infinitely often (for the case when the client calls infinitely many operations), or every operation that has not been starved by the scheduler return (for the case when the client calls only finitely many operations).

Note that the semantics of §2 allows for unfair schedulers that starve some threads. A crucial requirement in the definition of lock-freedom is that the property has to be satisfied under such schedulers: the threads that do get scheduled have to make progress even if others are starved. In Definition 8 we formalise it using starve actions.

**Example.** Consider the algorithm in Figure 2, ignoring the `elim` function and calls to it for now. For readability, the example is presented in C, rather than in our minimalistic language. It is a simple non-blocking implementation of a concurrent stack due to Treiber [13]. A client using the implementation can call several `push` or `pop` operations concurrently. To ensure the correctness of the algorithm, we assume that `pop` does not reclaim the memory taken by the deleted node [9]. The stack is stored as a linked list, and is updated by compare-and-swap (CAS) instructions. CAS takes three arguments: a memory address `addr`, an expected value `v1`, and a new value `v2`. It atomically reads the memory address and updates it with the new value when the address contains the expected value; otherwise, it does nothing. In C syntax this might be written as follows:

```
atomic { if (*addr==v1) {*addr=v2; return 1;} else {return 0;} }
```

In most architectures an efficient CAS (or an equivalent operation) is provided natively by the processor. The operations on the stack are implemented as follows. The function

```

struct Node {
    value_t data;
    Node *next;
};
Node *S;
int collision[SIZE];

void init() { S = NULL; }
void push(value_t v) {
    Node *t, *x;
    x = new Node();
    x->data = v;
    while (1) {
        t = S; x->next = t;
        if (CAS(&S,t,x)) return;
        elim(); } }

void elim() { // Elimination scheme
    // ...
    int pos = GetPos(); // 0 ≤ pos ≤ SIZE-1
    int hisId = collision[pos];
    while (!CAS(&collision[pos],hisId,MYID))
        hisId = collision[pos];
    // ...
}

value_t pop() {
    Node *t, *x;
    while (1) {
        t = S;
        if (t == NULL) return EMPTY;
        x = t->next;
        if (CAS(&S,t,x)) return t->data;
        elim(); } }

```

**Fig. 2.** A non-blocking stack implementation

init initialises the data structure. The push operation (i) allocates a new node x; (ii) reads the current value of the top-of-the-stack pointer S; (iii) makes the next field of the newly created node point to the read value of S; and (iv) atomically updates the top-of-the-stack pointer with the new value x. If the pointer has changed between (ii) and (iv) and has not been restored to its initial value, the CAS fails and the operation is restarted. The pop operation is implemented in a similar way.

Note that a push or pop operation of Treiber's stack may diverge if other threads are continually modifying S: in this case the CAS instruction may always fail, which will cause the operation to restart continually. However, the algorithm is lock-free: if push and pop execute concurrently, some operation will always terminate.

Lock-freedom of some algorithms, including Treiber's stack, can be proved automatically [6].

**Compositionality of lock-freedom.** It is easy to check that the property LF in Definition 8 is linearization-closed. Thus, if  $A$  is a lock-free library and is linearized by a specification  $\{m = (\text{skip}^\circ; c_m; \text{skip}^\circ; \text{return}(E_m)) \mid m \in \text{sig}(A)\}$ , proving a liveness property of a client of  $A$  can be simplified if we replace  $A$  by the specification and consider only traces  $\tau$  of the client such that  $\text{history}(\tau)$  satisfies LF. As we now show, in the case when the client is itself a concurrent algorithm being proved lock-free, we can strengthen this result: we can assume a specification of  $A$  where every method terminates in all cases. We thus prove that lock-freedom is a compositional property of linearizable libraries.

To simplify presentation, we have not considered nested libraries, which makes the direct formulation of this result impossible. Instead, we rely on the reduction in [6], which says that an algorithm is lock-free if and only if any number of its operations running in parallel do not have infinite traces, i.e., terminate if not starved. Thus, it suffices to prove the result for the termination of the client.

**Theorem 9.** *Let  $M$  be a set of method names. Consider libraries*

$$\begin{aligned}
 A_1 &= \{m = D_m \mid m \in M\}, & A_2 &= \{m = (c_m; \text{return}(E_m)) \mid m \in M\}, \\
 A_3 &= \{m = (\text{skip}^\circ; c_m; \text{skip}^\circ; \text{return}(E_m)) \mid m \in M\},
 \end{aligned}$$

where  $c_m$  are atomic commands,  $A_1$  is lock-free, and  $A_1 \sqsubseteq A_3$ . If  $\llbracket C(A_2) \rrbracket$  does not have infinite traces, then neither does  $\llbracket C(A_1) \rrbracket$ .

Given the above reduction, the theorem implies that a concurrent algorithm using  $A_1$  is lock-free if it is lock-free when it uses  $A_2$  instead.

We note that some concurrent algorithms rely on locks, while satisfying lock-freedom under the assumption that the scheduler is fair [9]. Perhaps surprisingly, Theorem 9 does not hold in this case: lock-freedom under fair scheduling is not a compositional property. The intuitive reason is as follows: we can replace  $A_3$  with  $A_2$  in Theorem 9 because the effect of operations of  $A_3$  diverging at one of the  $\text{skip}^\circ$  statements is already covered by the possible unfairness of the scheduler. This reasoning becomes invalid once the scheduler is fair. We provide a counterexample in §C.

## 7 Example

Theorem 9 allows giving proofs of lock-freedom to non-blocking concurrent algorithms that are compositional in the structure of the algorithms, as we now illustrate. As an example, we consider an improvement of Treiber’s stack proposed by Hendler, Shavit, and Yerushalmi (HSY), which performs better in the case of higher contention among threads [8]. Figure 2 shows an adapted and abridged version of the algorithm. The implementation combines Treiber’s stack with a so-called elimination scheme, implemented by the function `elim` (partially elided). A push or a pop operation first tries to modify the stack as in Treiber’s algorithm, by doing a CAS to change the shared top-of-the-stack pointer. If the CAS succeeds, the operation terminates. If the CAS fails (because of interference from another thread), the operation backs off to the elimination scheme. If this scheme fails, the whole operation is restarted.

The elimination scheme works on data structures that are separate from the list implementing the stack and, hence, can be considered as a library used by the HSY stack with the only method `elim`. The idea behind the scheme is that two contending push and pop operations can eliminate each other without modifying the stack if pop returns the value that push is trying to insert. An operation determines the existence of another operation it could eliminate itself with by selecting a random slot `pos` in the `collision` array, and atomically reading that slot and overwriting it with its thread identifier `MYID`. The algorithm implements the atomic read-and-write operation on the `collision` array in a lock-free fashion using CAS. The identifier of another thread read from the array can be subsequently used to perform elimination. The corresponding code does not affect the lock-freedom of the algorithm and is elided in Figure 2.

According to Theorem 9, to prove the lock-freedom of the HSY stack, it is sufficient to prove (i) the lock-freedom of the push and pop with a call to `elim` replaced by its atomic always-terminating specification; and (ii) the lock-freedom and linearizability of the `elim` method. The former is virtually identical to the proof of lock-freedom of Treiber’s stack, since `elim` acts on data structures disjoint from those of the stack. Informally, this proof is done as follows (see [6] for a detailed formal proof). It is sufficient to check the termination of the program consisting of a parallel composition of an arbitrary number of threads each executing one push or pop operation. For such a program, we have two facts. First, no thread executes a successful CAS in push or pop infinitely often. This is because once the CAS succeeds, the corresponding while-loop

terminates. Second, the while-loop in an operation terminates if no other thread executes a successful CAS in push or pop infinitely often. This is because the operation does not terminate only when its CAS always fails, which requires the other threads to execute the CASes infinitely often. From these two facts, the termination of each thread follows.

The lock-freedom of the `elim` method can be proved in the same way and its linearizability can be proved using existing methods [14, 15]. This completes the proof of lock-freedom of the HSY stack. We have thus decomposed the proof of a complicated non-blocking algorithm with two nested loops into proofs of two simple algorithms.

## 8 Related Work

Filipović et al. [5] have previously characterised linearizability in terms of observational refinement (technically, their result is similar to our Lemma 11, §B). They did not consider infinite computations and treated non-terminating methods approximately; thus, they could not handle liveness properties. Besides, the work of Filipović et al. did not justify any compositional proof methods, as we have done in Theorem 4.

Petrank et al. [12] were the first to observe that lock-freedom is compositional, as we prove in Theorem 9. However, their formulation and ‘proof’ of this property are presented as a piece of informal text talking about artefacts without a clear semantics. As a consequence, their compositionality theorem misses an important requirement that library methods be linearizable.

Burckhardt et al. [3] have attempted to generalise linearizability on finite histories to the case of non-terminating method calls. However, their definition is too restrictive, as it requires any non-termination in the library implementation to be reproducible in the *sequential* specification of the library. This requirement is not satisfied on infinite traces by common lock-free algorithms, where some methods may diverge while others make progress. Additionally, their definition considers any library where methods may modify the library state before diverging (e.g., [7]) as non-linearizable. We provide a more flexible definition.

Atomicity refinement is a well-known method for formal development of concurrent programs [11], which allows refining an atomic specification to a concurrent implementation. As atomicity refinement and abstractions are duals of each other, our results can also be used in the context of formal program development.

## References

1. B. Alpern and F. B. Schneider. Defining liveness. *Inf. Process. Lett.*, 21(4), 1985.
2. D. Amit, N. Rinetzky, T. W. Reps, M. Sagiv, and E. Yahav. Comparison under abstraction for verifying linearizability. In *CAV*, 2007.
3. S. Burckhardt, C. Dern, M. Musuvathi, and R. Tan. Line-up: A complete and automatic linearizability checker. In *PLDI*, 2010.
4. B. Cook, A. Gotsman, A. Podelski, A. Rybalchenko, and M. Y. Vardi. Proving that programs eventually do something good. In *POPL*, 2007.
5. I. Filipović, P. O’Hearn, N. Rinetzky, and H. Yang. Abstraction for concurrent objects. In *ESOP*, 2009.
6. A. Gotsman, B. Cook, M. Parkinson, and V. Vafeiadis. Proving that non-blocking algorithms don’t block. In *POPL*, 2009.

7. T. Harris. A pragmatic implementation of non-blocking linked lists. In *DISC*, 2001.
8. D. Hendler, N. Shavit, and L. Yerushalmi. A scalable lock-free stack algorithm. In *SPAA*, 2004.
9. M. Herlihy and N. Shavit. *The art of multiprocessor programming*. 2008.
10. M. P. Herlihy and J. M. Wing. Linearizability: a correctness condition for concurrent objects. *TOPLAS*, 12, 1990.
11. C. Jones. Splitting atoms safely. *TCS*, 375, 2007.
12. E. Petrank, M. Musuvathi, and B. Steensgaard. Progress guarantee via bounded lock-freedom. In *PLDI*, 2009.
13. R. K. Treiber. Systems programming: Coping with parallelism. Technical Report RJ 5118, IBM Almaden Research Center, 1986.
14. V. Vafeiadis. Modular fine-grained concurrency verification. PhD Thesis. Technical Report UCAM-CL-TR-726, University of Cambridge, 2008.
15. V. Vafeiadis. Automatically proving linearizability. In *CAV*, 2010.
16. M. Y. Vardi. Verification of concurrent programs—the automata-theoretic framework. *Annals of Pure and Applied Logic*, 51, 1991.

## A Additional Definitions for the Programming Language

**Semantics of typical primitive commands.** We consider the following sample primitive commands:

$$\text{skip}_i, (x = E)_i, (x = [E])_i, ([E] = E')_i, \text{assume}(E)_i,$$

where the subscript  $i \in \{\text{client}, \text{lib}\}$  indicates whether the command is for the client code or for the library code. We assume that if the subscript  $i$  of a command is client, the command uses only client variables in CVar and make a similar assumption for the case  $i = \text{lib}$ .

For these commands, we define corresponding transition relations  $\rightsquigarrow$  in Figure 3. If a command has the client subscript, this relation transforms client states in CState, and if the commands has the lib subscript, the relation changes library states in LState. Using these transition relations, we then define  $f_c$  for the above commands  $c$  as follows:

$$f_c(\theta) = \bigcup \{ \theta' \mid c, \theta \rightsquigarrow \theta' \}.$$

Here  $\theta$  is a client or library state depending on whether  $c$  is a client command or a library command.

**Definition of loops and conditionals.** Let  $!E$  be the C-language style negation of an expression  $E$ , so that  $\llbracket !E \rrbracket s = 1$  if  $\llbracket E \rrbracket s = 0$ , and  $\llbracket E \rrbracket s = 0$  for all the other cases. The standard commands for conditionals and loops are defined in our language as follows:

$$\begin{aligned} (\text{if}_i E \text{ then } C_1 \text{ else } C_2) &= (\text{assume}(E)_i; C_1) + (\text{assume}(!E)_i; C_2), \\ (\text{while}_i E \text{ do } C) &= (\text{assume}(E)_i; C)^\circ; \text{assume}(!E)_i, \end{aligned}$$

where  $i$  is client or lib, depending on which part of the code the command belongs to.

**Translation of commands to CFGs.** We construct the CFG of a command  $C$  by induction on its syntax:

1. A primitive command  $c$  has the CFG  $(\{\text{start}, \text{end}\}, \{(\text{start}, c, \text{end})\}, \text{start}, \text{end})$ .
2. Assume  $C_1$  and  $C_2$  have CFGs  $(N_1, T_1, \text{start}_1, \text{end}_1)$  and  $(N_2, T_2, \text{start}_2, \text{end}_2)$ , respectively. Then  $C_1; C_2$  has the CFG

$$(N_1 \cup N_2, T_1 \cup T_2 \cup \{(\text{end}_1, \text{skip}_i, \text{start}_2)\}, \text{start}_1, \text{end}_2).$$

$$\begin{aligned} &\text{skip}_{\text{client}}, (s_C, h_C) \rightsquigarrow (s_C, h_C) \\ &(x = E)_{\text{client}}, (s_C, h_C) \rightsquigarrow (s_C[x : \llbracket E \rrbracket s_C], h_C) \\ &(x = [E])_{\text{client}}, (s_C, h_C) \rightsquigarrow (s_C[x : h_C(\llbracket E \rrbracket s_C)], h_C) && (\text{when } \llbracket E \rrbracket s_C \in \text{CLoc}) \\ &([E] = E')_{\text{client}}, (s_C, h_C) \rightsquigarrow (s_C, h_C[\llbracket E \rrbracket s_C : \llbracket E' \rrbracket s_C]) && (\text{when } \llbracket E \rrbracket s_C \in \text{CLoc}) \\ &(\text{assume}(E))_{\text{client}}, (s_C, h_C) \rightsquigarrow (s_C, h_C) && (\text{when } \llbracket E \rrbracket s_C \neq 0) \\ \\ &\text{skip}_{\text{lib}}, (s_L, h_L) \rightsquigarrow (s_L, h_L) \\ &(x = E)_{\text{lib}}, (s_L, h_L) \rightsquigarrow (s_L[x : \llbracket E \rrbracket s_L], h_L) \\ &(x = [E])_{\text{lib}}, (s_L, h_L) \rightsquigarrow (s_L[x : h_L(\llbracket E \rrbracket s_L)], h_L) && (\text{when } \llbracket E \rrbracket s_L \in \text{LLoc}) \\ &([E] = E')_{\text{lib}}, (s_L, h_L) \rightsquigarrow (s_L, h_L[\llbracket E \rrbracket s_L : \llbracket E' \rrbracket s_L]) && (\text{when } \llbracket E \rrbracket s_L \in \text{LLoc}) \\ &(\text{assume}(E))_{\text{lib}}, (s_L, h_L) \rightsquigarrow (s_L, h_L) && (\text{when } \llbracket E \rrbracket s_L \neq 0) \end{aligned}$$

**Fig. 3.** Transition relation for sample primitive commands. Here  $(s_C, h_C)$  is a client state in CState and  $(s_L, h_L)$  a library state in LState.

$$\begin{array}{c}
\frac{(v, c, v') \in T \quad \theta' \in f_c(\theta)}{\text{pc}[t : v], \theta \xrightarrow{(t, \text{Client}(c))}_{C(\cdot)} \text{pc}[t : v'], \theta'} \\
\frac{(v, m(E), v') \in T \quad \llbracket E \rrbracket s = u}{\text{pc}[t : v], (s, h) \xrightarrow{(t, \text{call } m(u))}_{C(\cdot)} \text{pc}[t : \langle v', m \rangle], (s, h)} \\
\text{pc}[t : \langle v, m \rangle], (s, h) \xrightarrow{(t, \text{ret } m(u))}_{C(\cdot)} \text{pc}[t : v], (s[\text{retval}_t : u], h)
\end{array}$$

**Fig. 4.** Client-local semantics

3. Assume  $C_1$  and  $C_2$  have CFGs  $(N_1, T_1, \text{start}_1, \text{end}_1)$  and  $(N_2, T_2, \text{start}_2, \text{end}_2)$ , respectively. Then  $C_1 + C_2$  has the CFG
$$(N_1 \cup N_2 \cup \{\text{start}, \text{end}\}, T_1 \cup T_2 \cup \{(\text{start}, \text{skip}_i, \text{start}_1), (\text{start}, \text{skip}_i, \text{start}_2), (\text{end}_1, \text{skip}_i, \text{end}), (\text{end}_2, \text{skip}_i, \text{end})\}, \text{start}, \text{end}).$$
4. Assume  $C$  has a CFG  $(N, T, \text{start}, \text{end})$ . Then  $C^\circ$  has the CFG
$$(N, T \cup \{(\text{end}, \text{skip}_i, \text{start})\}, \text{start}, \text{end}).$$

As before,  $i$  is client or lib, depending on which part of the code the command belongs to.

## B Proof of Theorem 4

We first present an outline of the proof of Theorem 4; proofs of the lemmas below are given in the following sections. To prove the theorem, we need to be able to transform traces of  $C(A_1)$  into traces of  $C(A_2)$ , which uses a different implementation of the library. We perform this transformation with the aid of a *client-local semantics*, which produces all behaviours of  $C$  regardless of the particular library implementation it uses. Let  $n$  be the number of threads in  $C$ . The semantics is defined by a transition relation  $\longrightarrow_{C(\cdot)}: \text{CConfig} \times \text{Act} \times \text{CConfig}$  in Figure 4, which transforms configurations  $\text{CConfig} = (\{1, \dots, n\} \rightarrow \text{CPos}) \times \text{CState}$  for  $\text{CPos} = \text{CNode} \cup (\text{CNode} \times \text{Method})$ . Note that, upon a call, we do not execute library actions, but just save the return point  $v'$  and the method  $m$  called in a thread position of the form  $\langle v', m \rangle$ . The semantics allows for an arbitrary library behaviour, since we let library methods return with any value. We define the client-local semantics of  $C$  as the set  $\llbracket C(\cdot) \rrbracket \subseteq \text{CTrace}$  of all traces generated using  $\longrightarrow_{C(\cdot)}$  from any initial configuration in  $\text{CConfig}$ .

We thus have three semantics related to a program  $C(A)$  used in the proof: the standard semantics  $\llbracket C(A) \rrbracket \subseteq \text{Trace}$ , the client-local semantics  $\llbracket C(\cdot) \rrbracket \subseteq \text{CTrace}$ , and the library-local semantics  $\llbracket A \rrbracket \subseteq \text{LTrace}$ . They are defined by the corresponding transition relations  $\longrightarrow_{C(A)}$ ,  $\longrightarrow_{C(\cdot)}$  and  $\longrightarrow_{\text{MGC}_n(A)}$ .

For a trace  $\tau$  we define its *core history*  $\text{corehistory}(\tau)$  as the projection of  $\tau$  to actions in  $\text{CallRetAct}$ . We denote with  $\text{CoreHistory}$  the set of all core histories. A client trace  $\tau \in \text{CTrace}$  is *well-formed* if for all  $t \in \text{ThreadID}$ , every call action  $(t, \text{call } m(u))$  in the trace  $\tau|_t$  is either the last one in the trace or is immediately followed by the corresponding return action  $(t, \text{ret}(u') m)$ , i.e., if every such projection behaves sequentially. The definition of well-formed core histories is the same.

We first state a lemma showing that a trace of  $C(A)$  generates two traces in the client-local and library-local semantics, and any two such traces agreeing on the core history can be combined into a valid trace of  $C(A)$ .

**Lemma 10 (Decomposition).** *1.  $\forall \tau \in \llbracket C(A) \rrbracket. \text{client}(\tau) \in \llbracket C(\cdot) \rrbracket \wedge \text{lib}(\tau) \in \llbracket A \rrbracket.$*   
*2.  $\forall \eta \in \llbracket C(\cdot) \rrbracket, \forall \xi \in \llbracket A \rrbracket, \text{corehistory}(\eta) = \text{corehistory}(\xi) \Rightarrow$*   
 *$\exists \tau \in \llbracket C(A) \rrbracket. \text{client}(\tau) = \eta \wedge \text{lib}(\tau) = \xi.$*

The following lemma presents the core of the trace transformation used to generate  $\tau_2$  out of  $\tau_1$  in Theorem 4: it shows that a client trace can be transformed into an equivalent one with a given history linearizing the history of the original one.

**Lemma 11 (Rearrangement).** *Consider well-formed core histories  $H, H' \in \text{CoreHistory}$  such that  $H \sqsubseteq H'$ . For all well-formed client traces  $\tau \in \text{CTrace}$  such that  $\text{corehistory}(\tau) = H$  there exists  $\tau' \in \text{CTrace}$  such that  $\tau \sim \tau' \wedge \text{corehistory}(\tau') = H'$ .*

Finally, the following lemma shows that the trace resulting from the transformation in Lemma 11 is derivable in the client-local semantics if the original one is.

**Lemma 12.** *The set  $\llbracket C(\cdot) \rrbracket$  is closed under trace equivalence.*

**Proof of Theorem 4.** Take  $\tau_1 \in \llbracket C(A_1) \rrbracket$ . By Lemma 10(1),

$$\text{client}(\tau_1) \in \llbracket C(\cdot) \rrbracket \wedge \text{lib}(\tau_1) \in \llbracket A_1 \rrbracket.$$

Let  $H_1 = \text{history}(\tau_1)$ . Then,  $H_1 \in \text{history}(\llbracket A_1 \rrbracket)$ . Furthermore, since  $A_1 \sqsubseteq A_2$ , there exists a history  $H_2 \in \text{history}(\llbracket A_2 \rrbracket)$  such that  $H_1 \sqsubseteq H_2$ . Then  $\text{corehistory}(H_1) \sqsubseteq \text{corehistory}(H_2)$ . Applying Lemma 11, we can construct a trace  $\eta \in \text{CTrace}$  such that

$$\text{client}(\tau_1) \sim \eta \wedge \text{corehistory}(\eta) = \text{corehistory}(H_2).$$

By Lemma 12,  $\eta \in \llbracket C(\cdot) \rrbracket$ . Since  $H_2 \in \text{history}(\llbracket A_2 \rrbracket)$ , there exists a library trace  $\xi \in \llbracket A_2 \rrbracket$  such that  $\text{history}(\xi) = H_2$ . Then  $\text{corehistory}(\eta) = \text{corehistory}(\xi)$ . By Lemma 10(2), for some  $\tau_2 \in \llbracket C(A_2) \rrbracket$  we have  $\eta = \text{client}(\tau_2)$  and  $\xi = \text{lib}(\tau_2)$ . Thus,

$$\text{client}(\tau_1) \sim \text{client}(\tau_2) \wedge \text{history}(\tau_2) = \text{history}(\text{lib}(\tau_2)) = H_2,$$

which implies that  $\tau_2$  is what we are looking for.  $\square$

## B.1 Notation

Before proving the lemmas, we introduce some auxiliary notation.

For a state  $\theta = (s, h)$ ,  $x \in \text{Var}$  and  $u \in \text{Val}$  we let  $\theta[x : u] = (s[x : u], h)$  and  $\theta(x) = s(x)$ . For a configuration  $\sigma = (\text{pc}, \theta)$ ,  $t \in \text{ThreadID}$  and  $x \in \text{CVar}$ , we write  $\sigma(t)$  for  $\text{pc}(t)$  and  $\sigma(x)$  for  $\theta(x)$ . For a state  $\theta$  or a configuration  $\sigma$ , we denote with  $\llbracket E \rrbracket \theta$  or  $\llbracket E \rrbracket \sigma$  the value of the expression  $E$  in the stack of the state or the configuration.

We define functions  $\text{client} : \text{Pos} \rightarrow \text{CPos}$  and  $\text{lib}_t : \text{Pos} \rightarrow \text{LPos}$ ,  $t \in \text{ThreadID}$  that compute thread positions in the client-local and library-local semantics corresponding to a position in the complete program:  $\text{client}(v) = v$ , for  $v \in \text{CNode}$ ;  $\text{client}(\langle u, v', v \rangle) = \langle v', \text{method}(v) \rangle$  for  $v' \in \text{CNode}$  and  $v \in \text{LNode}$ ;  $\text{lib}_t(v) = v_{\text{mgc}}^t$  for  $v \in \text{CNode}$ ;  $\text{lib}_t(\langle u, v', v \rangle) = \langle u, v_{\text{mgc}}^t, v \rangle$  for  $v' \in \text{CNode}$  and  $v \in \text{LNode}$ . We then lift  $\text{client}$  and  $\text{lib}$  to program counters as follows:  $(\text{client}(\text{pc}))(t) = \text{client}(\text{pc}(t))$  and  $(\text{lib}(\text{pc}))(t) = \text{lib}_t(\text{pc}(t))$ . Finally, we lift them to configurations:  $\text{client}(\text{pc}, \theta) =$

$(\text{client}(\text{pc}), \text{client}(\theta))$  and  $\text{lib}(\text{pc}, \theta) = (\text{lib}(\text{pc}), \text{lib}(\theta))$ . We lift the client and lib operations on states defined in §2 to sets of states pointwise.

We define a partial operation  $\circ : \text{CPos} \times \text{LPos} \rightarrow \text{Pos}$  that combines thread positions in the client-local and library-local semantics to obtain a position in the complete program:  $v \circ v_{\text{mgc}}^t = v$  for  $v \in \text{CNode}$ ;  $\langle v, m \rangle \circ \langle u, v_{\text{mgc}}^t, v' \rangle = \langle u, v, v' \rangle$  for  $v \in \text{CNode}$  and  $v' \in \text{LNode}$  such that  $\text{method}(v') = m$ ; all other combinations are undefined. We then lift  $\circ$  to program counters pointwise and to configurations as follows:  $(\text{pc}_1, \theta_1) \circ (\text{pc}_2, \theta_2) = (\text{pc}_1 \circ \text{pc}_2, \theta_1 \circ \theta_2)$ . Note that for all  $\sigma \in \text{State}$  we have  $\text{client}(\sigma) \circ \text{lib}(\sigma) = \sigma$ .

For a state  $\theta \in \text{CState}$ , let  $\text{core}(\theta)$  be the state  $\theta$  with the stack excluding the  $\text{retval}_t$  variables. (Strictly speaking, we are overloading the word ‘state’ here, because  $\text{core}(\theta)$  has the type  $(\text{CVar}' \rightarrow \text{Val}) \times \text{Heap}$  for  $\text{CVar}' = \text{CVar} - \{\text{retval}_t \mid t \in \text{ThreadID}\}$ .) We lift core to sets of states pointwise and let  $\text{core}(\text{pc}, \theta) = \text{core}(\theta)$ .

In the following we sometimes write  $\sqsubseteq_\pi$  and  $\sim_\pi$  instead of  $\sqsubseteq$  and  $\sim$  to make the bijection  $\pi$  used to establish the relations between histories or traces explicit.

Finally, we recall the construction of transformers for primitive commands from §2 which is used in the proofs:

$$\forall \theta \in \text{State}. f_c(\theta) \stackrel{\text{def}}{=} \begin{cases} \{\text{client}(\theta)\} \circ f_c(\text{lib}(\theta)), & \text{if } c \in \text{LibPComm}; \\ f_c(\text{client}(\theta)) \circ \{\text{lib}(\theta)\}, & \text{if } c \in \text{ClientPComm}. \end{cases} \quad (1)$$

## B.2 Proof of Lemma 10

We prove each of the two cases in the lemma separately.

*Case 1.* Consider  $\tau \in \llbracket C(A) \rrbracket$  and let  $\eta = \text{client}(\tau)$  and  $\xi = \text{lib}(\tau)$ . We need to show that  $\eta \in \llbracket C(\cdot) \rrbracket$  and  $\xi \in \llbracket A \rrbracket$ . Since  $\tau \in \llbracket C(A) \rrbracket$ , there exists a  $\tau$ -labelled computation sequence that starts from some initial configuration  $\sigma_0 \in \text{Config}$  and follows the relation  $\rightarrow_{C(A)}$ . Let  $n$  be the number of threads in  $C(A)$ . From the computation sequence of  $\tau$ , we construct the computation sequence of  $\eta$  using  $\rightarrow_{C(\cdot)}$  and that of  $\xi$  using  $\rightarrow_{\text{MGC}_n(A)}$ . Our construction first considers every finite prefix  $\tau_1$  of  $\tau$  and builds client-local and library-local computation sequences for  $\tau_1$ . Then we construct the desired computation sequences for  $\eta$  and  $\xi$  as the limits of these sequences (our construction is such that this limit exists). The following claim lies at the core of our construction:

Consider a finite prefix  $\tau_1$  of  $\tau$  and a configuration  $\sigma \in \text{Config}$  such that

$$\begin{aligned} \sigma_0 &\xrightarrow{\tau_1}_{C(A)}^* \sigma \wedge \text{client}(\sigma_0) \xrightarrow{\text{client}(\tau_1)}_{C(\cdot)}^* \text{client}(\sigma) \\ &\wedge \text{lib}(\sigma_0) \xrightarrow{\text{lib}(\tau_1)}_{\text{MGC}_n(A)}^* \text{lib}(\sigma). \end{aligned}$$

If  $\tau = \tau_1 \varphi \tau_2'$  for some action  $\varphi$  and trace  $\tau_2'$ , and  $\sigma \xrightarrow{\varphi}_{C(A)} \sigma'$  for some  $\sigma'$ , we have that

$$\text{client}(\sigma_0) \xrightarrow{\text{client}(\tau_1 \varphi)}_{C(\cdot)}^* \text{client}(\sigma') \wedge \text{lib}(\sigma_0) \xrightarrow{\text{lib}(\tau_1 \varphi)}_{\text{MGC}_n(A)}^* \text{lib}(\sigma').$$

To prove the claim, we assume  $\tau_1, \varphi, \tau_2', \sigma, \sigma'$  satisfying the assumptions in the claim. There are four cases:

- $\varphi \in \text{ClientAct}$ . In this case, there exist a thread  $t \in \{1, \dots, n\}$ , client nodes  $v, v' \in \text{CNode}$ , a client command  $c \in \text{ClientPCComm}$ , and states  $\theta, \theta' \in \text{State}$ , such that  $(v, c, v')$  is in the control-flow relation of  $C(A)$  and

$$\sigma = (\text{pc}[t : v], \theta) \wedge \sigma' = (\text{pc}[t : v'], \theta') \wedge \theta' \in f_c(\theta).$$

Since  $c$  is a client operation, from (1) it follows that

$$\text{client}(\theta') \in \text{client}(f_c(\theta)) = f_c(\text{client}(\theta)).$$

This in turn implies

$$\text{client}(\text{pc}[t : v], \text{client}(\theta)) \xrightarrow{\varphi}_{C(\cdot)} \text{client}(\text{pc}[t : v'], \text{client}(\theta')).$$

Since  $v, v' \in \text{CNode}$ , we have

$$\text{client}(\text{pc}[t : v]) = \text{client}(\text{pc}[t : v]) \wedge \text{client}(\text{pc}[t : v']) = \text{client}(\text{pc}[t : v']).$$

Hence, the transition above is equivalent to  $\text{client}(\sigma) \xrightarrow{\varphi}_{C(\cdot)} \text{client}(\sigma')$ , which implies that

$$\text{client}(\sigma_0) \xrightarrow{\text{client}(\tau_1 \varphi)}^*_{C(\cdot)} \text{client}(\sigma').$$

For the library computation sequence, we use (1) again and infer that

$$\text{lib}(\theta') \in \text{lib}(f_c(\theta)) = \{\text{lib}(\theta)\}.$$

Thus,

$$\text{lib}(\sigma) = (\text{lib}(\text{pc}[t : v_{\text{mgc}}^t], \text{lib}(\theta)) = (\text{lib}(\text{pc}[t : v_{\text{mgc}}^t], \text{lib}(\theta')) = \text{lib}(\sigma').$$

From this and  $\text{lib}(\tau_1 \varphi) = \text{lib}(\tau_1)$ , it follows that

$$\text{lib}(\sigma_0) \xrightarrow{\text{lib}(\tau_1 \varphi)}^*_{\text{MGC}_n(A)} \text{lib}(\sigma').$$

- $\varphi \in \text{LibAct}$ . This case is treated similarly to the previous one. We establish that  $\text{lib}(\sigma) \xrightarrow{\varphi}_{\text{MGC}_n(A)} \text{lib}(\sigma')$  and  $\text{client}(\sigma') = \text{client}(\sigma)$ . Since  $\text{lib}(\tau_1 \varphi) = \text{lib}(\tau_1) \varphi$  and  $\text{client}(\tau_1 \varphi) = \text{client}(\tau_1)$ , this implies our claim.
- $\varphi \in \text{CallAct}$ . In this case, there exist a thread  $t \in \{1, \dots, n\}$ , client nodes  $v, v' \in \text{CNode}$ , a method  $m$ , and a state  $\theta \in \text{State}$ , such that  $(v, m(E), v')$  is in the control-flow relation of  $C(A)$  and

$$\sigma = (\text{pc}[t : v], \theta) \wedge \sigma' = (\text{pc}[t : \langle \llbracket E \rrbracket \theta, v', \text{start}_m \rangle], \theta).$$

Then,

$$\begin{aligned} \text{client}(\sigma) &= (\text{client}(\text{pc}[t : v], \text{client}(\theta)) \wedge \\ \text{client}(\sigma') &= (\text{client}(\text{pc}[t : \langle v', m \rangle], \text{client}(\theta)) \wedge \\ \text{lib}(\sigma) &= (\text{lib}(\text{pc}[t : v_{\text{mgc}}^t], \text{lib}(\theta)) \wedge \\ \text{lib}(\sigma') &= (\text{lib}(\text{pc}[t : \langle \llbracket E \rrbracket \theta, v_{\text{mgc}}^t, \text{start}_m \rangle], \text{lib}(\theta)). \end{aligned}$$

From this we can establish  $\text{client}(\sigma) \xrightarrow{\varphi}_{C(\cdot)} \text{client}(\sigma')$  and  $\text{lib}(\sigma) \xrightarrow{\varphi}_{\text{MGC}_n(A)} \text{lib}(\sigma')$ . Furthermore,  $\text{client}(\tau_1 \varphi) = \text{client}(\tau_1) \varphi$  and  $\text{lib}(\tau_1 \varphi) = \text{lib}(\tau_1) \varphi$ . Hence,

$$\text{client}(\sigma_0) \xrightarrow{\text{client}(\tau_1 \varphi)}^*_{C(\cdot)} \text{client}(\sigma') \wedge \text{lib}(\sigma_0) \xrightarrow{\text{lib}(\tau_1 \varphi)}^*_{\text{MGC}_n(A)} \text{lib}(\sigma').$$

- $\varphi \in \text{RetAct}$ . This case is treated similarly to the previous one. We establish  $\text{client}(\sigma) \xrightarrow{\varphi}_{C(\cdot)} \text{client}(\sigma')$  and  $\text{lib}(\sigma) \xrightarrow{\varphi}_{\text{MGC}_n(A)} \text{lib}(\sigma')$ . Just like in the previous case, we also have  $\text{client}(\tau_1 \varphi) = \text{client}(\tau_1) \varphi$  and  $\text{lib}(\tau_1 \varphi) = \text{lib}(\tau_1) \varphi$ , which implies our claim.

We have just shown that the claim holds for all  $\varphi$ .

*Case 2.* Assume  $\eta \in \llbracket C(\cdot) \rrbracket$  and  $\xi \in \llbracket A \rrbracket$  such that  $\text{corehistory}(\eta) = \text{corehistory}(\xi)$ . There exists a  $\eta$ -labelled client-local computation sequence that starts from an initial configuration  $\sigma_0^1 \in \text{CConfig}$  and follows the transition relation  $\longrightarrow_{C(\cdot)}$ . Let  $n$  be the number of threads in  $C(A)$ . Since  $\text{corehistory}(\eta) = \text{corehistory}(\xi)$ , the thread identifiers mentioned in  $\xi$  all occur in  $\eta$ . Hence, using  $\text{MGC}_n(A)$ , we can generate a library-local computation sequence for  $\xi$ . This sequence is labelled with  $\xi$ , starts from some initial configuration  $\sigma_0^2 \in \text{LConfig}$ , and uses the transition relation  $\longrightarrow_{\text{MGC}_n(A)}$ . Out of these two computation sequences, we now construct the required trace  $\tau \in \llbracket C(A) \rrbracket$  together with its computation sequence using  $\longrightarrow_{C(A)}$ . We first build a series of finite traces

$$\tau_0, \tau_1, \tau_2, \dots$$

and their computation sequences. One important feature of this series is that for  $i < j$ , the computation sequence of  $\tau_i$  is a prefix of that of  $\tau_j$ , which also implies that  $\tau_i$  is a prefix of  $\tau_j$ . Because of this feature, this series has the limit computation sequence and the limit trace, which are the desired ones.

The first element in the series is the empty trace  $\varepsilon$  and the empty computation sequence consisting of the initial configuration  $\sigma_0^1 \circ \sigma_0^2$  only. For the  $(i+1)$ -st element with  $i > 0$ , we assume that the  $i$ -th element  $\tau_i$  and its computation have been constructed and satisfy the following property:

The client projection  $\text{client}(\tau_i)$  is a finite prefix of  $\eta$ , and the library projection  $\text{lib}(\tau_i)$  is a finite prefix of  $\xi$ . Furthermore, for some client configuration  $\sigma_i^1 \in \text{CConfig}$ , and some library configuration  $\sigma_i^2 \in \text{LConfig}$ , the constructed computation sequence for  $\tau_i$  leads to  $\sigma_i^1 \circ \sigma_i^2$ :

$$\sigma_0^1 \circ \sigma_0^2 \xrightarrow{\tau_i}_{C(A)}^* \sigma_i^1 \circ \sigma_i^2,$$

and the given computation sequences for  $\eta$  and  $\xi$  have the following prefixes:

$$\sigma_0^1 \xrightarrow{\text{client}(\tau_i)}_{C(\cdot)}^* \sigma_i^1 \quad \wedge \quad \sigma_0^2 \xrightarrow{\text{lib}(\tau_i)}_{\text{MGC}_n(A)}^* \sigma_i^2.$$

Now we define the  $(i+1)$ -th element  $\tau_{i+1}$  and its computation sequence that maintain this property. As we explained above, the computation sequence for  $\tau_{i+1}$  will be an extension of that for  $\tau_i$  by one or more steps.

Assume  $\eta = \text{client}(\tau_i)\varphi_1\eta'$  and  $\xi = \text{lib}(\tau_i)\varphi_2\xi'$  for some actions  $\varphi_1$  and  $\varphi_2$  and traces  $\eta'$  and  $\xi'$  (the case that  $\eta = \text{client}(\tau_i)$  or  $\xi = \text{lib}(\tau_i)$  is treated analogously). Let the following be the transitions by  $\varphi_1$  and  $\varphi_2$  in the computation sequences for  $\eta$  and  $\xi$ :

$$\sigma_i^1 \xrightarrow{\varphi_1}_{C(\cdot)} \sigma^1 \quad \wedge \quad \sigma_i^2 \xrightarrow{\varphi_2}_{\text{MGC}_n(A)} \sigma^2$$

for some  $\sigma^1 \in \text{CConfig}$  and  $\sigma^2 \in \text{LConfig}$ . We have the following cases:

- $\varphi_1, \varphi_2 \in \text{CallRetAct}$ . In this case,  $\varphi_1$  is the same as  $\varphi_2$ . This is because  $\text{corehistory}(\eta_1)$  and  $\text{corehistory}(\xi_1)$  are the same by assumption so that their prefixes  $\text{corehistory}(\tau_i)\varphi_1$  and  $\text{corehistory}(\tau_i)\varphi_2$  of the same length should be identical. Assume  $\varphi_1 \in \text{CallAct}$  (the case when  $\varphi_1 \in \text{RetAct}$  can be treated analogously). Then, there exist  $t \in \{1, \dots, n\}$ ,  $v, v' \in \text{CNode}$ ,  $\theta^1 \in \text{CState}$ , and  $\theta^2 \in \text{LState}$  such that  $(v, m(E), v')$  is in the control-flow relation of  $C(A)$  and

$$\begin{aligned} \sigma_i^1 &= (\text{pc}_1[t : v], \theta^1) \quad \wedge \quad \sigma^1 = (\text{pc}_1[t : \langle v', m \rangle], \theta^1) \quad \wedge \\ \sigma_i^2 &= (\text{pc}_2[t : v_{\text{mgc}}^t], \theta^2) \quad \wedge \quad \sigma^2 = (\text{pc}_2[t : \langle \llbracket E \rrbracket \theta^1, v_{\text{mgc}}^t, \text{start}_m \rangle], \theta^2). \end{aligned}$$

Let  $pc = pc_1 \circ pc_2$ . Then

$$\begin{aligned}\sigma_i^1 \circ \sigma_i^2 &= (pc[t : v], \theta^1 \circ \theta^2) \wedge \\ \sigma^1 \circ \sigma^2 &= (pc[t : \langle \llbracket E \rrbracket \theta^1, v', \text{start}_m \rangle], \theta^1 \circ \theta^2).\end{aligned}$$

Furthermore,  $\llbracket E \rrbracket \theta^1 = \llbracket E \rrbracket (\theta^1 \circ \theta^2)$ . Then,  $\sigma_i^1 \circ \sigma_i^2 \xrightarrow{\varphi_1}_{C(A)} \sigma^1 \circ \sigma^2$ . Hence, in this case the desired  $\tau_{i+1}$  is  $\tau_i \varphi_1$ , and the computation sequence for  $\tau_{i+1}$  is:

$$\sigma_0^1 \circ \sigma_0^2 \xrightarrow{\tau_i}^*_{C(A)} \sigma_i^1 \circ \sigma_i^2 \xrightarrow{\varphi_1}_{C(A)} \sigma^1 \circ \sigma^2.$$

Finally, since  $\text{client}(\tau_i \varphi_1) = \text{client}(\tau_i) \varphi_1$  and  $\text{lib}(\tau_i \varphi_2) = \text{lib}(\tau_i) \varphi_2$ , the conditions on the prefixes of the computation sequences of  $\eta$  and  $\xi$  in this case follow from those for  $\tau_i$ .

- $\varphi_1 \in \text{RetAct}$ ,  $\varphi_2 \in \text{LibAct}$  and they are performed by the same thread. In this case for some  $t \in \{1, \dots, n\}$ ,  $\theta^1 \in \text{CState}$ ,  $\theta^2 \in \text{LState}$ ,  $\theta^3 \in \text{LState}$ ,  $v_0 \in \text{CNode}$ ,  $v, v' \in \text{LNode}$  and  $u \in \text{Val}$ , we have that  $(v, c, v')$  is in the control-flow relation of  $C(A)$  and

$$\begin{aligned}\sigma_i^1 &= (pc_1[t : \langle v_0, \text{method}(v) \rangle], \theta^1) \wedge \\ \sigma_i^2 &= (pc_2[t : \langle u, v_{\text{mgc}}^t, v \rangle], \theta^2) \wedge \\ \sigma^2 &= (pc_2[t : \langle \theta^3(\text{param}), v_{\text{mgc}}^t, v' \rangle], \theta^3) \wedge \theta^3 \in f_c(\theta^2[\text{param} : u]).\end{aligned}$$

Let  $pc = pc_1 \circ pc_2$ . Then

$$\begin{aligned}\sigma_i^1 \circ \sigma_i^2 &= (pc[t : \langle u, v_0, v \rangle], \theta^1 \circ \theta^2) \wedge \\ \sigma_i^1 \circ \sigma^2 &= (pc[t : \langle (\theta^1 \circ \theta^3)(\text{param}), v_0, v' \rangle], \theta^1 \circ \theta^3).\end{aligned}$$

From (1) we have

$$\begin{aligned}\theta^1 \circ \theta^3 &\in \{\theta^1\} \circ f_c(\theta^2[\text{param} : u]) = f_c(\theta^1 \circ (\theta^2[\text{param} : u])) \\ &= f_c((\theta^1 \circ \theta^2)[\text{param} : u]).\end{aligned}$$

Then  $\sigma_i^1 \circ \sigma_i^2 \xrightarrow{\varphi_2}_{C(A)} \sigma_i^1 \circ \sigma^2$ . The desired  $\tau_{i+1}$  is thus  $\tau_i \varphi_2$ , and its computation sequence is:

$$\sigma_0^1 \circ \sigma_0^2 \xrightarrow{\tau_i}^*_{C(A)} \sigma_i^1 \circ \sigma_i^2 \xrightarrow{\varphi_2}_{C(A)} \sigma_i^1 \circ \sigma^2.$$

Finally, the conditions on the prefixes of the computation sequences for  $\eta$  and  $\xi$  follow from  $\text{client}(\tau_i \varphi_2) = \text{client}(\tau_i)$  and  $\text{lib}(\tau_i \varphi_2) = \text{lib}(\tau_i) \varphi_2$ .

- $\varphi_1 \in \text{ClientAct}$ ,  $\varphi_2 \in \text{CallAct}$  and they are performed by the same thread. This case is treated similarly to the previous one: we show that  $\sigma_i^1 \circ \sigma_i^2 \xrightarrow{\varphi_1}_{C(A)} \sigma^1 \circ \sigma_i^2$ .
- $\varphi_1 \in \text{ClientAct}$ ,  $\varphi_2 \in \text{LibAct}$  and they are done by different threads. In this case,

$$\text{client}(\tau_i \varphi_1 \varphi_2) = \text{client}(\tau_i) \varphi_1 \quad \wedge \quad \text{lib}(\tau_i \varphi_1 \varphi_2) = \text{lib}(\tau_i) \varphi_2.$$

As before, we can show that

$$\sigma_i^1 \circ \sigma_i^2 \xrightarrow{\varphi_1}_{C(A)} \sigma^1 \circ \sigma_i^2 \quad \wedge \quad \sigma^1 \circ \sigma_i^2 \xrightarrow{\varphi_2}_{C(A)} \sigma^1 \circ \sigma^2.$$

This gives the extension of the given computation for  $\tau_i$  by two further steps:

$$\sigma_0^1 \circ \sigma_0^2 \xrightarrow{\tau_i \varphi_1 \varphi_2}^*_{C(A)} \sigma^1 \circ \sigma^2.$$

It follows that the trace  $\tau_i \varphi_1 \varphi_2$  is the desired  $\tau_{i+1}$ .

- $\varphi_1 \in \text{CallRetAct}$ ,  $\varphi_2 \in \text{LibAct}$  and they are performed by different threads. In this case

$$\text{client}(\tau_i \varphi_2) = \text{client}(\tau_i) \quad \wedge \quad \text{lib}(\tau_i \varphi_2) = \text{lib}(\tau_i) \varphi_2.$$

Here we can show that

$$\sigma_0^1 \circ \sigma_0^2 \xrightarrow{\tau_i}^*_{C(A)} \sigma_i^1 \circ \sigma_i^2 \xrightarrow{\varphi_2}_{C(A)} \sigma_i^1 \circ \sigma^2,$$

which implies that  $\tau_i \varphi_2$  is the desired trace.

- $\varphi_1 \in \text{ClientAct}$ ,  $\varphi_2 \in \text{CallRetAct}$  and they are performed by different threads. This case is similar to the previous one.
- $\varphi_1$  and  $\varphi_2$  are done by the same thread and one of the two conditions holds:  $\varphi_1 \in \text{ClientAct}$  and  $\varphi_2 \in (\text{RetAct} \cup \text{LibAct})$ , or  $\varphi_1 \in \text{CallAct}$  and  $\varphi_2 \in \text{LibAct}$ . Using the definition of  $\circ$ , it is easy to check that these cases are impossible.

We have just shown how to construct  $\tau_i$  for all the cases. The desired computation sequence is constructed as the limit of the sequence for  $\tau_i$ . It is easy to show that the resulting trace  $\tau$  satisfies  $\text{client}(\tau) = \eta$  and  $\text{lib}(\tau) = \xi$ .  $\square$

### B.3 Proof of Lemma 11

Consider a well-formed client trace  $\tau \in \text{CTrace}$  and well-formed core histories  $H, S \in \text{CoreHistory}$  such that  $\text{corehistory}(\tau) = H$  and  $H \sqsubseteq S$ . We need to prove that there exists a well-formed client trace  $\tau' \in \text{CTrace}$  such that  $\text{corehistory}(\tau') = S$  and  $\tau \sim \tau'$ . To this end, we define a (possibly infinite) sequence of steps that transforms  $\tau$  into  $\tau'$ . The trace  $\tau'$  is constructed as a limit of a sequence of well-formed traces  $\xi_k$ , defined for every finite prefix  $S_k$  of  $S$  of length  $k$ . This sequence is defined inductively, and every trace  $\xi_k$  in it is such that for some prefix  $\eta_k$  of  $\xi_k$  we have  $\text{corehistory}(\eta_k) = S_k$  and  $\text{corehistory}(\xi_k) \sqsubseteq_{\pi} S$ , where  $\pi$  is an identity on actions from  $S_k$  in  $\text{corehistory}(\xi_k)$ . To construct the sequence, we let  $\xi_0 = \tau$  and let the prefix  $\eta_0$  contain all the client actions preceding the first call or return action in  $\xi_0$ . The trace  $\xi_{k+1}$  is constructed from the trace  $\xi_k$  by applying the following lemma for  $\tau_1 = \eta_k$ ,  $\tau_1\tau_2 = \xi_k$ ,  $H_1 = S_k$  and  $H_1\psi H_2 = S$ .

**Lemma 13.** *Consider a well-formed core history  $H_1\psi H_2$ , where  $\psi \in \text{CallRetAct}$ , and a well-formed client trace  $\tau_1\tau_2$  such that*

$$\text{corehistory}(\tau_1) = H_1, \quad (2)$$

$$\text{corehistory}(\tau_1\tau_2) \sqsubseteq_{\pi} H_1\psi H_2, \quad (3)$$

where  $\pi$  is an identity on actions from  $H_1$  in  $\text{corehistory}(\tau_1\tau_2)$ . Then there exist traces  $\tau'_2$  and  $\tau''_2$  such that  $\tau_1\tau'_2\tau''_2$  is a well-formed trace and

$$\tau_1\tau_2 \sim_{\rho} \tau_1\tau'_2\tau''_2, \quad (4)$$

$$\text{corehistory}(\tau_1\tau'_2) = H_1\psi, \quad (5)$$

$$\text{corehistory}(\tau_1\tau'_2\tau''_2) \sqsubseteq_{\pi'} H_1\psi H_2, \quad (6)$$

where  $\pi'$  is an identity on actions from  $H_1\psi$  in  $\text{corehistory}(\tau_1\tau'_2\tau''_2)$  and  $\rho$  is an identity on actions from  $\tau_1$  in  $\tau_1\tau_2$ .

It is easy to see that for all  $i, j$  with  $i < j$  and for all prefixes  $\eta_i$  and  $\eta_j$  of the traces  $\xi_i$  and  $\xi_j$  thus constructed,  $\eta_i$  is a prefix of  $\eta_j$ . Hence, the sequence of traces  $\eta_k$  has a limit trace  $\tau'$  such that for every  $k$ ,  $\eta_k$  is a prefix of  $\tau'$  and  $\text{corehistory}(\tau') = S$ , which shows that Lemma 13 indeed entails Lemma 11.

To prove Lemma 13, we convert  $\tau_1\tau_2$  into  $\tau_1\tau'_2\tau''_2$  by applying a finite number of the following transformations that preserve its properties of interest, described by the proposition below.

**Proposition 14.** *Let  $\tau$  be a well-formed client trace and  $H$  a well-formed core history such that  $\text{corehistory}(\tau) \sqsubseteq_{\pi} H$ . Then swapping any two adjacent actions  $\varphi_1$  and  $\varphi_2$  in  $\tau$  executed by different threads such that*

1.  $\varphi_1 \in \text{CallAct}$  and  $\varphi_2 \notin \text{RetAct}$ ; or
2.  $\varphi_2 \in \text{RetAct}$  and if  $\varphi_1 \in \text{CallAct}$ , then  $\varphi_2$  precedes  $\varphi_1$  in  $H$ ,

yields a well-formed trace  $\tau'$  such that  $\tau \sim_\rho \tau'$  and  $\text{corehistory}(\tau') \sqsubseteq_{\pi'} H$  for the following bijections  $\pi'$  and  $\rho$ .

The bijection  $\pi'$  is defined as follows. If  $\varphi_1 \in \text{ClientAct}$  or  $\varphi_2 \in \text{ClientAct}$ , then  $\pi' = \pi$ . Otherwise, let  $i$  be the index of  $\varphi_1$  in  $\text{corehistory}(\tau)$ . Then  $\pi'(i+1) = \pi(i)$ ,  $\pi'(i) = \pi(i+1)$  and  $\pi'(k) = \pi(k)$  for  $k \notin \{i, i+1\}$ .

The bijection  $\rho$  is defined as follows. Let  $j$  be the index of  $\varphi_1$  in  $\tau$ . Then  $\rho'(j+1) = \rho(j)$ ,  $\rho'(j) = \rho(j+1)$  and  $\rho'(k) = \rho(k)$  for  $k \notin \{j, j+1\}$ .

**Proof of Lemma 13.** From (2) and (3) it follows that  $\tau_2 = \tau'_3 \psi \tau'_4$  for some traces  $\tau'_3$  and  $\tau'_4$ . We have two cases.

1.  $\psi \in \text{CallAct}$ . Then  $\tau'_3$  cannot contain a return action  $\varphi$ , because in this case  $\varphi$  would precede  $\psi$  in  $\text{corehistory}(\tau_1 \tau_2)$ . However,  $\varphi \in H_2$  and, thus,  $\psi$  precedes  $\varphi$  in  $H_1 \psi H_2$ , so this would contradict (3). Hence, there are no return actions in  $\tau'_3$ . Moreover, since  $\tau_1 \tau_2$  is well-formed, for any call action  $\varphi = (t, \text{call } m(u))$  in  $\tau'_3$  there are no actions by the thread  $t$  in  $\tau'_3$  following  $\varphi$ . Thus, we can move all call actions in the subtrace  $\tau'_3$  of  $\tau_1 \tau_2$  to the position right after  $\psi$  by swapping adjacent actions in  $\tau_1 \tau_2$  a finite number of times as described in Proposition 14(1). We thus obtain the trace  $\tau_1 \tau''_3 \psi \tau''_4 \tau'_4$ , where  $\tau''_4$  consists of call actions in  $\tau'_3$  and  $\tau''_3$  of the rest of actions in the subtrace. Conditions (4)–(6) then follow from Proposition 14(1) and the transitivity of  $\sim$  for  $\tau'_2 = \tau''_3 \psi$  and  $\tau'_2 = \tau''_4 \tau'_4$ .

2.  $\psi \in \text{RetAct}$ . Since the history  $H_1 \psi H_2$  is well-formed, the matching call of  $\psi$  is in  $H_1$ . From (2) and (3) it then follows that this call is not in  $\tau'_3$ . Furthermore, since the trace  $\tau_1 \tau_2$  is well-formed, the thread that executed  $\psi$  does not execute any actions in the subtrace in  $\tau'_3$ . Thus, we can move the action  $\psi$  to the beginning of  $\tau'_3$  by swapping adjacent actions in  $\tau_1 \tau_2$  a finite number of times as described in Proposition 14(2). We thus obtain the trace  $\tau_1 \psi \tau'_3 \tau'_4$ . Conditions (4)–(6) then follow from Proposition 14(2) and the transitivity of  $\sim$  for  $\tau'_2 = \psi \tau'_3$  and  $\tau'_2 = \tau'_3 \tau'_4$ .

#### B.4 Proof of Lemma 12

Take  $\tau \in \llbracket C(\cdot) \rrbracket$  and  $\eta$  such that  $\tau \sim \eta$ . Let us fix the bijection  $\pi$  used to establish this equivalence. We consider only the case that  $\tau$  is infinite (the finite case is easier and can be handled using the same ideas). Since  $\tau \sim \eta$ , we have

$$\text{visible}(\tau) = \text{visible}(\eta).$$

Furthermore, there exists a  $\tau$ -labelled computation sequence from some initial configuration  $\sigma_0 \in \text{CConfig}$  such that each step of the sequence uses the relation  $\longrightarrow_{C(\cdot)}$ . That is, if  $\tau = \varphi_1 \varphi_2 \varphi_3 \dots$ , we have

$$\sigma_0 \xrightarrow{\varphi_1}_{C(\cdot)} \sigma_1 \xrightarrow{\varphi_2}_{C(\cdot)} \sigma_2 \xrightarrow{\varphi_3}_{C(\cdot)} \sigma_3 \xrightarrow{\varphi_4}_{C(\cdot)} \dots \quad (7)$$

for some  $\sigma_i \in \text{CConfig}$ . Using this computation sequence for  $\tau$ , we construct a series of finite computation sequences and define the desired computation sequence for  $\eta$  as the limit of this series.

The starting point of the series is the empty sequence  $\sigma_0$ . To construct the  $(i+1)$ -st element of the series, we make three assumptions about the  $i$ -th one:

1. The  $i$ -th computation sequence has the form

$$\sigma'_0 \xrightarrow{\psi_1}_{C(\cdot)} \sigma'_1 \xrightarrow{\psi_2}_{C(\cdot)} \sigma'_2 \xrightarrow{\psi_3}_{C(\cdot)} \dots \xrightarrow{\psi_i}_{C(\cdot)} \sigma'_i,$$

where  $\sigma'_0 = \sigma_0$ , the trace  $\psi_1 \dots \psi_i$  is a prefix of  $\eta$  and  $\sigma'_1, \dots, \sigma'_i \in \text{CConfig}$ .

2. For all  $j \leq i$ , if  $\tau_1$  is a finite prefix of  $\tau$  such that  $\text{visible}(\tau_1) = \text{visible}(\psi_1 \dots \psi_j)$ , then

$$\text{core}(\sigma_{|\tau_1|}) = \text{core}(\sigma'_j).$$

3. For all  $j \leq i$  and  $t \in \{1, \dots, n\}$ , if  $\tau_1$  is a finite prefix of  $\tau$  such that  $\tau_1|_t = (\psi_1 \dots \psi_j)|_t$ , then

$$\sigma_{|\tau_1|}(t) = \sigma'_j(t) \quad \wedge \quad \sigma_{|\tau_1|}(\text{retval}_t) = \sigma'_j(\text{retval}_t).$$

Under these assumptions, we extend the given  $i$ -th computation sequence by the  $(i+1)$ -st action of  $\eta$ . The result of this extension becomes the  $(i+1)$ -st sequence, which as we show, meets the three assumptions described above.

Let  $\psi_{i+1}$  be the  $(i+1)$ -st action of  $\eta$ . To find a desired computation sequence, we only need to find a client configuration  $\sigma'_{i+1}$  such that

$$\sigma'_i \xrightarrow{\psi_{i+1}}_{C(\cdot)} \sigma'_{i+1}$$

and  $\sigma'_{i+1}$  satisfies assumptions 2 and 3 above. We show that such a  $\sigma'_{i+1}$  exists by a case analysis on  $\psi_{i+1}$ .

–  $\psi_{i+1} = (t, \text{Client}(c))$  for some  $t \in \{1, \dots, n\}$  and  $c \in \text{PComm}$ . Let  $\varphi_k$  be the action of  $\tau$  that is mapped to  $\psi_{i+1}$  by  $\pi$ . Then, the computation sequence of  $\tau$  in (7) gives us the transition:

$$\sigma_{k-1} \xrightarrow{\varphi_k}_{C(\cdot)} \sigma_k. \quad (8)$$

Let  $\sigma_k = (\text{pc}_k, (s_k, h_k))$  and  $\sigma'_i = (\text{pc}'_i, (s'_i, h'_i))$ . We define  $s'_{i+1}$  and  $\sigma'_{i+1}$  as follows:

$$s'_{i+1}(x) = \begin{cases} s'_i(x), & \text{if } x \text{ is } \text{retval}_{t'} \text{ for } t' \neq t; \\ s_k(x), & \text{otherwise;} \end{cases}$$

$$\sigma'_{i+1} = (\text{pc}_i[t : \text{pc}_k(t)], (s'_{i+1}, h_k)).$$

We show that  $\sigma'_{i+1}$  is the desired configuration. Since  $\pi$  preserves the order of actions from  $\text{ClientAct}$ ,  $\text{visible}(\varphi_1 \dots \varphi_{k-1}) = \text{visible}(\psi_1 \dots \psi_i)$ . Then assumption 2 for the  $i$ -th computation sequence implies

$$\text{core}(\sigma_{k-1}) = \text{core}(\sigma'_i).$$

Furthermore, since  $\pi$  preserves the order of actions within the same thread,  $(\varphi_1 \dots \varphi_{k-1})|_t = (\psi_1 \dots \psi_i)|_t$ . Then assumption 3 for the  $i$ -th computation sequence implies

$$\sigma_{k-1}(t) = \sigma'_i(t) \quad \wedge \quad \sigma_{k-1}(\text{retval}_t) = \sigma'_i(\text{retval}_t).$$

Recall that the transitions of thread  $t$  do not access the positions of other threads or  $\text{retval}_{t'}$  for  $t' \neq t$ . Additionally,  $\varphi_k = \psi_{i+1}$ . Hence, transition (8) and the definition of  $\sigma'_{i+1}$  entails that the following transition is also possible:

$$\sigma'_i \xrightarrow{\psi_{i+1}}_{C(\cdot)} \sigma'_{i+1}.$$

Now it remains to show that  $\sigma'_{i+1}$  satisfies the conditions in assumptions 2 and 3. To handle assumption 2, consider a finite prefix  $\tau_1$  of  $\tau$  such that  $\text{visible}(\tau_1) = \text{visible}(\psi_1 \dots \psi_{i+1})$ . Then

$$\text{core}(\sigma_{|\tau_1|}) = \text{core}(\sigma_k).$$

But  $\text{core}(\sigma_k) = \text{core}(\sigma'_{i+1})$  by the definition of  $\sigma'_{i+1}$ . Hence  $\text{core}(\sigma_{|\tau_1|}) = \text{core}(\sigma'_{i+1})$ , as desired. For assumption 3, we take an arbitrary thread  $t' \in \{1, \dots, n\}$  and consider a finite prefix  $\tau_1$  of  $\tau$  such that  $\tau_1|_{t'} = (\psi_1 \dots \psi_{i+1})|_{t'}$ . If  $t' \neq t$ , we have

$$\tau_1|_{t'} = (\psi_1 \dots \psi_i \psi_{i+1})|_{t'} = (\psi_1 \dots \psi_i)|_{t'}.$$

Hence, by assumption 3 on  $\sigma'_i$ ,

$$\sigma_{|\tau_1|}(t') = \sigma'_i(t') \quad \wedge \quad \sigma_{|\tau_1|}(\text{retval}_{t'}) = \sigma'_i(\text{retval}_{t'}).$$

On the other hand, by the definition of  $\sigma'_{i+1}$ ,

$$\sigma'_i(t') = \sigma'_{i+1}(t') \quad \wedge \quad \sigma'_i(\text{retval}_{t'}) = \sigma'_{i+1}(\text{retval}_{t'}).$$

From the four equalities above, the condition in assumption 3 follows. If  $t' = t$ ,

$$\sigma_{|\tau_1|}(t') = \sigma_k(t') = \sigma'_{i+1}(t') \quad \wedge \quad \sigma_{|\tau_1|}(\text{retval}_{t'}) = \sigma_k(\text{retval}_{t'}) = \sigma'_{i+1}(\text{retval}_{t'}),$$

which again implies the condition in assumption 3.

- $\varphi \in (t, \text{call } m(u'))$  for some  $t \in \{1, \dots, n\}$  and  $u' \in \text{Val}$ . Let  $\varphi_k$  be the action of  $\tau$  that is mapped to  $\psi_{i+1}$  by  $\pi$ . Then, the computation sequence of  $\tau$  in (7) gives us the transition:

$$\sigma_{k-1} \xrightarrow{\varphi_k} C(\cdot) \sigma_k. \quad (9)$$

Let  $m(E)$  be the instruction executed by this transition. Then,

$$\llbracket E \rrbracket \sigma_{k-1} = u. \quad (10)$$

Now, define  $\sigma'_{i+1}$  as identical to  $\sigma'_i$  except  $\sigma'_{i+1}(t) = \sigma_k(t)$ . We show that  $\sigma'_{i+1}$  is the configuration we are looking for. Since  $\pi$  preserves the order of actions within threads,  $(\varphi_1 \dots \varphi_k)|_t = (\psi_1 \dots \psi_{i+1})|_t$ . As  $\varphi_k$  and  $\psi_{i+1}$  are the same action by thread  $t$ , this implies

$$(\varphi_1 \dots \varphi_{k-1})|_t = (\psi_1 \dots \psi_i)|_t.$$

Hence, assumption 3 for the  $i$ -th computation sequence gives us

$$\sigma_{k-1}(t) = \sigma'_i(t) \quad \wedge \quad \sigma_{k-1}(\text{retval}_t) = \sigma'_i(\text{retval}_t). \quad (11)$$

We now argue that for all variables  $x$  local to thread  $t$

$$\sigma_{k-1}(x) = \sigma'_i(x). \quad (12)$$

Note that (11) already takes care of the case when  $x$  is  $\text{retval}_t$ . For the rest of the variables, we consider two cases, depending on whether or not  $(\psi_1 \dots \psi_i)|_t$  contains any actions in  $\text{ClientAct}$ . First, assume that it does not contain them. In this case,  $(\varphi_1 \dots \varphi_{k-1})|_t$  does not contain any actions from  $\text{ClientAct}$  either. Since only such actions by thread  $t$  can change variables  $x$  local to thread  $t$  other than  $\text{retval}_t$ , for all such variables  $x$  we have

$$\sigma_{k-1}(x) = \sigma_0(x) = \sigma'_i(x).$$

Hence, (12) holds in this case. Next, assume that  $(\varphi_1 \dots \varphi_{k-1})|_t$  contains an action from  $\text{ClientAct}$ . Let  $\psi_j$  be the last action from  $\text{ClientAct}$  in  $(\psi_1 \dots \psi_i)|_t$ , and  $\varphi_l$  the corresponding action in  $(\varphi_1 \dots \varphi_{k-1})|_t$ . In this case,

$$\text{visible}(\varphi_1 \dots \varphi_l) = \text{visible}(\psi_1 \dots \psi_j).$$

So, by assumption 2 on  $\sigma'_j$ , we have that

$$\text{core}(\sigma_l) = \text{core}(\sigma'_j).$$

Furthermore, by the choice of  $\psi_j$  and  $\varphi_l$ , if  $x$  is a variable local to thread  $t$  and it is not  $\text{retval}_t$ , then

$$\sigma_{k-1}(x) = \sigma_t(x) \quad \wedge \quad \sigma'_i(x) = \sigma'_j(x).$$

From the three equations above (12) follows.

It is now time to use (12). Recall that the parameter expression  $E$  can include only variables local to the thread  $t$ . Furthermore, because of (12), all  $t$ -local variables have the same values in  $\sigma_{k-1}$  and  $\sigma'_i$ . Hence,

$$\llbracket E \rrbracket \sigma_{k-1} = \llbracket E \rrbracket \sigma'_i. \quad (13)$$

From (9)-(13) and the definition of  $\sigma'_{i+1}$ , it follows that

$$\sigma'_i \xrightarrow{\psi_{i+1}}_{C(\cdot)} \sigma'_{i+1}.$$

It remains to show that  $\sigma'_{i+1}$  satisfies the requirements in assumptions 2 and 3. The requirement for assumption 2 holds for  $\sigma'_{i+1}$ , because

$$\text{visible}(\psi_1 \dots \psi_i) = \text{visible}(\psi_1 \dots \psi_{i+1}) \quad \wedge \quad \text{core}(\sigma'_i) = \text{core}(\sigma'_{i+1})$$

and  $\sigma'_i$  already satisfies the same requirement. Our proof for requirement 3 is the same as in the previous case.

- $\psi_{i+1} = (t, \text{ret } m(u))$  for some  $t \in \{1, \dots, n\}$  and  $u \in \text{Val}$ . Let  $\varphi_k$  be the action in the trace  $\tau$  that is related to  $\psi_{i+1}$  by the bijection  $\pi$ . Then, the computation sequence of  $\tau$  in (7) gives us the transition:

$$\sigma_{k-1} \xrightarrow{\varphi_k}_{C(\cdot)} \sigma_k.$$

Since  $\pi$  preserves the order of actions by the same thread,  $(\varphi_1 \dots \varphi_{k-1})|_t = (\psi_1 \dots \psi_i)|_t$ . Hence, by assumption 3 for the  $i$ -th computation sequence,

$$\sigma'_i(t) = \sigma_{k-1}(t).$$

Let  $\sigma'_{i+1}$  be the same as  $\sigma'_i$  except  $\sigma'_{i+1}(\text{retval}_t) = \sigma_k(\text{retval}_t)$  and  $\sigma'_{i+1}(t) = \sigma_k(t)$ . Then

$$\sigma'_i \xrightarrow{\psi_{i+1}}_{C(\cdot)} \sigma'_{i+1}.$$

Assumption 2 holds for  $\sigma'_{i+1}$  because  $\text{core}(\sigma'_i) = \text{core}(\sigma'_{i+1})$ ,  $\text{visible}(\psi_1 \dots \psi_i) = \text{visible}(\psi_1 \dots \psi_i \psi_{i+1})$  and  $\sigma'_i$  already satisfies assumption 2. The remaining assumption 3 follows from the definition of  $\sigma'_{i+1}$  and the fact that only the actions by thread  $t$  can change its thread position and the  $\text{retval}_t$  variable.  $\square$

## C Proof of Theorem 9 and Additional Material for Section 6

**Reduction from lock-freedom to termination.** For completeness, we repeat the reduction from lock-freedom to termination from [6]. For a library  $A = \{m = C_m \mid m \in M\}$  let  $\llbracket A \rrbracket_1$  be defined like  $\llbracket A \rrbracket$  (see §3), but where the CFG of thread  $t$  in  $\text{MGC}_n(A)$  is  $(N_t, T_t, v_{\text{mgc}}^t, \text{end}_{\text{mgc}}^t)$  with  $N_t = \{v_{\text{mgc}}^t \mid t = 1..n\} \cup \{\text{end}_{\text{mgc}}^t \mid t = 1..n\}$  and  $T_t = \{(v_{\text{mgc}}^t, m(u), \text{end}_{\text{mgc}}^t) \mid m \in M, u \in \text{Val}\}$ . Thus,  $\llbracket A \rrbracket_1$  defines the set of traces of an arbitrary number of library operations running in parallel. We can now formulate the reduction from lock-freedom to termination we described informally in §6.

**Theorem 15 ([6]).** *A library  $A$  is lock-free if and only if there are no infinite traces in  $\llbracket A \rrbracket_1$ .*

**Proof Theorem 9.** By contrapositive, assume  $\llbracket C(A_1) \rrbracket$  has an infinite trace  $\tau$ . From Lemma 10(1), we have that  $\text{lib}(\tau) \in \llbracket A_1 \rrbracket$ . If  $\text{client}(\tau)$  is finite, then the trace  $\text{lib}(\tau)$  has infinitely many actions from  $\text{LibAct}$ , but only finitely many from  $\text{CallRetAct}$ . By the definition of  $\llbracket A_1 \rrbracket$ , this means that  $\text{history}(\text{lib}(\tau))$  does not satisfy LF, which contradicts the lock-freedom of  $A_1$ .

Assume now  $\text{client}(\tau)$  is infinite. By Theorem 4, there exists a trace  $\tau' \in \llbracket C(A_3) \rrbracket$  with infinitely many actions from  $\text{ClientAct} \cup \text{CallRetAct}$ . From this trace we can easily construct an infinite trace  $\tau'' \in \llbracket C(A_2) \rrbracket$  if we replace any divergence at  $\text{skip}^\circ$  in  $A_3$  by starving the corresponding thread. (Note that we can do this because the semantics in Figure 1 allows for unfair schedulers.) This contradicts the assumptions of the theorem.  $\square$

### Counterexample to the compositionality of lock-freedom under fair scheduling.

We now provide a counterexample showing that lock-freedom under fair scheduling is not compositional. Consider the following library  $A_1$ :

```
int x = 1;
void wait() { while (x == 0); }
void blip() { x = 0; x = 1; }
```

and another library  $B$  built on top of  $A_1$ :

```
int y = 0;
void m1() { wait(); y = 1; }
void m2() { while (y == 0) blip(); }
```

The library  $A_1$  is lock-free under fair scheduling: in a program using it some method always terminates. This may not be true under an unfair one, which can suspend a `blip` operation forever in between  $x = 0$  and  $x = 1$ . The library  $A_1$  is also linearizable with respect to the specification

$$A_3 = \{\text{wait} = \text{blip} = (\text{skip}^\circ; \text{skip}; \text{skip}^\circ)\}.$$

The library  $B$  is lock-free assuming that it uses

$$A_2 = \{\text{wait} = \text{blip} = \text{skip}\}.$$

However, the library  $B$  implemented in terms of  $A_1$  is not lock-free: `m2` can continually execute `blip`, which will prevent `wait` in `m1` from returning. The statement `y = 1` in `m1`, which could stop `blips`, will thus never be executed.