


# Polynomial-Time Verification and Testing of Implementations of the Snapshot Data Structure

Gal Amram ✉ 

Ben Gurion University of the Negev, IBM Research

Avi Hayoun ✉

Ben Gurion University of the Negev

Lior Mizrahi

Ben Gurion University of the Negev

Gera Weiss ✉

Ben Gurion University of the Negev

---

## Abstract

We analyze correctness of implementations of the snapshot data structure in terms of linearizability. We show that such implementations can be verified in polynomial time. Additionally, we identify a set of representative executions for testing and show that the correctness of each of these executions can be validated in linear time. These results present a significant speedup considering that verifying linearizability of implementations of concurrent data structures, in general, is EXPSPACE-complete in the number of program-states, and testing linearizability is NP-complete in the length of the tested execution. The crux of our approach is identifying a class of executions, which we call *simple*, such that a snapshot implementation is linearizable if and only if all of its simple executions are linearizable. We then divide all possible non-linearizable simple executions into three categories and construct a small automaton that recognizes each category. We describe two implementations (one for verification and one for testing) of an automata-based approach that we develop based on this result and an evaluation that demonstrates significant improvements over existing tools. For verification, we show that restricting a state-of-the-art tool to analyzing only simple executions saves resources and allows the analysis of more complex cases. Specifically, restricting attention to simple executions finds bugs in 27 instances, whereas, without this restriction, we were only able to find 14 of the 30 bugs in the instances we examined. We also show that our technique accelerates testing performance significantly. Specifically, our implementation solves the complete set of 900 problems we generated, whereas the state-of-the-art linearizability testing tool solves only 554 problems.

**2012 ACM Subject Classification** Software and its engineering → Formal software verification; Theory of computation → Concurrent algorithms

**Keywords and phrases** Snapshot, Linearizability, Verification, Formal Methods

**Digital Object Identifier** 10.4230/LIPIcs...

**Funding** This research was partially funded by grant no. 2714/19 from the Israel Science Foundation and by the Lynn and William Frankel Center for Computer Science at Ben-Gurion University.

## 1 Introduction

As concurrency is very effective for accelerating the performance of computer programs, there is much scientific research and practical attention on the design, implementation, and verification of data structures that allow parallel access. We focus on the well-known *snapshot* data structure which is an essential building block of distributed arrays [4, 7, 9]. This data structure allows asynchronous processes to write values to a shared array of single-writer registers, by executing **update** operations, and to take instantaneous snapshots of the array values, by executing **scan** operations. It is useful for allowing processes to share information while maintaining a correct joint view of the data.



© Gal Amram, Avi Hayoun, Lior Mizrahi, and Gera Weiss;  
licensed under Creative Commons License CC-BY 4.0



Leibniz International Proceedings in Informatics  
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

For proving the correctness of implementations of the snapshot data structure, we consider the standard *linearizability* [32] condition. Roughly speaking, linearizability is the requirement that for every execution of a given implementation, the procedure executions can be ordered linearly such that (a) the resulting linear order is consistent with the definition of the data structure; (b) it preserves the precedence of procedure executions in time. In the specific case of snapshot, the definition of the data structure is that a sequential (linear) execution is correct if every **scan** operation reports the value written by the last **update** operation of each of the processes. Linearizability is widely accepted as a correctness criterion since, effectively, it formulates the requirement that procedure executions are seen to a user as if they were executed one after the other (i.e., atomically).

Automatic verification of linearizability is known to be computationally expensive. The verification of finite-state implementations is EXPSPACE-complete in the number of program states [5, 30] and undecidable for infinite-state implementations [14]. Testing linearizability, i.e., deciding whether a given execution is linearizable, is NP-complete [28]. These complexities do not stop the community from pursuing effective verification and testing techniques, because it is very difficult to provide correct implementations of concurrent data structures; bugs have been found in both academic and deployed implementations [18, 20, 44]. These made it clear that there is an acute necessity for reliable verification and testing techniques.

One commonly used technique is the *linearization points* based verification approach, which often does not work in the case of snapshot. A linearization point of a procedure execution is an action that represents the moment at which the procedure “actually occurs”. Once fixed linearization points are identified, verifying linearizability becomes PSPACE-complete [14]. Unfortunately, snapshot implementations do not usually admit fixed linearization points (e.g., all twelve published implementations listed in [36] do not admit such points). Researchers also suggested using linearization points as an optimization: ask the user to provide them (whether fixed or conditional) and use this information to accelerate verification [3, 6, 13, 52]. However, practice shows that it is difficult to find and specify the linearization points of snapshot implementations, even in a conditional manner. One difficulty is that the linearization points of **scan** operations often belong to other, parallel, procedure executions (see [4, 11, 48]).

**In this paper, we propose an effective polynomial-time technique for verifying snapshot implementations, and an effective linear-time technique for testing snapshot executions.** The crux of our techniques is an optimization approach that exponentially reduces the number of reachable program states. Specifically, we prove that if an algorithm is data-independent [56] then, in order to verify its correctness, it suffices to consider only a small fraction of its executions which we call *simple*.

The simple executions that we focus on are those in which:

1. All but two processes invoke only **update**( $v_0$ ) and **scan** operations, where  $v_0$  is the initial value of the array segments. In other words,  $n-2$  of the  $n$  processes are not allowed to change the initial value in their segments;
2. Each of the two remaining processes may only change their data value once, to a predetermined value: it executes only **update**( $v_0$ ) and **scan** operations up to an arbitrary point in the execution, after which it transitions to executing only **update**( $v_1$ ) and **scan** operations, where  $v_1 \neq v_0$  are fixed data values.

The focus on simple executions reduces the number of reachable states significantly, as  $n-2$  entries of the array are essentially constants (see Section 3).

After showing that it is enough to verify the correctness of simple executions, we continue and show that every non-linearizable simple execution falls into one of three categories that we

identify. Moreover, we show that each of these three possible bug patterns can be recognized by an automaton with at most  $n$  states and  $n^2$  transitions (see Section 4). This enables verifying linearizability of snapshot implementations via a reachability check applied to the graph product of the implementation and the automata where the target states of the reachability are the automata's accepting states. As there are  $O(n^2)$  combinations to choose the two excluded processes, snapshot implementations can be verified with this method in time  $O(mn^4)$  where  $m$  is the number of reachable states via simple executions (which is significantly smaller than the number of reachable states via all executions). Furthermore, by feeding a simple execution to these automata, an execution of length  $l$  can be tested in time  $O(l)$ . As it is sufficient to consider simple executions, this effectively means that snapshot executions can be tested in linear-time (see Section 5).

We have implemented and evaluated the proposed verification and testing techniques and ran them against state-of-the-art tools. For verification, we compared with the PAT [46] model checker. The results show that our approach allows deeper exploration of implementations from the literature. This allowed us to detect 27 of 30 inserted bugs, compared to 16 found by the baseline method. Furthermore, we managed to verify an algorithm by Bowman [17] for three and four processes, whereas the baseline method failed to do so. For testing, we compared with the linearizability testing tool proposed by Lowe [43]. The results show that our testing technique is robust and scalable and that it can cope with much longer histories than the baseline (see Section 7).

Due to lack of space, we give proof sketches and skip technical details. The complete proofs and all the details necessary for verification of the results are given as appendices.

## 2 Preliminaries

This section presents definitions and notations used throughout this paper. Appendix A provides further definitions, required for all complete proofs, and extended discussions.

Let  $Vals$  be an infinite set of abstract data values, and let  $v_0 \in Vals$  be the distinguished value used to initialize the segments of a snapshot. For  $n \in \mathbb{N}$ , let  $p_0, \dots, p_{n-1}$  be processes. We model an execution of a snapshot algorithm by the processes as a sequence of actions. Among the actions the processes perform, we are interested in the invocations and responses of procedure executions. For process  $p_i$  and data values  $u, u_0, \dots, u_{n-1}$ ,  $inv.update_i(u)$ ,  $res.update_i$ ,  $inv.scan_i$ ,  $res.scan_i(u_0, \dots, u_{n-1})$  are  $p_i$ -actions. Let  $\Sigma$  be the set of all such actions.

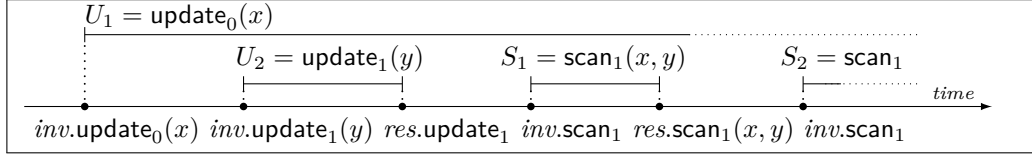
Throughout the paper, we refer to these actions using general terms such as: an **update** invocation, a **scan** response, a  $p_i$ -invocation etc., which are defined in a straightforward manner. For example, we may say that the action  $res.scan_i(u_0, \dots, u_{n-1})$  is a **scan** response, or a  $p_i$ -action, etc.

A *history* is a word  $h$  over  $\Sigma$  that exhibits the following properties:

1. For every process  $p_i$ , the first  $p_i$ -action in  $h$ , if any, is a  $p_i$ -invocation.
2. For every  $p_i$ -**update** (respectively, **scan**) invocation in  $h$ , the following  $p_i$ -action in  $h$ , if any, is a  $p_i$ -**update** (respectively, **scan**) response.
3. For every  $p_i$ -response in  $h$ , the following  $p_i$ -action, if any, is a  $p_i$ -invocation.

An operation is an execution of an **update/scan** procedure. We identify operations in histories with their invocation and response actions. Operations that do not return are identified by their invocation alone.

A *complete operation* in a history  $h = \alpha_0 \cdots \alpha_m$  is a pair of actions,  $(\alpha_k, \alpha_l)$ , where  $k < l$ ,  $\alpha_k$  is an  $update_i$  (respectively,  $scan_i$ ) invocation,  $\alpha_l$  is an  $update_i$  (respectively,  $scan_i$ )



■ **Figure 1** A linearizable history.  $U_2$ ,  $S_1$  are complete, while  $U_1$ ,  $S_2$  are pending ops.

response, and there is no  $p_i$ -action in between. A *pending operation* in  $h$  is a single action,  $(\alpha_k)$ , where  $\alpha_k$  is a  $p_i$ -invocation, and there is no  $p_i$ -action that follows  $\alpha_k$  in  $h$ .

Similarly to actions, we refer to operations using general terms: an operation  $O$  is, e.g., a  $p_i$ -operation, an **update** operation, a **scan** $_i(u_0, \dots, u_{n-1})$  operation, etc. In a history  $h$ , for an **update** $(u)$  operation  $U$ , we write  $val_h(U) = u$ , and for a **scan** $(u_0, \dots, u_{n-1})$  operation  $S$  and  $i < n$ , we write  $val_{h:i}(S) = u_i$  and  $val_h(S) = (u_0, \dots, u_{n-1})$ .

For a complete operation  $A = (\alpha_k, \alpha_l)$  and an operation  $B \in \{(\alpha_m, \alpha_t), (\alpha_m)\}$  in a history  $h = \alpha_0 \alpha_1 \dots$ , we write  $A <_h B$  if  $l < m$ . Clearly,  $<_h$  is a partial order over the operations in  $h$ , in which pending operations are maximal elements. Figure 1 illustrates a two-process history with pending and complete operations.

Linearizability [32] is the standard correctness condition for concurrent data structures. Roughly speaking, a history  $h$  is linearizable if the partial ordering  $<_h$  can be extended to a linear ordering that satisfies the sequential specification of the snapshot data structure. That is, each scan operation  $S$  returns in each entry  $i$  the value written by the maximal **update** $_i$  operation that precedes it. The extension should include all complete operations, and each pending operation is either completed or omitted.

We now turn to define the linearizability condition formally:

► **Definition 1.** A history  $h$  is linearizable if it can be extended into a history  $h'$  by appending zero or more response events to  $h$ , such that there exists a linear ordering  $\prec_{h'}$  of the complete operations in  $h'$  that satisfies the following conditions:

1. For  $A, B \in h$ , if  $A <_h B$ , then  $A \prec_{h'} B$ .
2. If  $S \in h'$  is a **scan** operation and  $U_i \in h'$  is the maximal **update** $_i$  operation such that  $U_i \prec_{h'} S$ , then  $val_h(U_i) = val_{h:i}(S)$ . If no **update** $_i$  operation precedes  $S$  in  $h'$ , then  $val_{h:i}(S) = v_0$ .

Any  $\prec_{h'}$  that satisfies these conditions is said to be a linearization of  $h$ .

► **Example 2.** The history depicted in Figure 1 is linearizable by the order  $U_1 \prec_h U_2 \prec_h S_1$ . To obtain a linearization, we completed the pending operation  $U_1$ , as its value is read by  $S_1$ . However, we chose to omit the pending scan operation  $S_2$ .

Our main goal is to analyze the linearizability of snapshot algorithms, defined as follows:

► **Definition 3 (Snapshot Linearizability).** A snapshot algorithm is linearizable if all of its histories are linearizable.

The data independence property, proposed by Wolper [56], roughly means that the behavior of an algorithm does not depend on the data values passed as arguments to the procedure executions. The formal definition employs the notion of a *renaming*: a function  $f: Vals \rightarrow Vals$ . An algorithm is data-independent if for a every history  $h$  of the algorithm and a renaming  $f$ : (1) the history  $f(h)$ , obtained by replacing each data value  $u$  with  $f(u)$ ,

is also a history of the algorithm; and (2) if  $h = f(h')$ , then  $h'$  is a history of the algorithm. See Appendix B for more details.

Data independence is natural to assume, as snapshot implementations synchronize accesses to a shared resource and thus are expected to be value-agnostic. This is substantiated by all twelve different published implementations [4, 7–11, 26, 35–37, 48] listed in [36].

Finally, a history is *differentiated* if no two **update** operations in it were invoked with the same data value.<sup>1</sup> Abdulla et al. [1] showed that it is sufficient to consider *differentiated* histories to prove linearizability of data-independent algorithms.

### 3 Simple Histories

In this section, we identify a set of histories, which we name *simple*. We then prove that a data-independent snapshot implementation is linearizable if and only if all of its simple histories are linearizable. Therefore, this section shows that it is sufficient to consider only some histories to determine the linearizability of data-independent snapshot implementations.

In a simple history, the **update** operations are invoked with only two distinct values. The first is the initial value  $v_0$ , and without loss of generality, we take some other  $v_1 \in Vals$  as the second value. All but two processes invoke only **update**( $v_0$ ) and **scan** operations. The remaining two execute only **update**( $v_0$ ) and **scan** operations, and at some (possibly different) point, each of the two processes shifts to executing only **update**( $v_1$ ) and **scan** operations.

► **Definition 4** (Simple histories). *A history  $h$  of  $n$  processes is  $(i, j)$ -simple for  $i < j < n$ , if there are  $r_i, r_j \in \mathbb{N}$  such that the following conditions hold:*

1. *Let  $U$  be the  $r$ -th **update** <sub>$i$</sub>  operation in  $h$ . If  $r < r_i$ , then  $U$  is an **update** <sub>$i$</sub> ( $v_0$ ) operation, and if  $r \geq r_i$ , then  $U$  is an **update** <sub>$i$</sub> ( $v_1$ ) operation.*
2. *In the same way, let  $U$  be the  $r$ -th **update** <sub>$j$</sub>  operation in  $h$ . If  $r < r_j$ , then  $U$  is an **update** <sub>$j$</sub> ( $v_0$ ) operation, and if  $r \geq r_j$ , then  $U$  is an **update** <sub>$j$</sub> ( $v_1$ ) operation.*
3. *Any **update** <sub>$k$</sub>  operation is an **update** <sub>$k$</sub> ( $v_0$ ) operation, if  $k \notin \{i, j\}$ .*

*A history  $h$  is simple if it is  $(i, j)$ -simple for some  $i < j < n$ .*

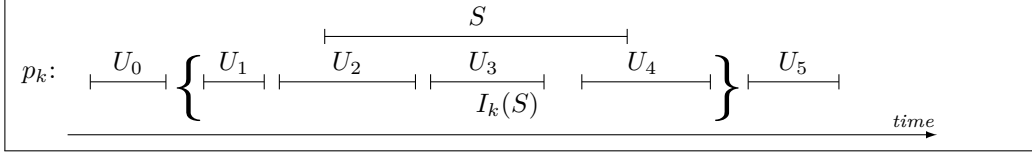
We are ready to prove the sufficiency of focusing on simple histories. We provide a proof sketch below and a rigorous proof in Appendix C.

► **Theorem 5.** *A data-independent snapshot algorithm  $\mathcal{L}_{\text{snap}}$  is linearizable if and only if all its simple histories are linearizable.*

**Proof sketch.** Anderson’s shrinking lemma identifies five properties that are equivalent to the linearizability of a snapshot history [8]. To prove the non-trivial direction of theorem 5 (‘if’), we assume that  $\mathcal{L}_{\text{snap}}$  is not linearizable. Consider some non-linearizable differentiated history  $h$ . Since  $\mathcal{L}_{\text{snap}}$  is not linearizable,  $h$  violates (at least) one of the shrinking lemma’s properties. Based on the violated property, we construct a renaming  $f: Vals \rightarrow \{v_0, v_1\}$ , and apply it to  $h$  to obtain a non-linearizable simple history. ◀

► **Remark 6.** In the context of simple histories, **scan** operations return  $v_0$  in all entries except for entries  $i$  and  $j$ . Thus, for the remainder of this paper, we use  $\text{res.scan}_k(u_i, u_j)$  as shorthand for  $\text{res.scan}_k(v_0, \dots, v_0, u_i, v_0, \dots, v_0, u_j, v_0, \dots, v_0)$ .

<sup>1</sup> For generating differentiated histories, a minor modification is required: we should allow different initial values for the array segments. See comment in Appendix B



■ **Figure 2** The  $k$ -th interval of  $S$ ,  $I_k(S)$

► **Remark 7.** From this point on, for readability, we will use 0 and 1 instead of  $v_0$  and  $v_1$ , respectively.

#### 4 A Simple Condition for the Linearizability of Simple Histories

In this section, we formulate three properties that are equivalent to the linearizability of an  $(i, j)$ -simple history. We then show that the negation of each property is regular, and present a construction of a matching automaton. Before providing our properties (in upcoming Theorem 10), we discuss each intuitively and explain why it is mandatory for linearizability.

**Property 1: No Inversion.** Assume that a scan operation  $S_1$  returns 0 at the  $i$ th entry (for example), while  $S_2$  returns 1. This indicates that  $S_2$  read a more recent value from the  $i$ th segment. Hence, in any linearization,  $S_1$  must precede  $S_2$ . As the same reasoning goes for the  $j$ th entry, it is forbidden for  $S_1$  to return 0 and 1 at the  $i$ th and  $j$ th entries, while  $S_2$  returns the opposite values.

**Property 2: Non-Decreasing.** If a scan operation  $S_1$  precedes a scan operation  $S_2$ , then  $S_2$  must obtain more recent values from all array segments. Therefore, it is forbidden for  $S_1$  to return 1 in entry  $k \in \{i, j\}$ , while  $S_2$  returns 0 in its  $k$ th entry.

**Property 3: Appropriateness.** We require that for each scan operation there are “appropriate” update operations,  $U_i$  by  $p_i$  and  $U_j$  by  $p_j$ , that we can linearize before  $S$ . “Appropriate” means that the next three conditions hold.

**First condition.** The timings of the update operations must not prevent them from being linearized before  $S$ . For example, they must not succeed  $S$ . Formally, we require that they belong to the *interval of  $S$* , defined below and illustrated in Figure 2:

► **Definition 8.** Let  $S$  be a scan operation in a history  $h$ , and let  $k < n$ . The  $k$ th interval of  $S$ , denoted  $I_k(S)$ , is the set of  $\text{update}_k$  operations  $U \in h$  such that:

1.  $\neg(S <_h U)$ .
2. There is no  $\text{update}_k$  operation  $U'$  such that  $U <_h U' <_h S$ .

**Second condition.** The values of the update operations  $U_i$  and  $U_j$  are the values returned by  $S$  in its corresponding entries.

**Third condition.** There is no, e.g.,  $\text{update}_i$  operation between  $U_i$  and  $U_j$ . This is because the existence of such an  $\text{update}_i$  operation, say  $U_i < U'_i < U_j$ , would prevent us from linearizing both  $U_i$  and  $U_j$  before  $S$ .

We formalize the notion of appropriateness in the following definition:

► **Definition 9.** Let  $S$  be a complete scan operation in an  $(i, j)$ -simple history  $h$ . A pair  $(U_i, U_j)$  where  $U_i$  is an  $\text{update}_i$  operation and  $U_j$  is an  $\text{update}_j$  operation, is said to be  $S$ -appropriate, if:

1.  $U_i \in I_i(S)$  and  $U_j \in I_j(S)$ .

2.  $(val_h(U_i), val_h(U_j)) = (val_{h:i}(S), val_{h:j}(S))$ .
3. There is no  $update_i$  operation  $U'_i$  such that  $U_i < U'_i < U_j$ , and there is no  $update_j$  operation  $U'_j$  such that  $U_j < U'_j < U_i$ .

So far, we have presented our properties and explained intuitively why they form a necessary condition for linearizability: i.e., why their negation prevents linearizability. The main theorem of this section asserts a much stronger claim: these properties also constitute a sufficient condition for linearizability. We provide a proof for Theorem 10 in Appendix D.

► **Theorem 10.** *An  $(i, j)$ -simple history  $h$  is linearizable if and only if the following properties hold.*

**No Inversion.** *There are no complete scan operations  $S_1$  and  $S_2$  in  $h$  such that  $(val_{h:i}(S_1), val_{h:j}(S_1)) = (0, 1)$  and  $(val_{h:i}(S_2), val_{h:j}(S_2)) = (1, 0)$ .*

**Non-Decreasing.** *If  $S_1$  and  $S_2$  are two complete scan operations in  $h$  such that  $S_1 <_h S_2$ , then  $val_{h:i}(S_1) \leq val_{h:i}(S_2)$  and  $val_{h:j}(S_1) \leq val_{h:j}(S_2)$ .*

**Appropriateness.** *For each complete scan operation  $S$  in  $h$ , there exists an  $S$ -appropriate pair of update operations.*

## 4.1 Detecting Incorrect Simple Histories

Finally, we show that the properties of Theorem 10 can be detected by an NFA. We provide here proof sketches for most claims, and full proofs for all claims in Appendix E.

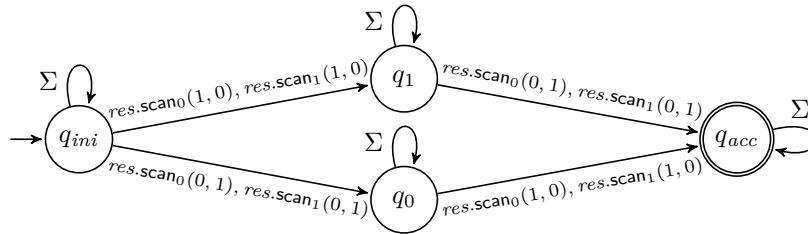
► **Theorem 11.** *For  $i < j < n$ , there exists an automaton  $M$  with  $O(n)$  states and  $O(n^2)$  transitions, such that an  $(i, j)$ -simple history  $h$  is not linearizable if and only if  $h \in L(M)$ .*

To prove Theorem 11, we construct automata that detect violations of the three properties presented in Theorem 10.

### 4.1.1 Detecting Violations of No-Inversion

► **Proposition 12.** *There exists an automaton  $M_1$  such that, for any  $(i, j)$ -simple history  $h$ ,  $h$  violates No-Inversion if and only if  $h \in L(M_1)$ . Moreover,  $M_1$  has  $O(1)$  states and  $O(n)$  transitions.*

**Proof sketch** We demonstrate the construction for the case that  $n = 2$ :

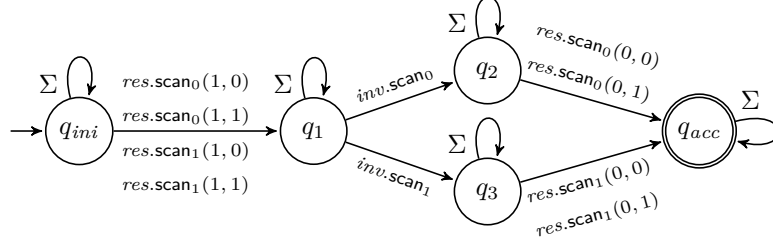


### 4.1.2 Detecting Violations of Non-Decreasing

► **Proposition 13.** *There exists an automaton  $M_2$  such that, for any  $(i, j)$ -simple history  $h$ ,  $h$  violates Non-Decreasing if and only if  $h \in L(M_2)$ . Moreover,  $M_2$  has  $O(n)$  states and  $O(n^2)$  transitions.*



**Proof sketch** As an illustrative demonstration, we present below a simpler automaton. It detects the existence of a violation of Non-Decreasing, for  $n = 2$ , and  $S_1 < S_2$  where  $val_{h:i}(S_1) = 1$ .



### 4.1.3 Detecting Violations of Appropriateness

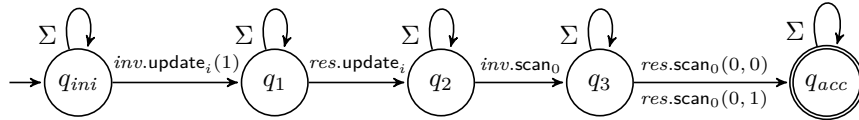
It remains to construct an automaton that accepts all  $(i, j)$ -simple histories that violate Appropriateness. To this end, we reformulate Appropriateness as a regular safety property; a word is rejected if and only if it has a “bad”-prefix.

► **Lemma 14.** *Let  $h$  be an  $(i, j)$ -simple history, and let  $S$  be a complete scan operation in  $h$ . For  $l \in \{i, j\}$ , let  $F_l$  be the first  $update_l(1)$  operation in  $h$ , if exists. Then, there is no  $S$ -appropriate pair in  $h$  if and only if any of the following holds:*

1. *For  $l \in \{i, j\}$ ,  $F_l$  exists,  $val_{h:l}(S) = 0$ , and  $F_l <_h S$ .*
2. *For  $l \in \{i, j\}$ ,  $val_{h:l}(S) = 1$ , and either  $S <_h F_l$  or  $F_l$  doesn't exist.*
3.  *$(val_{h:i}(S), val_{h:j}(S)) = (0, 1)$  and  $F_i <_h F_j$ .*
4.  *$(val_{h:i}(S), val_{h:j}(S)) = (1, 0)$  and  $F_j <_h F_i$ .*

► **Proposition 15.** *There exists an automaton  $M_3$  such that, for any  $(i, j)$ -simple history  $h$ ,  $h$  violates Appropriateness if and only if  $h \in L(M_3)$ . Moreover,  $M_3$  has  $O(n)$  states and  $O(n^2)$  transitions.*

**Proof sketch** The automaton is a “union” of four automata, such that the  $k$ th automaton checks whether there exists a complete scan operation  $S$  for which the  $k$ th case of Lemma 14 holds. Below, we provide an automaton that identifies the first case where  $l = i$  and  $S$  is a  $scan_0$  operation (for  $n = 2$ ). Hence, in fact, the first case is a union of  $2n$  automata. We leave it for the reader to verify that (rather simple) automata exist for all other cases.



► **Corollary 16.** *Theorem 11 is trivially correct by propositions 12, 13, and 15.*

## 5 Verifying and Testing Linearizability

The results of the previous section allow us to both verify data-independent snapshot implementations, and test the linearizability of simple snapshot histories, in polynomial time.

For verifying a data-independent snapshot implementation, by Theorem 5, it is sufficient to verify that all of its simple histories are linearizable. Theorem 11 allows one to apply



model checking of regular properties [12, Chapter 4.2], i.e., one can check whether the implementation admits an  $(i, j)$ -simple history accepted by the automaton (and thus not linearizable). As there are  $O(n^2)$  valuations for  $i$  and  $j$ , our first key result follows:

► **Theorem 17** (Polynomial-time verification). *Let  $\mathcal{L}_{\text{snap}}$  be a data-independent snapshot algorithm such that only finitely many states of  $\mathcal{L}_{\text{snap}}$  are reachable by its simple histories. Determining the linearizability of  $\mathcal{L}_{\text{snap}}$  is decidable in  $O(mn^4)$  time, where  $m$  is the size of an automaton that accepts all simple histories of  $\mathcal{L}_{\text{snap}}$ .*

Moreover, Theorem 11 enables the testing of simple histories efficiently, by feeding the automaton of Theorem 11 (or its determinization) with the  $(i, j)$ -simple histories to be tested. The automaton will report acceptance once it identifies a non-linearizable prefix of the input history  $h$  (which testifies that  $h$  is not linearizable). Hence, our second key result follows.

► **Theorem 18** (Linear-time testing). *For  $i < j < n$ ,  $(i, j)$ -simple histories can be tested in linear-time, i.e., in time  $O(|h|)$ .*

## 6 Optimization: Omitting Redundant Commands

The focus on simple histories yields an optimization that can significantly reduce the state space of an examined snapshot algorithm, speeding up its verification. The optimization relies on the observation that in the executions of  $(i, j)$ -simple histories, some commands are vacuous. To elaborate, assume that register  $R$  stores the data value of process  $p_k$ ,  $k \neq i, j$ . In all executions of  $(i, j)$ -simple histories,  $R$  will only ever store the value 0. Thus, read and write commands from and to  $R$  can be ignored, reducing the possible values of the program counters. In some cases, we can even ignore  $R$  altogether, reducing the number of registers.

We use Bowman's obstruction-free snapshot algorithm [17] (Algorithm 1) to demonstrate the optimization. During an **update** operation, process  $p_k$  writes its new value to register  $A[k]$  (line 3). During a **scan** operation, the values stored in  $A[0], \dots, A[n-1]$  are read into the local variables  $a[0], \dots, a[n-1]$  (lines 7-8). Let  $i < j$  be two process ids, and consider executions of  $(i, j)$ -simple histories of Algorithm 1. In such executions, every write command to register  $A[k]$ ,  $k \notin \{i, j\}$ , writes 0. Hence, we may ignore and omit all registers  $A[k]$ ,  $k \notin \{i, j\}$ . This yields a simplified version of the algorithm, as shown in Algorithm 2, which has a substantially smaller state space than Algorithm 1, as it employs fewer registers. Since we omitted only vacuous commands (i.e. commands that always write and read 0) Algorithm 2 is linearizable if and only if all of Algorithm 1's  $(i, j)$ -simple histories are linearizable.

## 7 Implementation and Evaluation

In this section, we describe implementations of the procedures described in Section 5, and the experiments we performed to evaluate their efficiency. We provide the means to reproduce all experiments in the paper's supporting materials [51].

### 7.1 Implementation of our Verification Procedures

We used the model checker PAT [46] as the basis for our two verification approaches. PAT contains a system for checking the linearizability of a given concurrent algorithm against an abstract specification, via refinement [40, 42]. We made use of this system in our first verification approach: we encoded known snapshot algorithms from the literature (listed in

■ **Algorithm 1** Unoptimized algorithm

---

```

1: procedure updatek(v)
2:   Active ← ⊥
3:   A[k] ← v

4: procedure scank
5:   repeat
6:     Active ← k
7:     for ℓ = 0, ..., n-1 do
8:       a[ℓ] ← A[ℓ]
9:   until Active = k
10:  return (a[0], ..., a[n-1])

```

---

■ **Algorithm 2** Optimized for (i, j)-simple executions

---

```

1: procedure updatek                                ▷ k ∉ {i, j}
2:   Active ← ⊥

3: procedure updater(v)                                ▷ r ∈ {i, j}
4:   Active ← ⊥
5:   A[r] ← v

6: procedure scanq                                    ▷ q < n
7:   repeat
8:     Active ← q
9:     a[i] ← A[i]
10:    a[j] ← A[j]
11:  until Active = q
12:  return (0, ..., 0, a[i], 0, ..., 0, a[j], 0, ..., 0)

```

---

■ **Figure 3** Illustration of the redundant command omission optimization with Bowman’s algorithm.

subsection 7.4), modified to admit only simple histories. We provided a matching abstract simple-history snapshot specification.

For our second approach, we encoded the automaton from Theorem 11 in PAT. As that automaton is a union of several automata, we treated each one as a separate process, and encoded the union as the parallel composition of these processes. We exploited PAT’s reachability checker to encode the accepting states of the automaton. We then asked PAT to check whether the algorithms listed in subsection 7.4 admit any simple histories that are accepted by the automaton.

We note three sources of possible errors in our implementations: (1) We could have encoded the snapshot algorithms incorrectly. (2) We could have encoded the automata or the abstract specification incorrectly. (3) PAT itself may have bugs. To mitigate the first two threats, we used PAT’s linearizability system to ensure that the algorithms we encoded are linearizable, that we manage to find several artificially-inserted bugs, and that the reachability approach agrees with PAT’s standard refinement approach. We did not take steps to mitigate the third threat, but as PAT is a widely used model checker which has itself been partially model-checked [50], our confidence in its correctness is high., our confidence in its correctness is high.

## 7.2 Implementation of our Testing Procedure

The testing procedure we implemented receives an (i, j)-simple history, and runs it through an implementation of the automaton described in Theorem 11. The tool announces whether the automaton accepts the history, indicating it is not linearizable, or it rejects the history, indicating it is linearizable.

To validate that our implementation has no bugs, we generated hundreds of random simple histories, both linearizable and non-linearizable, and ensured our implementation classified them correctly.

### 7.3 Research Questions

We start with research questions related to our verification technique. As we propose a model checking approach, although polynomial, it still suffers from the state explosion problem [23]. This holds since the algorithms we check admit an enormous number of states, even when we restrict ourselves to simple histories. Model-checking approaches are mainly evaluated based on their feasibility; their ability to verify correctness/find bugs, perhaps only up to a reasonable depth, measured in the number of operations each process executes, with real-world resources: realistic time and space and limitations. Hence, we formulate the following research questions:

**RQ1** Does the focus on simple histories help to prove/disprove correctness, in terms of feasibility/depth to be processed?

**RQ2** Is our polynomial-time technique efficient for proving/disproving correctness, in terms of feasibility/depth to be processed?

We use the following research question to evaluate our testing technique:

**RQ3** Is our testing technique efficient, in terms of feasibility, and time and space consumption?

### 7.4 Corpus

To address RQ1 and RQ2, we constructed a corpus for our experiments that includes several snapshot algorithms from the literature: An obstruction-free [31] algorithm by Bowman [17], denoted BOWMAN; A snapshot algorithm by Jayanti [36], denoted JAYANTI; The bounded and unbounded versions of Afek et al. [4], denoted AFEK1 and AFEK2, respectively; and A snapshot algorithm by Riany et al [48], denoted RIANY.

For each algorithm and  $n \in \{3, 4, 5, 6\}$  processes, we encoded the original version (denoted ‘full’), as well as a modified version which generates only  $(0, 1)$ -simple histories, with the optimization detailed in Section 6 (denoted ‘simple-only’). Then, for  $n \in \{3, 4, 5, 6, 8, 10\}$ , we also encoded buggy versions thereof (denoted, ‘buggy-full’ and ‘buggy-simple-only’, respectively). Overall, we created 100 configurations of pairs of algorithm encoding with  $n$  processes.

To address RQ3, we began by generating 25 linearizable histories of length  $l \in \{200, 500, 1000\}$  with  $n \in \{5, 8, 11, 14, 17, 20\}$  processes, by randomly executing an atomic snapshot implementation, and recording its actions. We then generated 25 non-linearizable histories of length  $l \in \{50, 100, 200\}$  with  $n \in \{3, 4, 5, 6, 8, 10\}$  processes as follows: we generated a random linearizable history, and changed its 20-length suffix by randomly changing the values of the scan responses. We repeated this process until we obtained 25 non-linearizable histories. In the context of RQ3, we refer to a choice of  $l$ ,  $n$ , and ‘linearizable/non-linearizable’ as a configuration. This resulted in 900 histories, divided into 18 linearizable and 18 non-linearizable configurations, added to our corpus.

### 7.5 Experiments and Results

In this section, we detail the experiments we performed to tackle our research questions, and report our results. All experiments were performed on a rather ordinary laptop with an Intel Core i7-6820HK CPU and 32GB of DDR4 RAM, running Windows 10 21H1 and the WSL2 Ubuntu 20.04.2 image from Microsoft.

test	normal			simple			polynomial			normal			simple			polynomial		
	b	t	s	b	t	s	b	t	s	b	t	s	b	t	s	b	t	s
algorithm	3 processes									4 processes								
BOWMAN	$\infty$	11	0.64	$\infty$	2	0.1	$\infty$	2	0.3	3	168	12.0	$\infty$	60	0.5	$\infty$	54	0.6
JAYANTI	14	272	22.8	23	393	25.1	3	72	0.7	3	149	11.9	6	218	16.0	3	98	0.7
AFEK1	-	-	-	2	242	1.9	2	417	1.8	-	-	-	2	305	2.0	2	506	2.3
AFEK2	2	50	0.5	4	422	4.3	3	215	1.4	2	163	2.0	4	522	7.0	3	255	2.1
RIANY	6	285	4.1	9	445	5.4	27	595	2.0	3	172	12.1	6	275	17	24	512	1.9
algorithm	5 processes									6 processes								
BOWMAN	1	9	0.4	3	290	18.4	40	575	4.4	1	66	3.8	1	7	0.5	35	507	3.3
JAYANTI	1	141	0.9	3	253	18.4	3	118	0.7	1	302	4.6	2	590	28.1	3	142	0.7
AFEK1	-	-	-	2	417	4.0	-	-	-	-	-	-	-	-	-	-	-	-
AFEK2	1	21	0.4	3	441	18.4	3	298	2.6	1	95	4.2	1	7	0.5	3	326	2.8
RIANY	-	-	-	-	-	-	23	579	1.8	-	-	-	-	-	-	21	508	2.2
algorithm	8 processes									10 processes								
BOWMAN	-	-	-	1	288	15.6	33	554	2.7	-	-	-	-	-	-	30	558	2.9
JAYANTI	-	-	-	1	386	15.6	3	197	0.7	-	-	-	-	-	-	3	267	1.1
AFEK1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
AFEK2	-	-	-	1	256	15.7	3	402	3.2	-	-	-	-	-	-	3	491	3.6
RIANY	-	-	-	-	-	-	19	502	2.2	-	-	-	-	-	-	18	586	3.0

■ **Table 1** Results of bug detection in non-linearizable implementations. b: max bound on #operation per process, t: time used (sec.), and s: memory used (GB)

### 7.5.1 Verification Experiments

To address RQ1 and RQ2, we used PAT to verify the correctness of our configurations. We ran three different types of linearizability experiments:

- normal. Using PAT's standard linearizability checker with **full** and **buggy-full** configurations.
- simple. Using PAT's standard linearizability checker with **simple-only** and **buggy-simple-only** configurations.
- polynomial. Using PAT's reachability checker with **simple-only** and **buggy-simple-only** configurations, in parallel to the automaton threads that detect bugs.

Furthermore, for each configuration and matching experiment type, we limited the number of operations that each process was allowed to perform. As some algorithms employ infinite data types (e.g. integers), at least in those cases, the bound is mandatory for PAT to terminate. We set a timeout of 10 min. for buggy implementations, and 1 hr. for correct implementations. We repeated each experiment with various bounds until we found the maximal bound for which each experiment terminated in the allotted time.

► **Remark 19.** For **simple** configurations, we checked only  $(0, 1)$ -simple histories. For full verification, it is required to test all  $(i, j)$ -histories. Nevertheless, this observation does not affect the feasibility of the approach, since the tests for  $(i_0, j_0)$  and  $(i_1, j_1)$  simple histories are independent, and can even run on separate machines. Furthermore, symmetry arguments may increase confidence even when checking only  $(0, 1)$ -simple histories.

► **Remark 20.** We also tried to use Cave [21, 52] and its extension Poling [47, 57], static analysis-based linearizability verifiers. Unfortunately, despite our best efforts, we could not make either tool work for the algorithms we tried to encode. Even for toy correct and

test	normal			simple			polynomial			normal			simple			polynomial		
	b	t	s	b	t	s	b	t	s	b	t	s	b	t	s	b	t	s
algorithm	3 processes									4 processes								
BOWMAN	2	47	0.7	$\infty$	3	0.1	$\infty$	11	0.1	1	29	0.6	$\infty$	134	1.8	$\infty$	460	0.7
JAYANTI	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
AFEK1	1	113	1.0	1	15	0.2	1	31	0.3	-	-	-	-	-	-	-	-	-
AFEK2	1	12	0.2	2	2627	19.5	2	2675	7.5	-	-	-	1	154	1.9	1	269	1.5
RIANY	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
algorithm	5 processes									6 processes								
BOWMAN	-	-	-	1	158	1.4	1	121	0.5	-	-	-	-	-	-	-	-	-
JAYANTI	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
AFEK1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
AFEK2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
RIANY	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

■ **Table 2** Results of verification of linearizable implementations. b: max bound on #operation per process, t: time used (sec.), and s: memory used (GB)

incorrect algorithms that operate atomically, Cave reported errors, and Poling returned unexpected responses. Perhaps the snapshot object deviates from the types of data structures that these tools aim to handle. To the best of our knowledge, PAT, Cave, and Poling are the only available tools that verify linearizability automatically, without requiring additional input.

We present the bug-detection results in Table 1, and the verification results in Table 2. For each configuration and linearizability experiment type, we report the maximal bound on the number of operations per process, for which the experiment terminated before the timeout. If the experiment terminated without imposing a bound, we report the value  $\infty$ . Furthermore, for the max bound we found, we report time and space consumption by the corresponding linearizability experiment. As an example, for RIANY buggy-simple-only with 4 processes, when we ran the polynomial linearizability experiment, we found the bug while limiting each process to 24 operations. The execution took 512 sec. and consumed 1.9 GB. Accordingly, in the upper part of Table 1, the cells on the row titled ‘RIANY’ and the columns titled ‘polynomial; 4 processes’ read: b:24, t:512, and s:1.9.

## 7.5.2 Testing Experiments

To address RQ3, we tested all linearizable and non-linearizable generated histories, applying two methods: our implemented method, and a tool by Lowe [39, 43], with a 10 min. timeout. For each configuration and each tool, we report the percentage of tests that successfully terminated within the allotted time. Furthermore, for the terminated executions, we report the median running time and space consumption. Table 3 presents results for linearizable configurations, and Table 4 for non-linearizable configurations. As an example, when we applied our method to linearizable histories of length 500 with 20 processes, 100% of the tests were successful, the median running time was 0.15sec, and the median space consumption was 150MB. Hence, in Table 3, the cells on the rows titled ‘500;terminated’, ‘500;median time’, and ‘500;median space’ with the column titled ‘20;This paper’ read 100%, 0.15, and 150, respectively.

## XX:14 Polynomial-Time Verification and Testing of the Snapshot Data Structure

#processes		5		8		11		14		17		20	
len.	mt.	This paper	Lowe	This paper	Lowe	This paper	Lowe	This paper	Lowe	This paper	Lowe	This paper	Lowe
	term.												
200	time	100%	100%	100%	100%	100%	100%	100%	84%	100%	52%	100%	32%
	space	0.02	0.20	0.02	0.22	0.02	0.28	0.02	1.34	0.02	1.11	0.03	2.08
		130	336	131	352	131	360	131	456	131	444	132	1228
500	term.	100%	100%	100%	100%	100%	100%	100%	80%	100%	48%	100%	16%
	time	0.04	0.20	0.06	0.22	0.09	0.30	0.12	1.45	0.16	12.57	0.15	0.21
	space	132	216	136	336	140	352	144	492	150	2414	150	346
1000	term.	100%	100%	100%	100%	100%	100%	100%	72%	100%	44%	100%	16%
	time	0.07	0.21	0.14	0.21	0.21	0.33	0.33	1.36	0.40	3.29	0.56	0.85
	space	136	344	146	336	156	352	171	482	182	1620	203	398

■ **Table 3** Linearizable simple history testing results. Terminated tests (%), median time used (sec.), and median memory used (MB)

#processes		3		4		5		6		8		10	
len.	mt.	This paper	Lowe	This paper	Lowe	This paper	Lowe	This paper	Lowe	This paper	Lowe	This paper	Lowe
	term.												
50	time	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
	space	0.06	0.28	0.06	0.32	0.06	0.34	0.06	0.35	0.06	0.65	0.06	1.19
		129	336	129	348	129	336	129	344	129	368	129	440
100	term.	100%	100%	100%	100%	100%	84%	100%	52%	100%	32%	100%	8%
	time	0.03	0.48	0.03	1.45	0.03	3.76	0.03	24.61	0.03	61.93	0.03	179.80
	space	129	340	129	508	129	2784	129	17896	129	12996	129	12192
200	term.	100%	36%	100%	4%	100%	0%	100%	0%	100%	0%	100%	0%
	time	0.03	30.78	0.03	5.11	0.03	-	0.03	-	0.03	-	0.03	-
	space	129	20392	129	3216	129	-	129	-	129	-	129	-

■ **Table 4** Non-linearizable simple history testing results. Terminated tests (%), median time used (sec.), and median memory used (MB)

## 7.6 Analysis of the Results

Focusing on simple histories is beneficial, as both **simple** and **polynomial** outperform the **normal** linearizability method of PAT for finding bugs. In addition, overall, **polynomial** performs better than **simple** (see Table 1). **normal** found the bug in 14/30 cases, with up to 6 processes. **simple** succeeded in 3 additional cases with up to 8 processes, with **polynomial** succeeding in 26/30 cases with up to 10 processes. Importantly, **simple** allows for larger bounds than **normal** in 16/17 cases, and the same bound in the remaining case. **polynomial** allows for larger bounds than **simple** in 16 cases, and smaller bounds in 5 cases. This indicates that **polynomial** enables deeper exploration than **simple**, and thus we conclude that it is more efficient. Both **polynomial** and **simple** manage to explore implementations significantly deeper than **normal**. We also observe that **polynomial** consumes less space, which is the main bottleneck of model checking, than **simple**. The peak memory consumption we recorded for **polynomial** was 4.4GB, whereas the peak we recorded for **simple** was 25.1GB, and 9/20 executions with more than 10GB. While the peak we recorded for **normal** was 22.8GB, it scaled much worse than **simple** and failed to cope with the more challenging configurations.

In Table 2, we see that **simple** and **polynomial** enable the verification of BOWMAN with 3 and 4 processes. To the best of our knowledge, this is the first time that this algorithm has been verified to some extent. Model-checking techniques are complete and mainly efficient for

bug detection. Verifying a concurrent algorithm for 4 processes is noteworthy (compare, e.g., to the results of [41]). Yet, excluding these results, although both methods perform better than `normal`, we did not manage to verify other implementations. We mention that, in some old evaluations we performed, we used a prototype tool we wrote that uses simple histories (but does not employ the automata of Section 4.1), and managed to verify JAYANTI with 3 processes within 21 sec. (reference hidden for double-blind review). As this deviates from what Table 2 illustrates, we believe that further investigation is required.

Tables 3 and 4 show that our testing technique outperforms [43] by several orders of magnitude, mainly and most importantly, in terms of feasibility. Our tool easily handled all 900 histories, while the competitor failed to cope with challenging configurations, successfully handling only 554/900 histories. We also observe that our technique is scalable. The differences in time and space consumption between extremum values are negligible.

Moreover, we note that our technique is insensitive to the correctness of the tested history. In contrast, our competitor quickly fails over non-linearizable histories. To gain more confidence in this observation, we further generated 25 non-linearizable histories of length 1000 for 20 processes, with a linearizable prefix of length at least 980. Our tool handled all with a median running time of 0.55sec. Note that our competitor failed almost entirely over non-linearizable histories of length 200, with 3-10 processes.

## 8 Related Work

Alur et al. proposed an EXPSPACE-technique for verifying linearizability [5], and Hamza proved EXPSPACE-completeness [30]. Bouajjani et al. proved the undecidability of linearizability of infinite-state systems, and the PSPACE-completeness of linearizability with fixed linearization points [14].

Due to the high complexity of the problem, sound and complete model-checking techniques manage to perform limited verification with up to 3 processes [19, 41, 54]. [41] also verifies a stack implementation for 4 processes, but only by limiting the stack size to two data values. Hsu et al. [34] proposed a bounded model checking technique for hyper-LTL, and used it to rediscover known bugs (see [25]) in the “Snark” dequeue implementation [24].

Static analysis efforts are incomplete, but can work for infinite-state implementations. However, most ask for additional information from the user. [3, 6, 13, 52] ask for linearization points, some in a conditional manner. [2] ask for linearization policies. [49] ask for the specification of sub-operations and relations between them. Cave [21, 53] and Poling [57] work without further information. However, as we report in Section 7, we did not manage to work with these tools. Perhaps the snapshot object deviates from the types of data structures that these tools aim to handle.

The way we employ the data independence property resembles Abdulla et al. [1]. They ran automata in parallel to queue and stack implementations to detect bugs. Their approach is incomplete, but works for infinite-state implementations. However, their automata detect incorrect sequential histories, in contrast to concurrent histories as we do, and thus their approach requires specifying linearization points. It is rather simple to construct an automaton that detects incorrect sequential snapshot histories, hence their approach can be applied to the snapshot object straightforwardly. But, as linearization points of snapshot implementations are evasive, the benefit of doing so is questionable.

Other works also focused on specific data structures. Bouajjani et al. [15] prove that verification of data-independent queue, stack, register, and mutex implementations is PSPACE-complete for a fixed number of processes, and EXPSPACE-complete for infinitely many



processes. In [16], Bouajjani et al. extend the latter result to data-independent and projection-closed priority queues. To the best of our knowledge, those techniques have not been implemented or evaluated. Chakraborty et al. [22] identified conditions that are equivalent to the linearizability of data-independent queue implementations, and use them to automatically verify Herlihy and Wing's queue [32]. Abdulla et al. [3] used those conditions and the results of [22] to extend their static analysis technique [2] to verify stack and queue implementations without linearization points.

Wing and Gong considered the problem of testing linearizability, and gave an exponential-time algorithm [55]. Gibbons and Korach proved NP-completeness [28], and further showed that register-histories with  $k$  processes can be tested in time  $O(n2^{O(k)} + n \log n)$ . Lowe [43] suggested optimizations for the algorithm of [55]. Horn and Kroening suggested an optimization that applies to set implementations [33]. Emmi and Enea [27] identified a class of data structures for which a polynomial-time testing algorithm exists. This class includes queue, stack, set, and map, but does not include snapshot.

## 9 Conclusion

We proved that a data-independent snapshot algorithm is linearizable if and only if all of its simple histories are linearizable. This gives rise to an optimization for proving/disproving the correctness of snapshot implementations, i.e., examining only simple histories. This optimization can exponentially reduce the number of reachable states to inspect. Moreover, we proved that non-linearizable simple histories are identified by a polynomial-sized automaton. This enables a polynomial-time technique for verifying the linearizability of snapshot implementations, and a linear-time technique for testing the linearizability of snapshot histories. We implemented our techniques, and reported on evaluations that support the efficiency of our methods over existing techniques.

## Future Work

We wonder if the notion of simple histories can be replicated to other data structures. In particular, it would be interesting to investigate whether such an adaptation would admit automata-based verification/testing techniques similar to those we presented for the snapshot object. The automata presented in [14] seem like a good place to begin in order to define simple histories geared at queues and stacks. Another future direction is to extend our results to multi-writer snapshots, and to implementations that are strongly linearizable [45].

---

## References

- 1 Parosh Aziz Abdulla, Frédéric Haziza, Lukás Holík, Bengt Jonsson, and Ahmed Rezine. An integrated specification and verification technique for highly concurrent data structures for highly concurrent data structures. *Int. J. Softw. Tools Technol. Transf.*, 19(5):549–563, 2017. doi:10.1007/s10009-016-0415-4.
- 2 Parosh Aziz Abdulla, Bengt Jonsson, and Cong Quy Trinh. Automated verification of linearization policies. In Xavier Rival, editor, *Static Analysis - 23rd International Symposium, SAS 2016, Edinburgh, UK, September 8-10, 2016, Proceedings*, volume 9837 of *Lecture Notes in Computer Science*, pages 61–83. Springer, 2016. doi:10.1007/978-3-662-53413-7\_4.
- 3 Parosh Aziz Abdulla, Bengt Jonsson, and Cong Quy Trinh. Fragment abstraction for concurrent shape analysis. In Amal Ahmed, editor, *Programming Languages and Systems - 27th European Symposium on Programming, ESOP 2018, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2018, Thessaloniki, Greece, April 14-20, 2018*,

- Proceedings*, volume 10801 of *Lecture Notes in Computer Science*, pages 442–471. Springer, 2018. doi:10.1007/978-3-319-89884-1\_16.
- 4 Yehuda Afek, Hagit Attiya, Danny Dolev, Eli Gafni, Michael Merritt, and Nir Shavit. Atomic snapshots of shared memory. *J. ACM*, 40(4):873–890, 1993. doi:10.1145/153724.153741.
  - 5 Rajeev Alur, Kenneth L. McMillan, and Doron A. Peled. Model-checking of correctness conditions for concurrent objects. *Inf. Comput.*, 160(1-2):167–188, 2000. doi:10.1006/inco.1999.2847.
  - 6 Daphna Amit, Noam Rinetzky, Thomas W. Reps, Mooly Sagiv, and Eran Yahav. Comparison under abstraction for verifying linearizability. In Werner Damm and Holger Hermanns, editors, *Computer Aided Verification, 19th International Conference, CAV 2007, Berlin, Germany, July 3-7, 2007, Proceedings*, volume 4590 of *Lecture Notes in Computer Science*, pages 477–490. Springer, 2007. doi:10.1007/978-3-540-73368-3\_49.
  - 7 James H. Anderson. Composite registers. *Distributed Comput.*, 6(3):141–154, 1993. doi:10.1007/BF02242703.
  - 8 James H. Anderson. Multi-writer composite registers. *Distributed Comput.*, 7(4):175–195, 1994. doi:10.1007/BF02280833.
  - 9 James Aspnes and Maurice Herlihy. Wait-free data structures in the asynchronous PRAM model. In Frank Thomson Leighton, editor, *Proceedings of the 2nd Annual ACM Symposium on Parallel Algorithms and Architectures, SPAA '90, Island of Crete, Greece, July 2-6, 1990*, pages 340–349. ACM, 1990. doi:10.1145/97444.97701.
  - 10 Hagit Attiya, Maurice Herlihy, and Ophir Rachman. Efficient atomic snapshots using lattice agreement (extended abstract). In Adrian Segall and Shmuel Zaks, editors, *Distributed Algorithms, 6th International Workshop, WDAG '92, Haifa, Israel, November 2-4, 1992, Proceedings*, volume 647 of *Lecture Notes in Computer Science*, pages 35–53. Springer, 1992. doi:10.1007/3-540-56188-9\_3.
  - 11 Hagit Attiya and Ophir Rachman. Atomic snapshots in  $o(n \log n)$  operations. *SIAM J. Comput.*, 27(2):319–340, 1998. doi:10.1137/S0097539795279463.
  - 12 Christel Baier and Joost-Pieter Katoen. *Principles of model checking*. MIT Press, 2008.
  - 13 Josh Berdine, Tal Lev-Ami, Roman Manevich, G. Ramalingam, and Shmuel Sagiv. Thread quantification for concurrent shape analysis. In Aarti Gupta and Sharad Malik, editors, *Computer Aided Verification, 20th International Conference, CAV 2008, Princeton, NJ, USA, July 7-14, 2008, Proceedings*, volume 5123 of *Lecture Notes in Computer Science*, pages 399–413. Springer, 2008. doi:10.1007/978-3-540-70545-1\_37.
  - 14 Ahmed Bouajjani, Michael Emmi, Constantin Enea, and Jad Hamza. Verifying concurrent programs against sequential specifications. In Matthias Felleisen and Philippa Gardner, editors, *Programming Languages and Systems - 22nd European Symposium on Programming, ESOP 2013, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2013, Rome, Italy, March 16-24, 2013. Proceedings*, volume 7792 of *Lecture Notes in Computer Science*, pages 290–309. Springer, 2013. doi:10.1007/978-3-642-37036-6\_17.
  - 15 Ahmed Bouajjani, Michael Emmi, Constantin Enea, and Jad Hamza. On reducing linearizability to state reachability. *Inf. Comput.*, 261:383–400, 2018. doi:10.1016/j.ic.2018.02.014.
  - 16 Ahmed Bouajjani, Constantin Enea, and Chao Wang. Checking linearizability of concurrent priority queues. In Roland Meyer and Uwe Nestmann, editors, *28th International Conference on Concurrency Theory, CONCUR 2017, September 5-8, 2017, Berlin, Germany*, volume 85 of *LIPIcs*, pages 16:1–16:16. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2017. doi:10.4230/LIPIcs.CONCUR.2017.16.
  - 17 Jack R Bowman. Obstruction-free snapshot, obstruction-free consensus, and fetch-and-add modulo  $k$ . Technical report, Technical Report TR2011-681, Dartmouth College, Computer Science, Hanover, NH, 2011.
  - 18 Sebastian Burckhardt, Rajeev Alur, and Milo M. K. Martin. Checkfence: checking consistency of concurrent data types on relaxed memory models. In Jeanne Ferrante and Kathryn S. McKinley, editors, *Proceedings of the ACM SIGPLAN 2007 Conference on Programming*

- Language Design and Implementation, San Diego, California, USA, June 10-13, 2007*, pages 12–21. ACM, 2007. doi:10.1145/1250734.1250737.
- 19 Sebastian Burckhardt, Chris Dern, Madanlal Musuvathi, and Roy Tan. Line-up: a complete and automatic linearizability checker. In Benjamin G. Zorn and Alexander Aiken, editors, *Proceedings of the 2010 ACM SIGPLAN Conference on Programming Language Design and Implementation, PLDI 2010, Toronto, Ontario, Canada, June 5-10, 2010*, pages 330–340. ACM, 2010. doi:10.1145/1806596.1806634.
  - 20 Jacob Burnim, George C. Necula, and Koushik Sen. Specifying and checking semantic atomicity for multithreaded programs. In Rajiv Gupta and Todd C. Mowry, editors, *Proceedings of the 16th International Conference on Architectural Support for Programming Languages and Operating Systems, ASPLOS 2011, Newport Beach, CA, USA, March 5-11, 2011*, pages 79–90. ACM, 2011. doi:10.1145/1950365.1950377.
  - 21 CAVE Website. <https://people.mpi-sws.org/~viktor/cave/>. Last Accessed: Aug. 31, 2021.
  - 22 Soham Chakraborty, Thomas A. Henzinger, Ali Sezgin, and Viktor Vafeiadis. Aspect-oriented linearizability proofs. *Log. Methods Comput. Sci.*, 11(1), 2015. doi:10.2168/LMCS-11(1:20)2015.
  - 23 Edmund M. Clarke, William Klieber, Milos Nováček, and Paolo Zuliani. Model checking and the state explosion problem. In Bertrand Meyer and Martin Nordio, editors, *Tools for Practical Software Verification, LASER, International Summer School 2011, Elba Island, Italy, Revised Tutorial Lectures*, volume 7682 of *Lecture Notes in Computer Science*, pages 1–30. Springer, 2011. doi:10.1007/978-3-642-35746-6\_1.
  - 24 David Detlefs, Christine H. Flood, Alex Garthwaite, Paul Alan Martin, Nir Shavit, and Guy L. Steele Jr. Even better dcas-based concurrent dequeues. In Maurice Herlihy, editor, *Distributed Computing, 14th International Conference, DISC 2000, Toledo, Spain, October 4-6, 2000, Proceedings*, volume 1914 of *Lecture Notes in Computer Science*, pages 59–73. Springer, 2000. doi:10.1007/3-540-40026-5\_4.
  - 25 Simon Doherty, David Detlefs, Lindsay Groves, Christine H. Flood, Victor Luchangco, Paul Alan Martin, Mark Moir, Nir Shavit, and Guy L. Steele Jr. DCAS is not a silver bullet for nonblocking algorithm design. In Phillip B. Gibbons and Micah Adler, editors, *SPAA 2004: Proceedings of the Sixteenth Annual ACM Symposium on Parallelism in Algorithms and Architectures, June 27-30, 2004, Barcelona, Spain*, pages 216–224. ACM, 2004. doi:10.1145/1007912.1007945.
  - 26 Cynthia Dwork, Maurice Herlihy, Serge A. Plotkin, and Orli Waarts. Time-lapse snapshots. *SIAM J. Comput.*, 28(5):1848–1874, 1999. doi:10.1137/S0097539793243685.
  - 27 Michael Emmi and Constantin Enea. Sound, complete, and tractable linearizability monitoring for concurrent collections. *Proc. ACM Program. Lang.*, 2(POPL):25:1–25:27, 2018. doi:10.1145/3158113.
  - 28 Phillip B. Gibbons and Ephraim Korach. Testing shared memories. *SIAM J. Comput.*, 26(4):1208–1244, 1997. doi:10.1137/S0097539794279614.
  - 29 Rachid Guerraoui and Eric Ruppert. Linearizability is not always a safety property. In Guevara Noubir and Michel Raynal, editors, *Networked Systems - Second International Conference, NETYS 2014, Marrakech, Morocco, May 15-17, 2014. Revised Selected Papers*, volume 8593 of *Lecture Notes in Computer Science*, pages 57–69. Springer, 2014. doi:10.1007/978-3-319-09581-3\_5.
  - 30 Jad Hamza. On the complexity of linearizability. *Comput.*, 101(9):1227–1240, 2019. doi:10.1007/s00607-018-0596-7.
  - 31 Maurice Herlihy, Victor Luchangco, and Mark Moir. Obstruction-free synchronization: Double-ended queues as an example. In *23rd International Conference on Distributed Computing Systems (ICDCS 2003), 19-22 May 2003, Providence, RI, USA*, pages 522–529. IEEE Computer Society, 2003. doi:10.1109/ICDCS.2003.1203503.

- 32 Maurice Herlihy and Jeannette M. Wing. Linearizability: A correctness condition for concurrent objects. *ACM Trans. Program. Lang. Syst.*, 12(3):463–492, 1990. doi:10.1145/78969.78972.
- 33 Alex Horn and Daniel Kroening. Faster linearizability checking via p-compositionality. In Susanne Graf and Mahesh Viswanathan, editors, *Formal Techniques for Distributed Objects, Components, and Systems - 35th IFIP WG 6.1 International Conference, FORTE 2015, Held as Part of the 10th International Federated Conference on Distributed Computing Techniques, DisCoTec 2015, Grenoble, France, June 2-4, 2015, Proceedings*, volume 9039 of *Lecture Notes in Computer Science*, pages 50–65. Springer, 2015. doi:10.1007/978-3-319-19195-9\_4.
- 34 Tzu-Han Hsu, César Sánchez, and Borzoo Bonakdarpour. Bounded model checking for hyperproperties. In Jan Friso Groote and Kim Guldstrand Larsen, editors, *Tools and Algorithms for the Construction and Analysis of Systems - 27th International Conference, TACAS 2021, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2021, Luxembourg City, Luxembourg, March 27 - April 1, 2021, Proceedings, Part I*, volume 12651 of *Lecture Notes in Computer Science*, pages 94–112. Springer, 2021. doi:10.1007/978-3-030-72016-2\_6.
- 35 Prasad Jayanti. *f*-arrays: implementation and applications. In Aleta Ricciardi, editor, *Proceedings of the Twenty-First Annual ACM Symposium on Principles of Distributed Computing, PODC 2002, Monterey, California, USA, July 21-24, 2002*, pages 270–279. ACM, 2002. doi:10.1145/571825.571875.
- 36 Prasad Jayanti. An optimal multi-writer snapshot algorithm. In Harold N. Gabow and Ronald Fagin, editors, *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*, pages 723–732. ACM, 2005. doi:10.1145/1060590.1060697.
- 37 Lefteris M. Kirousis, Paul G. Spirakis, and Philippos Tsigas. Reading many variables in one atomic operation: Solutions with linear or sublinear complexity. *IEEE Trans. Parallel Distrib. Syst.*, 5(7):688–696, 1994. doi:10.1109/71.296315.
- 38 Leslie Lamport. Proving the correctness of multiprocess programs. *IEEE Trans. Software Eng.*, 3(2):125–143, 1977. doi:10.1109/TSE.1977.229904.
- 39 Linearizability Tester Website. <http://www.cs.ox.ac.uk/people/gavin.lowe/LinearizabilityTesting/>. Last Accessed: Aug. 31, 2021.
- 40 Yang Liu, Wei Chen, Yanhong A. Liu, and Jun Sun. Model checking linearizability via refinement. In Ana Cavalcanti and Dennis Dams, editors, *Proceedings of the Second World Congress on Formal Methods (FM'09)*, volume 5850 of *Lecture Notes in Computer Science*, pages 321–337. Springer, 2009.
- 41 Yang Liu, Wei Chen, Yanhong A. Liu, and Jun Sun. Model checking linearizability via refinement. In Ana Cavalcanti and Dennis Dams, editors, *FM 2009: Formal Methods, Second World Congress, Eindhoven, The Netherlands, November 2-6, 2009. Proceedings*, volume 5850 of *Lecture Notes in Computer Science*, pages 321–337. Springer, 2009. doi:10.1007/978-3-642-05089-3\_21.
- 42 Yang Liu, Wei Chen, Yanhong A. Liu, Jun Sun, Shao Jie Zhang, and Jin Song Dong. Verifying linearizability via optimized refinement checking. *IEEE Trans. Software Eng.*, 39(7):1018–1039, 2013. doi:10.1109/TSE.2012.82.
- 43 Gavin Lowe. Testing for linearizability. *Concurr. Comput. Pract. Exp.*, 29(4), 2017. doi:10.1002/cpe.3928.
- 44 Maged M Michael and Michael L Scott. Correction of a memory management method for lock-free data structures. Technical report, University of Rochester, Computer Science, 1995.
- 45 Sean Owens and Philipp Woelfel. Strongly linearizable implementations of snapshots and other types. In Peter Robinson and Faith Ellen, editors, *Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing, PODC 2019, Toronto, ON, Canada, July 29 - August 2, 2019*, pages 197–206. ACM, 2019. doi:10.1145/3293611.3331632.
- 46 PAT Website. <https://pat.comp.nus.edu.sg/>. Last Accessed: Aug. 31, 2021.
- 47 Poling Website. <https://github.com/rowangithub/Poling/>. Last Accessed: Aug. 31, 2021.

- 48 Yaron Riany, Nir Shavit, and Dan Touitou. Towards a practical snapshot algorithm. *Theor. Comput. Sci.*, 269(1-2):163–201, 2001. doi:10.1016/S0304-3975(00)00412-6.
- 49 Vineet Singh, Iulian Neamtiu, and Rajiv Gupta. Proving concurrent data structures linearizable. In *27th IEEE International Symposium on Software Reliability Engineering, ISSRE 2016, Ottawa, ON, Canada, October 23-27, 2016*, pages 230–240. IEEE Computer Society, 2016. doi:10.1109/ISSRE.2016.31.
- 50 Jun Sun, Yang Liu, and Bin Cheng. Model checking a model checker: A code contract combined approach. In Jin Song Dong and Huibiao Zhu, editors, *Formal Methods and Software Engineering - 12th International Conference on Formal Engineering Methods, ICFEM 2010, Shanghai, China, November 17-19, 2010. Proceedings*, volume 6447 of *Lecture Notes in Computer Science*, pages 518–533. Springer, 2010. doi:10.1007/978-3-642-16901-4\_34.
- 51 Supporting materials. [https://github.com/hayounav/Thesis\\_experiments/tree/main/snapshot%20verification%20and%20testing](https://github.com/hayounav/Thesis_experiments/tree/main/snapshot%20verification%20and%20testing).
- 52 Viktor Vafeiadis. Shape-value abstraction for verifying linearizability. In Neil D. Jones and Markus Müller-Olm, editors, *Verification, Model Checking, and Abstract Interpretation, 10th International Conference, VMCAI 2009, Savannah, GA, USA, January 18-20, 2009. Proceedings*, volume 5403 of *Lecture Notes in Computer Science*, pages 335–348. Springer, 2009. doi:10.1007/978-3-540-93900-9\_27.
- 53 Viktor Vafeiadis. Automatically proving linearizability. In Tayssir Touili, Byron Cook, and Paul B. Jackson, editors, *Computer Aided Verification, 22nd International Conference, CAV 2010, Edinburgh, UK, July 15-19, 2010. Proceedings*, volume 6174 of *Lecture Notes in Computer Science*, pages 450–464. Springer, 2010. doi:10.1007/978-3-642-14295-6\_40.
- 54 Martin T. Vechev and Eran Yahav. Deriving linearizable fine-grained concurrent objects. In Rajiv Gupta and Saman P. Amarasinghe, editors, *Proceedings of the ACM SIGPLAN 2008 Conference on Programming Language Design and Implementation, Tucson, AZ, USA, June 7-13, 2008*, pages 125–135. ACM, 2008. doi:10.1145/1375581.1375598.
- 55 Jeannette M. Wing and Chun Gong. Testing and verifying concurrent objects. *J. Parallel Distributed Comput.*, 17(1-2):164–182, 1993. doi:10.1006/jpdc.1993.1015.
- 56 Pierre Wolper. Expressing interesting properties of programs in propositional temporal logic. In *Conference Record of the Thirteenth Annual ACM Symposium on Principles of Programming Languages, St. Petersburg Beach, Florida, USA, January 1986*, pages 184–193. ACM Press, 1986. doi:10.1145/512644.512661.
- 57 He Zhu, Gustavo Petri, and Suresh Jagannathan. Poling: SMT aided linearizability proofs. In Daniel Kroening and Corina S. Pasareanu, editors, *Computer Aided Verification - 27th International Conference, CAV 2015, San Francisco, CA, USA, July 18-24, 2015, Proceedings, Part II*, volume 9207 of *Lecture Notes in Computer Science*, pages 3–19. Springer, 2015. doi:10.1007/978-3-319-21668-3\_1.



## A Extended Preliminaries

We present the basic definitions and notations used throughout this paper to model snapshot implementations, and to reason about their executions.

### A.1 Actions and Histories

Let  $Vals = \{v_0, v_1, v_2, \dots\}$  be an infinite set of abstract data values, and for  $n \in \mathbb{N}$ , let  $p_0, \dots, p_{n-1}$  be processes. We model an execution of a snapshot algorithm by the processes as a sequence of actions. Among the actions the processes perform, we are interested in the invocations and responses of procedure executions. For process  $p_i$  and data values  $u, u_0, u_1, \dots, u_{n-1}$ ,  $inv.update_i(u)$ ,  $res.update_i$ ,  $inv.scan_i$ ,  $res.scan_i(u_0, \dots, u_{n-1})$  are  $p_i$ -actions. Let  $\Sigma$  be the set of all such actions, i.e.,  $\Sigma$  is the union of the following sets:

- $\{inv.update_i(u) : i < n, u \in Vals\}$ ,
- $\{res.update_i : i < n\}$ ,
- $\{inv.scan_i : i < n\}$ ,
- and  $\{res.scan_i(u_0, \dots, u_{n-1}) : i < n, u_0, \dots, u_{n-1} \in Vals\}$ .

Throughout the paper, we refer to these actions using general terms such as: an **update** invocation, an  $update_i(u)$  invocation, a **scan** response, a  $p_i$ -invocation etc., which are defined in a straightforward manner. For example, we may say that the action  $res.scan_i(u_0, \dots, u_{n-1})$  is a **scan** response, or a  $p_i$ -action, or a  $scan_i(u_0, \dots, u_{n-1})$  response etc.

A *history* is a *well formed* word  $h$  over  $\Sigma$ . That is,  $h$  satisfies the following:

1. For every process  $p_i$ , the first  $p_i$ -action in  $h$ , if any, is a  $p_i$ -invocation.
2. For every  $p_i$ -**update** (respectively, **scan**) invocation in  $h$ , the following  $p_i$ -action in  $h$ , if any, is a  $p_i$ -**update** (respectively, **scan**) response.
3. For every  $p_i$ -response in  $h$ , the following  $p_i$ -action in  $h$ , if any, is a  $p_i$ -invocation.

An operation is an execution of an **update/scan** procedure. We identify operations in histories with their invocation and response actions. Operations that do not return are identified by their invocation alone.

► **Definition 21.** A complete operation in a history  $h = \alpha_0, \dots, \alpha_m$  is a pair of actions,  $(\alpha_k, \alpha_l)$ , where  $k < l$ ,  $\alpha_k$  is an  $update_i$  (respectively,  $scan_i$ ) invocation,  $\alpha_l$  is an  $update_i$  (respectively,  $scan_i$ ) response, and there is no  $p_i$ -action in between.

A pending operation in a history  $h = \alpha_0, \dots, \alpha_m$  is a single action,  $(\alpha_k)$ , where  $\alpha_k$  is a  $p_i$ -invocation, and there is no  $p_i$ -action that follows  $\alpha_k$  in  $h$ .

We consider all operations in a history  $h$  to be distinct, although, formally, this assumption is not entirely aligned with the above definition. To bridge this minor discrepancy, one may add an identifier to each operation, for example by allowing the processes to count their operations. Then, we would replace e.g. an update invocation  $inv.update_i(u)$  with  $inv.update_i(u, c_i)$  where  $c_i$  is the “serial number” of the procedure execution. To simplify the presentation and to avoid notation overloading, we omit this technical discussion and just note that this discrepancy can be easily settled. Therefore, the reader should keep in mind that operations started at different points in time are not equal, and there are standard ways to settle this formally.

As for actions, we refer to operations using general terms. Thus, we may say that an operation  $O$  is, e.g., a  $p_i$ -operation, an **update** operation, a  $scan_i(u_0, \dots, u_{n-1})$  operation etc. In a

history  $h$ , for an  $\text{update}(u)$  operation  $U$ , we write  $\text{val}_h(U) = u$ , and for a  $\text{scan}(u_0, \dots, u_{n-1})$  operation  $S$  and  $i < n$ , we write  $\text{val}_{h:i}(S) = u_i$  and  $\text{val}_h(S) = (u_0, \dots, u_{n-1})$ .

For a history  $h = \alpha_0, \dots, \alpha_m$ , a complete operation  $O = (\alpha_k, \alpha_l)$ , and a pending operation  $O' = (\alpha_t)$ , we write  $\text{begin}(O) = k$ ,  $\text{end}(O) = l$ ,  $\text{begin}(O') = t$  and  $\text{end}(O') = \infty$ . For two operations  $A, B$  in a history  $h$ , we write  $A <_h B$  if  $\text{end}(A) < \text{begin}(B)$ . Clearly,  $<_h$  is a partial ordering over the set of operations in  $h$ , in which pending operations are maximal elements.

## A.2 Linearizability

Roughly speaking, a history  $h$  is linearizable if the partial ordering  $<_h$  can be extended to a linear ordering that satisfies the sequential specification of the snapshot object. That is, each scan operation  $S$  returns in each entry  $i$  the value written by the maximal  $\text{update}_i$  operation that precedes it. The extension should include all complete operations, where each pending operations is either completed or omitted.

We take  $v_0$  to be a distinguished initial value of each entry. To avoid the tedious discussion about scan operations that return initial values, we assume that each history starts with  $n$  update operations, one by each process, that merely write the initial value  $v_0$  into each segment:

► **Assumption 1.** *For every history  $h$ , the first  $n$  operations in  $h$  are  $\text{update}_0(v_0), \dots, \text{update}_{n-1}(v_0)$ . These operations are complete, and precede all other operations.*

This assumption is justified by the following argument: If a history  $h$  fails to fulfill Assumption 1, we artificially add to  $h$  the prefix:  $\text{inv.update}_0(v_0) \text{ inv.update}_1(v_0) \dots \text{inv.update}_{n-1}(v_0) \text{ res.update}_0 \text{ res.update}_1 \dots \text{res.update}_{n-1}$ . It is not difficult to see that  $h$  is linearizable if and only if it remains linearizable after adding this prefix. Hence, it suffices to verify linearizability while imposing the discussed assumption.

We turn to define the linearizability condition in a formal manner. For a history  $h$ ,  $\text{COP}(h)$  denotes the set of all complete operations in  $h$ , and  $\text{OP}(h)$  is the set of all operations in  $h$ , pending and complete (and hence,  $\text{COP}(h) \subseteq \text{OP}(h)$ ). For a set of operations  $\text{COP}(h) \subseteq \mathcal{E} \subseteq \text{OP}(h)$ ,  $\mathcal{E}'$  is a completion of  $\mathcal{E}$  if  $\mathcal{E}'$  is obtained by adding to each pending operation in  $\mathcal{E}$  a matching response.

► **Definition 22.** *A history  $h$  is linearizable if there exists a set of operations  $\text{COP}(h) \subseteq \mathcal{E} \subseteq \text{OP}(h)$ , a completion  $\mathcal{E}'$  of  $\mathcal{E}$ , and a linear ordering  $\prec_h$  of  $\mathcal{E}'$  such that the following hold:*

1. *For  $A, B \in \mathcal{E}'$ , if  $A <_h B$ , then  $A \prec_h B$ .*
2. *If  $S \in \mathcal{E}'$  is a scan operation and  $U_i \in \mathcal{E}'$  is the maximal  $\text{update}_i$  operation such that  $U_i \prec_h S$ , then  $\text{val}_h(U_i) = \text{val}_{h:i}(S)$ .*

*If  $\prec_h$  satisfies these requirements, we say that  $\prec_h$  is a linearization of  $h$ .*

## A.3 Modeling Snapshot Algorithms

We model algorithms using transition systems, based on [12]. A transition system is a tuple:  $(\mathcal{S}, \text{Act}, \longrightarrow, \mathcal{I})$  where  $\mathcal{S}$  is a set of states,  $\text{Act}$  is a set of actions,  $\longrightarrow \subseteq \mathcal{S} \times \text{Act} \times \mathcal{S}$  is the transition relation and  $\mathcal{I} \subseteq \mathcal{S}$  is a set of initial states. A finite execution of a transition system is an alternating sequence of states and actions:  $S_0, \alpha_1, S_1, \alpha_2, S_2, \dots, \alpha_m, S_m$  where  $S_0 \in \mathcal{I}$ ,  $S_m \in \mathcal{S}$ , and for each  $0 \leq i < m$ ,  $(S_i, \alpha_{i+1}, S_{i+1}) \in \longrightarrow$ .



► **Definition 23.** A snapshot algorithm for  $n$  processes is a transition system  $\mathcal{S}_{\text{snap}} = (\mathcal{S}, \text{Act}, \longrightarrow, \mathcal{I})$ , such that  $\Sigma_n \subseteq \text{Act}$ , and for every finite execution,  $S_0, \alpha_1, S_1, \alpha_2, S_2, \dots, \alpha_m, S_m$ , the subsequence of the execution that includes all actions from  $\Sigma_n$  is a history.

At this stage, we point out that, non-traditionally perhaps, we consider only finite executions. In [29], Guerraoui et al. proved that linearizability of deterministic objects (as the snapshot object is) is a safety property [38]. This means that every non-linearizable infinite history admits non-linearizable finite prefix.<sup>2</sup> Therefore, for our purposes, it is sufficient to consider only finite executions and finite histories.

Our main goal is to analyze the linearizability of snapshot algorithms, defined as follows:

► **Definition 24** (Linearizability). A snapshot algorithm is linearizable if all its histories are linearizable.

## B Data Independence

The data independence property, proposed by Wolper [56], roughly means that the behavior of an algorithm does not depend on the data values passed as arguments to the procedure executions. We adapt the simple formulation of the data independence property presented in [1] (which is equivalent to the original formulation of [56]). Wolper required that changing the data values passed to and returned by the methods in a valid history, results in another valid history, and vice-versa. Abdulla et al. [1] noted that it suffices to apply this requirement over differentiated histories.

► **Definition 25.** A history is differentiated if no two update operations in it are invoked with the same data value.

The meticulous reader may note that, for enabling the generation of differentiated snapshot histories, we shall assume that the processes may choose different initial values of their segments. This is a minor technical matter. Therefore, to maintain standard notations, we merely mention this required modification, and relate to  $v_0$  as a single initial value of the segments throughout the paper.

A renaming is a function,  $f: \text{Vals} \rightarrow \text{Vals}$ . Given a history  $h$  and a renaming  $f$ ,  $f(h)$  is the history obtained by replacing every data value  $v$  with  $f(v)$ . More precisely, every  $\text{inv.update}_i(v)$  is replaced with  $\text{inv.update}_i(f(v))$ , and every  $\text{res.scan}_i(u_0, \dots, u_{n-1})$  is replaced with  $\text{res.scan}_i(f(u_0), \dots, f(u_{n-1}))$ . Let  $h = \alpha_0 \dots \alpha_m$  be a history, let  $f$  be a renaming, and write  $f(h) = \beta_0 \dots \beta_m$ . If  $O = (\alpha_k, \alpha_l)$  is an  $\text{update}(v)$  (respectively,  $\text{scan}(u_0, \dots, u_{n-1})$ ) operation in  $h$ , then  $(\beta_k, \beta_l)$  is an  $\text{update}(f(v))$  (respectively,  $\text{scan}(f(u_0), \dots, f(u_{n-1}))$ ) operation in  $f(h)$ . We write  $h(O) = O' = (\beta_k, \beta_l)$  in this case, and the same applies to pending operations. Note that  $f$  forms a bijection between the operations in  $h$  and in  $f(h)$ .

Now, we can formulate the data independence property.

► **Definition 26** (Data Independence). Let  $\mathcal{H}$  be a set of histories.  $\mathcal{H}$  is data independent if for every  $h \in \mathcal{H}$  the following hold:

1. For every renaming  $f$ ,  $f(h) \in \mathcal{H}$ .
2. There is a differentiated history,  $\hat{h} \in \mathcal{H}$ , and a renaming,  $f$ , such that  $h = f(\hat{h})$ .

A snapshot algorithm is data independent if the set of all its histories is data independent.

<sup>2</sup> An infinite history is a word  $h \in (\Sigma_n)^\omega$  that every finite prefix of it is a history.

Given a snapshot algorithm  $\mathcal{Snap}$ , we follow Abdulla et al. [1] practices to prove that  $\mathcal{Snap}$  is linearizable. That is, we prove linearizability by showing that every differentiated history of  $\mathcal{Snap}$  is linearizable. The sufficiency of this approach stems from the next theorem from [1].

► **Theorem 27** (Abdulla et al. [1]). *Let  $\mathcal{H}$  and  $\mathcal{H}'$  be two data independent sets of histories. Then,  $\mathcal{H} \subseteq \mathcal{H}'$  iff every differentiated history in  $\mathcal{H}$  belongs to  $\mathcal{H}'$ .*

To invoke Theorem 27 for proving linearizability, we need to show that the set of all linearizable histories is data independent.

► **Lemma 28.** *The set of all linearizable histories, which we denote by  $\mathcal{H}_{lin}$ , is data independent.*

**Proof.** We start with the first item of Definition 26. Take  $h \in \mathcal{H}_{lin}$  and a renaming  $f$ . Let  $\prec_h$  be a linearization of  $h$ , which is defined over  $\mathcal{E}'$ , a completion of a set  $COP(h) \subseteq \mathcal{E} \subseteq OP(h)$ . To show that  $f(h)$  is linearizable, we need to define a total order  $\prec_{f(h)}$  over a completion of a set of operations in  $f(h)$ , that includes all complete operations. We take  $f(\mathcal{E}) = \{f(A) : A \in \mathcal{E}\}$ . Clearly,  $COP(f(h)) \subseteq f(\mathcal{E}) \subseteq OP(f(h))$ . Now, we define a completion of  $f(\mathcal{E})$ ,  $f(\mathcal{E})'$ . A pending  $p_i$ -update operation in  $f(\mathcal{E})$  is trivially completed by adding the response:  $res.update_i$ . If  $f(S) \in f(\mathcal{E})$  is a pending  $scan_i$  operation, then  $S$  is a pending  $scan_i$  operation in  $\mathcal{E}$ . Assume that  $S$  is completed in  $\mathcal{E}'$  by adding the response:  $res.scan_i(u_0, \dots, u_{n-1})$ . Then, we add to  $f(S)$  the response:  $res.scan_i(f(u_0), \dots, f(u_{n-1}))$ . The linear ordering  $\prec_{f(h)}$  is naturally defined by  $f(A) \prec_{f(h)} f(B)$  if  $A \prec_h B$ .

We show now that  $\prec_{f(h)}$  is indeed a linearization of  $f(h)$ . First, if  $f(A) \prec_{f(h)} f(B)$ , then  $A \prec_h B$ . Since  $\prec_h$  is a linearization of  $h$ ,  $A \prec_h B$  and hence,  $f(A) \prec_{f(h)} f(B)$ . Consequently, item 2 of Definition 22 holds, as required.

Now, to prove that the first item holds as well, let  $f(S)$  be a  $scan$  operation in  $f(\mathcal{E})'$ , and take  $i < n$ . Assume that  $U_i$  is the maximal  $update_i$  operation that precedes  $S$  in  $\prec_h$ . Hence,  $val_h(U_i) = val_{h,i}(S)$ . Since  $f$  is a renaming,  $val_{f(h)}(f(U_i)) = val_{f(h),i}(f(S))$ . Furthermore, by the definition of  $\prec_{f(h)}$ ,  $f(U_i)$  is the maximal  $update_i$  operation that precedes  $f(S)$  in  $\prec_{f(h)}$ . Consequently, item 1 of Definition 22 holds, and thus  $\prec_{f(h)}$  is a linearization of  $f(h)$ .

Now, we turn to prove that the second requirement of Definition 22 holds. Let  $h$  be a linearizable history, and let  $\prec_h$  be a linearization of  $h$ , defined over  $\mathcal{E}'$ , a completion of  $COP(h) \subseteq \mathcal{E} \subseteq OP(h)$ . We shall construct a linearizable differentiated history  $\hat{h}$ , and a renaming  $f$ , such that  $f(\hat{h}) = h$ .

For each  $update$  operation in  $h$ ,  $U$ , choose a unique value  $v_U \in Vals$ . If  $U$  is invoked with value  $v$ , define  $f(v_U) = v$ . Now, we construct the history  $\hat{h}$  by changing some of the letters of  $h$ . First, we replace each  $update$  invocation  $inv.update_i(v)$ , of an operation  $U$ , with  $inv.update_i(v_U)$ . Now, we change also the  $scan$  responses. Assume that the  $m$ -th letter of  $h$  is  $res.scan_i(u_0, \dots, u_{n-1})$ , which is the response of a  $scan$  operation,  $S$ . For each  $j < n$ , Let  $U_j$  be the  $update_j(u_j)$  operation that precedes  $S$  in  $\prec_h$ . Then, replace  $res.scan_i(u_0, \dots, u_{n-1})$  with  $res.scan(v_{U_0}, \dots, v_{U_{n-1}})$ .

Clearly,  $\hat{h}$  is a differentiated history and  $f(\hat{h}) = h$ . It is left to show that  $\hat{h}$  is linearizable. Take  $\hat{\mathcal{E}} = \{A : A \text{ is an operation in } \hat{h} \text{ such that } f(A) \in \mathcal{E}\}$ . Let  $\hat{\mathcal{E}}'$  be the completion of  $\hat{\mathcal{E}}$  in which every pending  $p_i$ -scan operation  $S$  is completed as follows: assume that  $f(S) \in \mathcal{E}$  is completed in  $\mathcal{E}'$  with the response  $res.scan_i(u_0, \dots, u_{n-1})$ . For each  $j < n$ , let  $U_j$  be the maximal  $update_j$  operation such that  $U_j \prec_h f(S)$  (clearly,  $val_h(U_j) = u_j$ ). Then,  $S$  is completed in  $\hat{\mathcal{E}}$  with the response:  $res.scan_i(v_{U_0}, \dots, v_{U_{n-1}})$ . Pending  $update$  operations are completed in a trivial manner. Finally, for  $A, B \in \hat{\mathcal{E}}'$ , define  $A \prec_{\hat{h}} B$  if  $f(A) \prec_{f(h)} f(B)$ . As in the former case, it is clear that  $\prec_{\hat{h}}$  is a linear extension of  $\prec_{\hat{h}}$ . To prove that it is a

linearization of  $\hat{h}$ , consider a scan operation  $S \in \hat{\mathcal{E}}'$ , take  $j < n$  and let  $W_j$  be the maximal  $\text{update}_j$  operation that precedes  $S$  in  $\prec_{\hat{h}}$ . Hence,  $f(W_j) = U_j$ , the maximal  $\text{update}_j$  operation that precedes  $f(S)$  in  $\prec_h$ . By the construction,  $\text{val}_{\hat{h}}(W_i) = v_{U_j} = \text{val}_{h:j}(S)$ , as required. ◀

Now we can show that is sufficient to consider differentiated histories.

► **Lemma 29.** *Let  $\mathcal{L}_{\text{snap}}$  be a data independent snapshot implementation. Then,  $\mathcal{L}_{\text{snap}}$  is linearizable if and only if all its differentiated histories are linearizable.*

**Proof.** The “only if” direction is trivial thus we focus on the “if” direction. Assume that every differentiated history of  $\mathcal{L}_{\text{snap}}$  is linearizable, and let  $\mathcal{H}$  be the set of all histories admitted by  $\mathcal{L}_{\text{snap}}$ . Therefore, by Theorem 27,  $\mathcal{H} \subseteq \mathcal{H}_{\text{lin}}$ , and the required follows. ◀

## B.1 Commonness of the Data-Independent Property

Wolper noted that it is undecidable to determine whether an algorithm is data independent. However, he also noted that some syntactic assumptions imply the data independence property. It is written in [56]:

“The following are sufficient conditions for the program to be data independent:

1. The only input/output operations appearing in the program are reading a value into a variable of type *data* or printing the value of a variable of type *data* that has been assigned a value.
2. Besides input/output operations, variables of type *data* only appear in instructions of the form  $\text{var1} := \text{var2}$  where both *var1* and *var2* are of type *data*.”

As said, since the snapshot object synchronizes accesses to a shared resource (an array of values), it is reasonable to assume that a snapshot algorithm will act in a way that is invariant to the data values read. To demonstrate the naturalness of the data Independence property, we looked at [36] which provides a comparison of fifteen snapshot algorithms.<sup>3</sup> Three of the algorithms in that list were taken from unpublished manuscripts. Among the remaining twelve, seven of the listed algorithms [4, 7, 8, 10, 11, 26] satisfy Wolper’s syntactic condition.<sup>4</sup> The remaining five algorithms [9, 35–37, 48] apply actions which write *null* to variables of type *Vals*, and check whether variables of type *Vals* store *null*. Therefore, those algorithms satisfy a modified version of Wolper’s syntactic condition, in which the processes may delete data type registers, and check whether a data type register stores a value. It is not difficult to see that this modified version still implies data independence. Consequently, as expected, all twelve published algorithms in that list are data independent.

## C Proof of Theorem 5

In this section we prove:

**Theorem 5.** *A data independent snapshot algorithm  $\mathcal{L}_{\text{snap}}$  is linearizable if and only if all its simple executions are linearizable.*

<sup>3</sup> We consider also multi-writer implementations, as those implementations can serve as single-writer snapshot algorithms. Thus, [4] includes two snapshot implementations.

<sup>4</sup> Some implementations use the LL/SC object. We consider the SC(*v*) command as a conditional write to *v*, where the condition addresses variables which are not of type *Vals*.

The “only if” direction of Theorem 5 is trivial. To prove the second direction, we invoke Anderson’s shrinking lemma [7]. This lemma provides a necessary and sufficient condition for the linearizability of snapshot histories. The lemma claims that a history is linearizable if and only if there are  $n$  functions,  $\phi_0, \dots, \phi_{n-1}$ , that satisfy certain properties. Each function  $\phi_i$  maps all complete **scan** operations and all **update** <sub>$i$</sub>  operations into the set of natural numbers  $\mathbb{N}$ . Intuitively, for an **update** <sub>$i$</sub>  operation  $U$  and a **scan** operation  $S$ ,  $\phi_i(U) = \phi_i(S)$  indicates that  $U$  is the maximal **update** <sub>$i$</sub>  operation we should linearize before  $S$ .

► **Lemma 30** (The shrinking lemma). *A history  $h$  of a snapshot algorithm is linearizable if and only if for each  $i < n$  there exists a function  $\phi_i$  such that,*

$$\begin{aligned} \text{Dom}(\phi_i) &= \{U : U \text{ is an update}_i \text{ operation}\} \cup \{S : S \text{ is a complete scan operation}\} \\ \text{Rng}(\phi_i) &= \mathbb{N} \end{aligned}$$

and the following are satisfied:

- Uniqueness.** *If  $U$  and  $U'$  are **update** <sub>$i$</sub>  operations such that  $U <_h U'$ , then  $\phi_i(U) < \phi_i(U')$ .*
- Integrity.** *For each complete **scan** operation  $S$  and  $i < n$ , there exists an **update** <sub>$i$</sub>  operation  $U$ , such that  $\phi_i(S) = \phi_i(U)$  and  $\text{val}_{h,i}(S) = \text{val}_h(U)$ .*
- Proximity(a).** *For each complete **scan** operation  $S$ , and an **update** <sub>$i$</sub>  operation  $U$ , if  $S <_h U$ , then  $\phi_i(S) < \phi_i(U)$ .*
- Proximity(b).** *For each complete **scan** operation  $S$ , and an **update** <sub>$i$</sub>  operation  $U$ , if  $U <_h S$ , then  $\phi_i(U) \leq \phi_i(S)$ .*
- Read precedence.** *For any two complete **scan** operations,  $S_1$  and  $S_2$ , and  $i < n$ , if  $\phi_i(S_1) < \phi_i(S_2)$ , then  $\forall j < n(\phi_j(S_1) \leq \phi_j(S_2))$ .*
- Write precedence.** *For any complete **scan** operation  $S$ , an **update** <sub>$i$</sub>  operation  $U_i$ , and an **update** <sub>$j$</sub>  operation,  $U_j$ , if  $U_i <_h U_j$  and  $\phi_j(U_j) \leq \phi_j(S)$ , then  $\phi_i(U_i) \leq \phi_i(S)$ .*

Before we proceed to the proof of Theorem 5, we add the following assumption:

► **Assumption 2.** *If  $S$  is a complete **scan** operation in a history  $h$  of a data independent snapshot algorithm  $\mathcal{L}_{\text{snap}}$ , then for every  $i < n$  there exists an **update** <sub>$i$</sub>  operation  $U_i$ , such that  $\text{val}_h(U_i) = \text{val}_{h,i}(S)$ .*

This assumption simplifies the presentation of our results, but does not diminish our contribution. If we omit this assumption, Theorem 5 remains correct (yet, its prove needs to be rewritten to include additional technical details). Indeed, if an history  $h$  includes a **scan** operation that returns a value that never been invoked, by item 1 of Definition 26, we can construct a history in which  $v_1$  is this problematic value, and further all **update** operations wrote:  $v_0$ . Hence, we obtain a non-linearizable simple history.

Now we can prove the non-trivial direction of Theorem 5.

**Proof of Theorem 5.** If  $\mathcal{L}_{\text{snap}}$  is linearizable, then all its simple histories are linearizable. To prove the other direction, we assume that  $\mathcal{L}_{\text{snap}}$  is not linearizable and we shall prove that there exists a non-linearizable simple history of  $\mathcal{L}_{\text{snap}}$ .

We fix a non-linearizable differentiate history,  $h$ . Since  $\mathcal{L}_{\text{snap}}$  is data independent, by Lemma 29, such a history exists. We define functions,  $\phi_0, \dots, \phi_{n-1}$ , as in Lemma 30. For the  $l$ -th **update** <sub>$i$</sub>  operation  $U$ , we set  $\phi_i(U) = l$ . Now, for a complete **scan** operation  $S$ , and  $i < n$ , let  $U$  be the unique **update** <sub>$i$</sub>  operation satisfying  $\text{val}_h(U) = \text{val}_{h,i}(S)$ . By Assumption 2, such an **update** operation exists. We define  $\phi_i(S) = \phi_i(U)$ .

Since  $h$  is not linearizable, one of the properties of Lemma 30 fails to hold. We construct a renaming  $f$  such that the history  $f(h)$  is simple and non-linearizable, according to the

property that does not hold. Note that by the way we defined  $\phi_0, \dots, \phi_{n-1}$ , the “uniqueness” and “integrity” requirements hold.

**Proximity(a).** Assume that proximity(a) does not hold. Namely, for a complete scan operation  $S$ , and an  $\text{update}_i$  operation  $U$ ,  $S <_h U$  but  $\phi_i(U) \leq \phi_i(S)$ . Let  $U_i$  be the unique  $\text{update}_i$  operation satisfying  $\text{val}_{h:i}(S) = \text{val}_h(U_i)$ . By integrity,  $\phi_i(S) = \phi_i(U_i)$  and hence, by uniqueness,  $U \leq_h U_i$ . Thus,  $S <_h U_i$  and  $\phi_i(S) = \phi_i(U_i)$ . Assume that  $U_i$  is the  $l$ -th  $\text{update}_i$  operation, and define a renaming  $f: \text{Vals} \rightarrow \text{Vals}$  as follows: Let  $A$  be an  $\text{update}$  operation with  $\text{val}_h(A) = v$ ,

$$f(v) = \begin{cases} v_1, & A \text{ is the } r\text{-th } \text{update}_i \text{ operation where } r \geq l \\ v_0, & \text{otherwise} \end{cases}$$

Therefore,  $f(h)$  is  $(i, j)$ -simple for any  $j \neq i$  with  $r_i = l$  and  $r_j$  sufficiently large (larger than the number of  $\text{update}_j$  operations). Observe that the following hold:

1.  $f(S) <_{f(h)} f(U_i)$  and  $\text{val}_{f(h):i}(f(S)) = \text{val}_{f(h)}(f(U_i)) = v_1$ .
2. Let  $A$  be an  $\text{update}_i$  operation in  $f(h)$ . If  $A <_{f(h)} f(U_i)$ , then  $\text{val}_{f(h)}(A) = v_0$ .

Therefore, we cannot linearize an  $\text{update}_i(v_1)$  operation before  $f(S)$  and hence,  $f(h)$  is not linearizable.

**Proximity(b).** Assume that proximity(b) does not hold. Namely, for a complete scan operation  $S$ , and an  $\text{update}_i$  operation  $U$ ,  $U <_h S$  but  $\phi_i(S) < \phi_i(U)$ . Assume that  $U$  is the  $l$ -th  $\text{update}_i$  operation, and define a renaming  $f$  as follows: Let  $A$  be an  $\text{update}$  operation with  $\text{val}_h(A) = v$ ,

$$f(v) = \begin{cases} v_1, & A \text{ is the } r\text{-th } \text{update}_i \text{ operation where } r \geq l \\ v_0, & \text{otherwise} \end{cases}$$

As before,  $f(h)$  is  $(i, j)$ -simple for any  $j \neq i$  with  $r_i = l$  and  $r_j$  sufficiently large. The following hold:

1.  $f(U) <_{f(h)} f(S)$ .
2. Let  $A$  be an  $\text{update}_i$  operation in  $f(h)$ . If  $A <_{f(h)} f(U)$ , then  $\text{val}_{f(h)}(A) = v_0$ , and otherwise,  $\text{val}_{f(h)}(A) = v_1$ .

Therefore, we can only linearize an  $\text{update}_i(v_1)$  operation before  $f(S)$ . To prove that  $f(h)$  is not linearizable, we show that  $\text{val}_{f(h):i}(f(S)) = v_0$ .

Let  $U_i$  be the unique  $\text{update}_i$  operation satisfying  $\phi_i(S) = \phi_i(U_i)$ . Recall that, by integrity,  $\text{val}_h(U_i) = \text{val}_{h:i}(S)$ , and conclude that  $\text{val}_{f(h)}(f(U_i)) = \text{val}_{f(h):i}(f(S))$ . Since  $\phi_i(S) = \phi_i(U_i)$ ,  $\phi_i(U_i) < \phi_i(U)$ . By uniqueness,  $U_i <_h U$  and hence,  $f(U_i) <_{f(h)} f(U)$ . Therefore,  $v_0 = \text{val}_{f(h)}(f(U_i)) = \text{val}_{f(h):i}(f(S))$ , as required.

**Read Precedence.** Assume that read precedence fails to hold. Namely, there are two complete scan operations,  $S_1$  and  $S_2$ , such that  $\phi_i(S_1) < \phi_i(S_2)$  and  $\phi_j(S_2) < \phi_j(S_1)$ . Let  $U_i$  be the  $\text{update}_i$  operation satisfying  $\phi_i(S_2) = \phi_i(U_i)$ . Hence,  $U_i$  is the unique  $\text{update}_i$  operation satisfying  $\text{val}_{h:i}(S_2) = \text{val}_h(U_i)$ . In the same way, let  $U_j$  be the unique  $\text{update}_j$  operation satisfying  $\phi_j(S_1) = \phi_j(U_j)$  and  $\text{val}_{h:j}(S_1) = \text{val}_h(U_j)$ . Assume that  $U_i$  is the  $l_1$ -th  $\text{update}_i$  operation in  $h$ , and assume that  $U_j$  is the  $l_2$ -th  $\text{update}_j$  operation in  $h$ . Define  $f: \text{Vals} \rightarrow \text{Vals}$  as follows: Let  $A$  be an  $\text{update}$  operation with  $\text{val}_h(A) = v$ .

$$f(v) = \begin{cases} v_1, & A \text{ is the } r\text{-th } \text{update}_i \text{ operation where } r \geq l_1 \\ v_1, & A \text{ is the } r\text{-th } \text{update}_j \text{ operation where } r \geq l_2 \\ v_0, & \text{otherwise} \end{cases}$$

Hence,  $f(h)$  is an  $(i, j)$ -simple history with  $r_i = l_1$  and  $r_j = l_2$ . Observe that the following hold.

1. Let  $U$  be an **update** <sub>$i$</sub>  operation in  $f(h)$ . If  $U <_{f(h)} f(U_i)$ , then  $\text{val}_{f(h)}(U) = v_0$ , and otherwise,  $\text{val}_{f(h)}(U) = v_1$ .
2. Let  $U$  be an **update** <sub>$j$</sub>  operation in  $f(h)$ . If  $U <_{f(h)} f(U_j)$ , then  $\text{val}_{f(h)}(U) = v_0$ , and otherwise,  $\text{val}_{f(h)}(U) = v_1$ .
3.  $\text{val}_{f(h):j}(f(S_1)) = \text{val}_{f(h)}(f(U_j)) = v_1$ .
4.  $\text{val}_{f(h):i}(f(S_2)) = \text{val}_{f(h)}(f(U_i)) = v_1$ .

It is left to show that  $f(h)$  is not linearizable. Towards a contradiction, assume that  $\prec$  is a linearization of  $f(h)$ . Since  $S_1$  and  $S_2$  are complete in  $h$ ,  $f(S_1)$  and  $f(S_2)$  are complete in  $f(h)$  and hence, belong to the base set of  $\prec$ . Assume, without loss of generality, that  $f(S_1) \prec f(S_2)$ . Let  $U$  be the maximal **update** <sub>$j$</sub>  operation linearized before  $f(S_1)$ . Hence,  $\text{val}_{f(h)}(U) = v_1$ . Since  $\prec$  extends  $<_{f(h)}$ , by item 2 we have,

$$f(U_j) \preceq U \prec f(S_1) \prec f(S_2).$$

Now, let  $U'$  be the maximal **update** <sub>$j$</sub>  operation linearized before  $f(S_2)$ . Hence,  $f(U_j) \preceq U \preceq U'$ , which implies that  $U_j \leq_{f(h)} U'$  and hence,  $\text{val}_{f(h)}(U') = v_1$ . To achieve a contradiction, we shall prove now that  $\text{val}_{f(h):j}(f(S_2)) = v_0$ , which implies that  $\prec$  is not a linearization of  $f(h)$ .

Let  $A$  be the unique **update** <sub>$j$</sub>  operation in  $h$  such that  $\phi_j(S_2) = \phi_j(A)$  and  $\text{val}_h(S_2) = \text{val}_h(A)$ . Therefore,  $\phi_j(A) < \phi_j(S_1) = \phi_j(U_j)$  and by uniqueness,  $A <_h U_j$ . Consequently,  $f(A) <_{f(h)} f(U_j)$  and hence,  $\text{val}_{f(h)}(f(A)) = v_0$ . Therefore,  $f(\text{val}_h(A)) = v_0$  and hence,  $\text{val}_{f(h):j}(f(S_1)) = v_0$ , which provides the desired contradiction.

**Write Precedence.** Assume that write precedence fails to hold. Namely, there exists a complete **scan** operation,  $S$ , and two **update** operations,  $U_i$  and  $U_j$ , by  $p_i$  and  $p_j$  respectively, such that  $U_i <_h U_j$  and  $\phi_j(U_j) \leq \phi_j(S)$ , but  $\phi_i(S) < \phi_i(U_i)$ . Assume that  $U_i$  is the  $l_1$ -th **update** <sub>$i$</sub>  operation and  $U_j$  is the  $l_2$ -th **update** <sub>$j$</sub>  operation. Define  $f: \text{Vals} \rightarrow \text{Vals}$  as follows: Let  $A$  be an **update** operation with  $\text{val}_h(A) = v$ .

$$f(v) = \begin{cases} v_1, & A \text{ is the } r\text{-th } \text{update}_i \text{ operation where } r \geq l_1 \\ v_1, & A \text{ is the } r\text{-th } \text{update}_j \text{ operation where } r \geq l_2 \\ v_0, & \text{otherwise} \end{cases}$$

Hence,  $f(h)$  is an  $(i, j)$ -simple history with  $r_i = l_1$  and  $r_j = l_2$ . Observe that the following hold.

1. Let  $U$  be an **update** <sub>$i$</sub>  operation in  $f(h)$ . If  $U <_{f(h)} f(U_i)$ , then  $\text{val}_{f(h)}(U) = v_0$ , and otherwise,  $\text{val}_{f(h)}(U) = v_1$ .
2. Let  $U$  be an **update** <sub>$j$</sub>  operation in  $f(h)$ . If  $U <_{f(h)} f(U_j)$ , then  $\text{val}_{f(h)}(U) = v_0$ , and otherwise,  $\text{val}_{f(h)}(U) = v_1$ .
3.  $f(U_i) <_{f(h)} f(U_j)$ .
4. Let  $U$  be the **update** <sub>$j$</sub>  operation in  $h$ , satisfying  $\phi_i(U) = \phi_i(S)$ . By item 2,  $\text{val}_{f(h):j}(f(S)) = \text{val}_{f(h)}(f(U)) = v_1$ .

It is left to show that  $f(h)$  is not linearizable. Towards a contradiction, assume that  $\prec$  is a linearization of  $f(h)$ . Since  $S$  is complete in  $h$ ,  $f(S)$  is complete in  $f(h)$  and hence, belongs to the base set of  $\prec$ . Let  $A_j$  be the **update** <sub>$j$</sub>  operation in  $f(h)$ , linearized before  $f(S)$ . Therefore,  $\text{val}_{f(h)}(A_j) = v_1$  and hence,  $f(U_j) \leq_{f(h)} A_j$ . Since  $\prec$  extends  $<_{f(h)}$ , we have,

$$f(U_i) \prec f(U_j) \preceq A_j \prec f(S).$$



Let  $A_i$  be the  $\text{update}_i$  operation linearized before  $f(S)$ . Thus,  $f(U_i) \preceq A_i$  and hence,  $\text{val}_{f(h)}(A_i) = v_1$ . To achieve a contradiction, we shall prove now that  $\text{val}_{f(h):i}(f(S)) = v_0$ , which implies that  $\prec$  is not a linearization of  $f(h)$ .

Let  $W$  be the unique  $\text{update}_i$  operation in  $h$ , such that  $\phi_i(S) = \phi_i(W)$  and  $\text{val}_{h:i}(S) = \text{val}_h(W)$ . Therefore, by uniqueness,  $W <_h U_i$ . As a result,  $f(W) <_{f(h)} f(U_i)$  and hence,  $\text{val}_{f(h)}(f(W)) = v_0$ . Since  $\text{val}_{f(h)}(f(W)) = \text{val}_{f(h):i}(f(S))$ , we get that  $\text{val}_{f(h):i}(f(S)) = v_0$  as required. ◀

## D Proof of Theorem 10

In this section we prove:

**Theorem 10.** *An  $(i, j)$ -simple history  $h$  is linearizable if and only if the following properties hold.*

**No Inversion.** *There are no complete scan operations  $S_1$  and  $S_2$  in  $h$  such that  $(\text{val}_{h:i}(S_1), \text{val}_{h:j}(S_1)) = (0, 1)$  and  $(\text{val}_{h:i}(S_2), \text{val}_{h:j}(S_2)) = (1, 0)$ .*

**Non-Decreasing.** *If  $S_1$  and  $S_2$  are two complete scan operations in  $h$  such that  $S_1 <_h S_2$ , then  $\text{val}_{h:i}(S_1) \leq \text{val}_{h:i}(S_2)$  and  $\text{val}_{h:j}(S_1) \leq \text{val}_{h:j}(S_2)$ .*

**Appropriateness.** *For each complete scan operation  $S$  in  $h$ , there exists an  $S$ -appropriate pair of update operations.*

First, we prove the simpler direction of Theorem 10. That is, we show that if  $h$  is a linearizable  $(i, j)$ -simple history, then the properties are satisfied.

**Proof.** Let  $h$  be a linearizable  $(i, j)$ -simple history. Assume that  $\prec_h$  is a linearization of  $h$ . Hence,  $\prec_h$  is defined over a set of operations  $\mathcal{E}$  that includes all complete operations and a completion of some of the pending operations. We need to verify that all three properties are satisfied.

**No Inversion.** Assume towards a contradiction that

$$(\text{val}_{h:i}(S_1), \text{val}_{h:j}(S_1)) = (0, 1) \text{ and } (\text{val}_{h:i}(S_2), \text{val}_{h:j}(S_2)) = (1, 0),$$

for two complete scan operations,  $S_1$  and  $S_2$ . As  $\prec_h$  is a linear ordering,  $S_1 \prec_h S_2$  or  $S_2 \prec_h S_1$ . Assume, without loss of generality, that  $S_1 \prec_h S_2$ . Let  $U_1$  be the maximal  $\text{update}_j$  operation that precedes  $S_1$  in  $\prec_h$ , and let  $U_2$  be the maximal  $\text{update}_j$  operation that precedes  $S_2$  in  $\prec_h$ .

Hence,  $\text{val}(U_1) = 1$  and  $\text{val}(U_2) = 0$  and thus  $U_1 \neq U_2$ . In addition, since  $S_1 \prec_h S_2$ ,  $U_1 \prec_h U_2$ .  $U_1$  and  $U_2$  are both  $p_j$ -operations and hence, comparable in  $<_h$ . As  $\prec_h$  extends  $<_h$ , we have  $U_1 <_h U_2$ . We get that  $p_j$  invoked an  $\text{update}_j(1)$  operation (namely,  $U_1$ ) and afterwards it invoked an  $\text{update}_j(0)$  operation ( $U_2$ ). This contradicts the assumption that  $h$  is an  $(i, j)$ -simple history.

**Non-Decreasing.** Assume towards a contradiction that Non-Decreasing does not hold and hence, without loss of generality,

$$S_1 <_h S_2 \text{ and } \text{val}_{h:i}(S_2) < \text{val}_{h:i}(S_1),$$

for two complete scan operations,  $S_1$  and  $S_2$ . As  $\text{val}_{h:i}(S_2) < \text{val}_{h:i}(S_1)$ , since  $h$  is an  $(i, j)$ -simple history, we conclude that  $\text{val}_{h:i}(S_2) = 0$  and  $\text{val}_{h:i}(S_1) = 1$ . Let  $U_1$  be the



maximal  $\text{update}_i$  operation that precedes  $S_1$  in  $\prec_h$ , and let  $U_2$  be the maximal  $\text{update}_i$  operation that precedes  $S_2$  in  $h$ . Hence,  $\text{val}_h(U_1) = 1$  and  $\text{val}_h(U_2) = 0$ .

Since  $\prec_h$  extends  $<_h$ ,  $S_1 \prec_h S_2$ . Therefore,  $U_1 \prec_h U_2$ . Since  $U_1$  and  $U_2$  are both  $p_i$ -operations, they are comparable in  $<_h$ , and since  $\prec_h$  extends  $<_h$ , we have  $U_1 <_h U_2$ . We get that  $p_i$  invoked an  $\text{update}_i(1)$  operation (i.e.  $U_1$ ), and afterwards an  $\text{update}_i(0)$  operation (i.e.  $U_2$ ), in contradiction to the fact that  $h$  is an  $(i, j)$ -simple history.

**Appropriateness.** Let  $S$  be a complete scan operation in  $h$ , and let  $U_i$  and  $U_j$  be the maximal  $\text{update}_i$  operation and  $\text{update}_j$  operation, respectively, that precede  $S$  in  $\prec_h$ . Clearly, the pair  $(U_i, U_j)$  is  $S$ -appropriate. ◀

It is left to prove the second direction of Theorem 10. The proof we provide is involved with some technical details, but the idea behind it is simple. We want to show that an  $(i, j)$ -simple history that satisfies our properties is linearizable. We add some constraints that any linearization must satisfy: for a complete scan operation,  $S$ , we consider the values:  $\text{val}_{h:i}(S)$ ,  $\text{val}_{h:j}(S)$ . For  $k \in \{i, j\}$ , if  $\text{val}_k(S) = 1$ , we require that  $S$  will be linearized after the first  $\text{update}_k(1)$  operation; if  $\text{val}_{h:k}(S) = 0$  then, similarly, we require that  $S$  will be linearized before the first  $\text{update}_k(1)$  operation. Then, we consider the precedence relation  $<_h$  strengthened by our constraints, and we show that the resulting binary relation is an acyclic relation and hence, can be extended into a linear ordering. Finally, we show that if  $\prec_h$  is a linear ordering that extends  $<_h$  together with our constraints, then  $\prec_h$  is a linearization of  $h$ .

We turn now to the proof. We fix an  $(i, j)$ -simple history  $h$  that satisfies the properties of Theorem 10, and we shall prove that it is linearizable. We construct a linearization of

$$\mathcal{E} = \{S : S \in h \text{ is a complete scan operation}\} \cup \{U : U \in h \text{ is an update operation}\}.$$

► **Definition 31.** Let  $F_i$  be the first  $\text{update}_i(1)$  operation in  $h$  (if exists), and let  $F_j$  be the first  $\text{update}_j(1)$  operation in  $h$  (if exists). We define a relation  $\triangleleft$  as follows:

Let  $S$  be a complete scan operation,

- If  $\text{val}_{h:i}(S) = 0$ , then  $S \triangleleft F_i$ , and if  $\text{val}_{h:i}(S) = 1$ , then  $F_i \triangleleft S$ .
- If  $\text{val}_{h:j}(S) = 0$ , then  $S \triangleleft F_j$ , and if  $\text{val}_{h:j}(S) = 1$ , then  $F_j \triangleleft S$ .

A cycle in a binary relation  $R$ , of length  $m > 1$ , is a sequence of elements  $(X_1, \dots, X_m)$  such that  $(X_i, X_{i+1}) \in R$  for each  $i < m$ , and  $X_1 = X_m$ . We aim to prove that  $<_h \cup \triangleleft$  is acyclic. As a first step towards that goal, we show  $\triangleleft$  is acyclic.

► **Lemma 32.** If  $S_1 \triangleleft F_k \triangleleft S_2$  where  $S_1$  and  $S_2$  are complete scan operations and  $k \in \{i, j\}$ , then  $\text{val}_{h:k}(S_1) < \text{val}_{h:k}(S_2)$ .

**Proof.** Since  $S_1 \triangleleft F_k$ ,  $\text{val}_{h:k}(S_1) = 0$  and since  $F_k \triangleleft S_2$ ,  $\text{val}_{h:k}(S_2) = 1$ . ◀

► **Lemma 33.** If  $S_1 \triangleleft F_k \triangleleft S_2$  where  $S_1$  and  $S_2$  are complete scan operations, then  $\text{val}_{h:i}(S_1) \leq \text{val}_{h:i}(S_2)$  and  $\text{val}_{h:j}(S_1) \leq \text{val}_{h:j}(S_2)$ .

**Proof.** Assume, without loss of generality, that  $k = i$ . By the previous lemma,  $\text{val}_{h:i}(S_1) < \text{val}_{h:i}(S_2)$ , and it is left to prove that  $\text{val}_{h:j}(S_1) \leq \text{val}_{h:j}(S_2)$ .

Assume for a contradiction that  $\text{val}_{h:j}(S_2) < \text{val}_{h:j}(S_1)$ . Since  $h$  is  $(i, j)$ -simple, we have  $\text{val}_{h:j}(S_1) = 1$  and  $\text{val}_{h:j}(S_2) = 0$ . However, by the same argument (as  $\text{val}_{h:i}(S_1) < \text{val}_{h:i}(S_2)$ ),  $\text{val}_{h:i}(S_1) = 0$  and  $\text{val}_{h:i}(S_2) = 1$ , in contradiction to No inversion. ◀

► **Lemma 34.** *There are no cycles in  $\triangleleft$ .*

**Proof.** Assume for a contradiction that for  $l > 1$ ,  $(X_1, \dots, X_l)$  is a cycle. That is,  $X_1 \triangleleft \dots \triangleleft X_l = X_1$ .  $\triangleleft$  is clearly irreflexive, thus  $l > 2$ . By shifting the cycle, if necessary, we may assume, without loss of generality, that  $X_1$  is a **scan** operation and the sequence is of the form

$$S_1 \triangleleft U_2 \triangleleft S_3 \cdots \triangleleft S_l = S_1$$

where each  $S_r$  is a **scan** operation, and each  $U_r$  is  $F_i$  or  $F_j$ . Several invocations of the previous two lemmas indicate that  $\text{val}_{h:i}(S_1) < \text{val}_{h:i}(S_l)$  or  $\text{val}_{h:j}(S_1) < \text{val}_{h:j}(S_l)$ . Hence,  $S_1 \neq S_l$ , in contradiction to the assumption that  $(X_1, \dots, X_l)$  is a cycle. ◀

So far, we have proved that there are no cycles in  $\triangleleft$ , and now we turn to prove the same for  $<_h \cup \triangleleft$ .

► **Lemma 35.** *There is no sequence in  $\triangleleft$  of length 5,  $X_1 \triangleleft X_2 \triangleleft \dots \triangleleft X_5$ , where  $X_1$  is an update operation.*

**Proof.** Assume for a contradiction that such a sequence exists, and consider a chain:

$$U_1 \triangleleft S_1 \triangleleft U_2 \triangleleft S_2 \triangleleft U_3$$

where  $U_1, U_2, U_3$  are either  $F_i$  or  $F_j$ , and  $S_1, S_2$  are **scan** operations.

Assume, without loss of generality, that  $U_1 = F_i$ , and conclude that  $\text{val}_{h:i}(S_1) = 1$ . Now, since  $S_1 \triangleleft U_2$  and  $\text{val}_{h:i}(S_1) = 1$ , necessarily  $\text{val}_{h:j}(S_1) = 0$  and  $U_2 = F_j$ . We see that  $(\text{val}_{h:i}(S_1), \text{val}_{h:j}(S_1)) = (1, 0)$ . By Lemma 33, we get that  $(\text{val}_{h:i}(S_2), \text{val}_{h:j}(S_2)) = (1, 1)$ . Therefore,  $S_2 \triangleleft U_3$  is impossible. ◀

► **Corollary 36.** *There is no sequence in  $\triangleleft$  of length 6.*

► **Lemma 37.** *If  $X_1 \triangleleft X_2$ , then  $\neg(X_2 <_h X_1)$ .*

**Proof.** Take a sequence  $X_1 \triangleleft X_2$ . Without loss of generality, the sequence is of the form  $S \triangleleft F_i$  or  $F_i \triangleleft S$  where  $S$  is a **scan** operation. First we consider the case where the sequence is of the form  $S \triangleleft F_i$ . Thus,  $\text{val}_{h:i}(S) = 0$ . Assume for a contradiction that  $F_i <_h S$ . By Appropriateness, there exists an  $S$ -appropriate pair  $(U_i, U_j)$ . Therefore,  $F_i <_h U_i$  and  $\text{val}_h(U_i) = \text{val}_{h:i}(S) = 0$ , in contradiction to the fact that  $h$  is an  $(i, j)$ -simple history.

Now, assume that the sequence is of the form  $F_i \triangleleft S$  and thus  $\text{val}_{h:i}(S) = 1$ . Assume, towards a contradiction that  $S <_h F_i$ . As in the former case, consider an  $S$ -appropriate pair  $(U_i, U_j)$ . Hence,  $U_i <_h F_i$  and  $\text{val}_h(U_i) = \text{val}_{h:i}(S) = 1$ , in contradiction to the fact that  $F_i$  is the first  $\text{update}_i(1)$  operation. ◀

► **Lemma 38.** *If  $X_1 \triangleleft X_2 \triangleleft X_3$ , then  $\neg(X_3 <_h X_1)$ .*

**Proof.** Note that  $X_1$  is either a **scan** operation, or  $X_1 \in \{F_i, F_j\}$ . If  $X_1$  is a **scan** operation, then  $X_3$  is also a **scan** operation and then, by Lemma 32 and Non-Decreasing, we conclude that  $\neg(X_3 <_h X_1)$ .

It is left to deal with the case that  $X_1 \in \{F_i, F_j\}$ . Assume, without loss of generality, that  $X_1 = F_i$  and thus the sequence is of the form:

$$F_i \triangleleft S \triangleleft F_j,$$

where  $S$  is a complete **scan** operation. Hence,  $(\text{val}_{h:i}(S), \text{val}_{h:j}(S)) = (1, 0)$ .

## XX:32 Polynomial-Time Verification and Testing of the Snapshot Data Structure

Now, assume towards a contradiction that  $F_j <_h F_i$ , and take an  $S$ -appropriate pair  $(U_i, U_j)$ . Since  $val_{h:j}(S) = 0$ ,  $val_h(U_j) = 0$ . As  $F_j$  is the first  $update_j(1)$  operation,

$$U_j <_h F_j.$$

Similarly,  $1 = val_{h:i}(S) = val_h(U_i)$ . As  $F_i$  is the first  $update_i(1)$  operation,

$$F_i \leq_h U_i.$$

We summarize the conclusions:

$$U_j <_h F_j <_h F_i \leq_h U_i.$$

Therefore, there exists an  $update_j$  operation (i.e.,  $F_j$ ) between  $U_j$  and  $U_i$ , in contradiction to our assumption that the pair  $(U_i, U_j)$  is  $S$ -appropriate.  $\blacktriangleleft$

► **Lemma 39.** *If  $X_1 \triangleleft X_2 \triangleleft X_3 \triangleleft X_4$ , then  $\neg(X_4 <_h X_1)$ .*

**Proof.** Consider a sequence of the form  $X_1 \triangleleft X_2 \triangleleft X_3 \triangleleft X_4$ . We shall prove that  $\neg(X_4 <_h X_1)$ .  $X_1$  is either a **scan** operation, or  $X_1 \in \{F_i, F_j\}$ . First we deal with the case where  $X_1$  is an **update** operation, and we assume, without loss of generality, that  $X_1 = F_i$ . Hence, our sequence is of the form:

$$F_i \triangleleft S_1 \triangleleft F_j \triangleleft S_2.$$

By definition of  $\triangleleft$  and by Lemmas 32 and 33 we have

- $(val_{h:i}(S_1), val_{h:j}(S_1)) = (1, 0).$
- $(val_{h:i}(S_2), val_{h:j}(S_2)) = (1, 1).$

Assume towards a contradiction that  $S_2 <_h F_i$ , and take an  $S_2$ -appropriate pair,  $(U_i, U_j)$ . Since  $U_i \in I_i(S_2)$ ,  $U_i <_h F_i$ . However,  $val_h(U_i) = val_{h:i}(S_2) = 1$ , in contradiction to the choice of  $F_i$  as the first  $update_i(1)$  operation.

Now, we deal with the second case, in which  $X_1$  is a **scan** operation, and, without loss of generality, our sequence is of the form

$$S_1 \triangleleft F_i \triangleleft S_2 \triangleleft F_j.$$

In this case, by definition of  $\triangleleft$  and by Lemmas 32 and 33 we have

- $(val_{h:i}(S_2), val_{h:j}(S_2)) = (1, 0).$
- $(val_{h:i}(S_1), val_{h:j}(S_1)) = (0, 0).$

Assume towards a contradiction that  $F_j <_h S_1$ , and take an  $S$ -appropriate pair,  $(U_i, U_j)$ . Hence, we get that  $F_j \leq_h U_j$  and  $val_h(U_j) = val_{h:j}(S_1) = 0$ , in contradiction to the fact that  $h$  is  $(i, j)$ -simple.  $\blacktriangleleft$

► **Lemma 40.** *If  $X_1 \triangleleft X_2 \triangleleft \dots \triangleleft X_l$ , then  $\neg(X_l <_h X_1)$ .*

**Proof.** Assume towards a contradiction that the claim is false, and consider a counter example:  $X_1 \triangleleft X_2 \triangleleft \dots \triangleleft X_l$ . By Corollary 36,  $l < 6$ , and by Lemmas 37, 38 and 39,  $l > 4$ . Thus,  $l = 5$ .

Since  $l = 5$ , by Lemma 35 our sequence is, without loss of generality, of the form:

$$S_1 \triangleleft F_i \triangleleft S_2 \triangleleft F_j \triangleleft S_3$$

where  $S_1, S_2, S_3$  are **update** operations. By Lemmas 32 and 33 we conclude that

- $(val_{h:i}(S_1), val_{h:j}(S_1)) = (0, 0).$
- $(val_{h:i}(S_3), val_{h:j}(S_3)) = (1, 1).$

Thus, by Non Decreasing,  $\neg(S_3 <_h S_1)$ , as required.  $\blacktriangleleft$

Now, we can finally prove:

► **Lemma 41.** *There are no cycles in  $<_h \cup \triangleleft$ .*

**Proof.** Assume for a contradiction that there are cycles in relation  $<_h \cup \triangleleft$ , and take such of a minimal length:  $(X_1, X_2, \dots, X_l)$ , where  $l > 1$  and  $X_1 = X_l$ . Since there are no cycles in  $\triangleleft$ , for some  $k < l$ ,  $X_k <_h X_{k+1}$ . Hence, by shifting the cycle if necessary, we may assume, without loss of generality, that  $X_1 <_h X_2$ . Since  $<_h$  is transitive and  $l$  is minimal,  $X_2 \triangleleft X_3$ . Therefore, there is a prefix of the cycle of the form

$$X_1 <_h X_2 \triangleleft X_3 \triangleleft \dots \triangleleft X_m.$$

Take such a prefix where  $m$  is as large as possible.

By Lemma 40,  $\neg(X_m <_h X_2)$ ; thus,  $X_m \neq X_1$ . Hence,  $m < l$  and by the maximality of  $m$ ,  $X_m <_h X_{m+1}$ . Since  $X_1 <_h X_2$ ,  $X_1$  is complete and  $end(X_1) < begin(X_2)$ . Since  $X_m <_h X_{m+1}$ ,  $X_m$  is complete and  $end(X_m) < begin(X_{m+1})$ . By Lemma 40,  $\neg(X_m <_h X_2)$ ; thus,  $begin(X_2) < end(X_m)$ . By combining our results, we have

$$end(X_1) < begin(X_2) < end(X_m) < begin(X_{m+1}).$$

We see that  $X_1 <_h X_{m+1}$  thus  $(X_1, X_{m+1}, \dots, X_l)$  is also a cycle. This, however, contradicts the minimality of  $l$ .  $\blacktriangleleft$

We mention that a binary relation can be extended into a linear ordering if and only if it is acyclic. Indeed, if a relation admits a linear extension, it clearly has no cycles, as a linear order is an acyclic relation. For the other direction, if there are no cycles in a binary relation, then its transitive closure is a partial ordering (irreflexive and transitive), and every partial ordering can be extended into a linear ordering. We can now prove Theorem 10.

**Proof.** Since there are no cycles in  $<_h \cup \triangleleft$ , there exists a linear ordering of  $\mathcal{E}$ ,  $\prec_h$  that extends  $<_h \cup \triangleleft$ . We shall prove that  $\prec_h$  satisfies the requirements (there is no need to speak about a completion of  $\mathcal{E}$ , since all scan operations in  $\mathcal{E}$  are complete, and update operations do not return an argument).

Let  $S \in \mathcal{E}$  be any scan operation. We need to show that if  $k < n$  and  $U_k$  is the maximal  $\text{update}_k$  operation that precedes  $S$  in  $\prec_h$ , then  $val_h(U_k) = val_{h:k}(S)$ . First, we deal with the case that  $k \notin \{i, j\}$ . In this case, since  $h$  is  $(i, j)$ -simple,  $val_h(U_k) = 0$ . Since  $k \notin \{i, j\}$ , all  $\text{update}_k$  operations are invoked with value 0 thus  $val_{h:k}(S) = 0$  as required.

Now, let  $U_i$  be the maximal  $\text{update}_i$  operation that precedes  $S$  in  $\prec_h$  and let  $U_j$  be the maximal  $\text{update}_j$  operation that precedes  $S$  in  $\prec_h$ . We need to prove that  $val_{h:i}(S) = val_h(U_i)$  and  $val_{h:j}(S) = val_h(U_j)$ . Since our argument is symmetric we prove only for  $U_i$ .

First, assume that  $val_i(S) = 0$ . If  $U$  is any  $\text{update}_i(1)$  operation, then  $S \triangleleft F_i \leq_h U$ . Therefore, since  $\prec_h$  extends  $<_h \cup \triangleleft$ , if  $U$  is any  $\text{update}_i(1)$  operation, then  $S \prec_h U$ . Thus,  $U_i \prec_h S$  implies that  $val_h(U_i) = 0$ , as required.

Now, assume that  $val_{h:i}(S) = 1$ . Since  $F_i \triangleleft S$ ,  $F_i \prec_h S$ . Now,  $U_i$  is the maximal  $\text{update}_i$  operation that precedes  $S$  in  $\prec_h$ , and hence,  $F_i \leq_h U_i$ . Both  $F_i$  and  $U_i$  are  $\text{update}_i$  operations; thus,  $U_i <_h F_i$  or  $F_i \leq_h U_i$ . As  $F_i \leq_h U_i$ , and as  $\prec_h$  extends  $<_h$ , we have  $F_i \leq_h U_i$ . Since our history is  $(i, j)$ -simple,  $val_h(U_i) = 1$ , as required.  $\blacktriangleleft$

## E Missing Proofs of 4.1

**Proposition 12.** *There exists an automaton  $M_1$  such that, for any  $(i, j)$ -simple history  $h$ ,  $h$  violates No-Inversion if and only if  $h \in L(M_1)$ . Moreover,  $M_1$  has  $O(1)$  states and  $O(n)$  transitions.*

**Proof.**

$$L_1 = L(\Sigma^*(res.scan_0(0, 1) + \dots + res.scan_{n-1}(0, 1))\Sigma^* \\ (res.scan_0(1, 0) + \dots + res.scan_{n-1}(1, 0))\Sigma^*)$$

$$L_2 = L(\Sigma^*(res.scan_0(1, 0) + \dots + res.scan_{n-1}(1, 0))\Sigma^* \\ (res.scan_0(0, 1) + \dots + res.scan_{n-1}(0, 1))\Sigma^*)$$

Clearly, there exists an automaton  $M_1$  such that  $L(M_1) = L_1 \cup L_2$ , and  $M_1$  satisfies the requirements.  $\blacktriangleleft$

**Proposition 13.** *There exists an automaton  $M_2$  such that, for any  $(i, j)$ -simple history  $h$ ,  $h$  violates Non-Decreasing if and only if  $h \in L(M_2)$ . Moreover,  $M_2$  has  $O(n)$  states and  $O(n^2)$  transitions.*

**Proof.** For  $k < n$ ,

$$L_1(k) = L(\Sigma^*(res.scan_0(1, 0) + res.scan_0(1, 1) + \dots + res.scan_{n-1}(1, 0) + \\ res.scan_{n-1}(1, 1))\Sigma^*(inv.scan_k)\Sigma^*(res.scan_k(0, 0) + res.scan_k(0, 1))\Sigma^*)$$

$$L_2(k) = L(\Sigma^*(res.scan_0(0, 1) + res.scan_0(1, 1) + \dots + res.scan_{n-1}(0, 1) + \\ res.scan_{n-1}(1, 1))\Sigma^*(inv.scan_k)\Sigma^*(res.scan_k(0, 0) + res.scan_k(1, 0))\Sigma^*)$$

Clearly, each of the languages,  $L_1(k)$  and  $L_2(k)$ , is accepted by an automaton with four states and  $O(n)$  transitions. Take an automaton  $M_2(k)$  such that  $L(M_2(k)) = L_1(k) \cup L_2(k)$ , and  $M_2(k)$  has  $O(1)$  states and  $O(n)$  transitions. Take  $M_2$  to be an automaton with  $O(n)$  states and  $O(n^2)$  transitions such that  $L(M_2) = \bigcup_{k=0}^{n-1} L(M_2(k))$ .  $\blacktriangleleft$

**Lemma 14.** *Let  $h$  be an  $(i, j)$ -simple history, and let  $S$  be a complete scan operation in  $h$ . For  $l \in \{i, j\}$ , let  $F_l$  be the first  $update_l(1)$  operation in  $h$ , if exists. Then, there is no  $S$ -appropriate pair in  $h$  if and only if any of the following holds:*

1. For  $l \in \{i, j\}$ ,  $F_l$  exists,  $val_{h:l}(S) = 0$ , and  $F_l <_h S$ .
2. For  $l \in \{i, j\}$ ,  $val_{h:l}(S) = 1$ , and either  $S <_h F_l$  or  $F_l$  doesn't exist.
3.  $(val_{h:i}(S), val_{h:j}(S)) = (0, 1)$  and  $F_i <_h F_j$ .
4.  $(val_{h:i}(S), val_{h:j}(S)) = (1, 0)$  and  $F_j <_h F_i$ .

For proving Lemma 14, we formulate and prove the next claim.

**► Lemma 42.** *Let  $h$  be an  $(i, j)$ -simple history, and let  $S$  be a complete scan operation in  $h$ . Assume that  $U_i \in I_i(S)$  (see Definition 5) is an  $update_i$  operation such that  $val_h(U_i) = val_{h:i}(S)$ , and  $U_j \in I_j(S)$  is an  $update_j$  operation such that  $val_h(U_j) = val_{h:j}(S)$ . If  $val_{h:i}(S) = val_{h:j}(S)$ , then there exists an  $S$ -appropriate pair in  $h$ .*

**Proof.** First, we prove for the case where  $(val_{h:i}(S), val_{h:j}(S)) = (0, 0)$ . Let  $U'_i$  be the first  $update_i$  operation in  $I_i(S)$ . Therefore,  $U'_i <_h S$ . By the minimality of  $U'_i$ ,  $U'_i \leq_h U_i$ , and hence, since  $h$  is  $(i, j)$ -simple,  $val_h(U'_i) = 0$ . Similarly, let  $U'_j$  be the first  $update_j$  operation

in  $I_j(S)$  and conclude that  $U'_j <_h S$  and  $val_h(U'_j) = 0$ . We claim that the pair  $(U'_i, U'_j)$  is  $S$ -appropriate. Towards a contradiction, assume that the pair is not  $S$ -appropriate, and hence, without loss of generality,  $h$  includes an  $\text{update}_i$  operation  $U$  such that  $U'_i <_h U <_h U'_j$ . Therefore, since  $U'_j <_h S$ , we get that  $U'_i \notin I_i(S)$ , in contradiction to the choice of  $U'_i$ .

Second, we deal with the case that  $(val_{h:i}(S), val_{h:j}(S)) = (1, 1)$ . If the pair  $(U_i, U_j)$  is  $S$ -appropriate, we are done. Otherwise, without loss of generality, there exist  $\text{update}_i$  operations that follow  $U_i$  and precede  $U_j$ . Let  $U$  be the maximal  $\text{update}_i$  operation such that  $U_i <_h U <_h U_j$ . Clearly,  $U \in I_i(S)$ . Since  $h$  is  $(i, j)$ -simple,  $val_h(U) = 1$ . Hence, the pair  $(U, U_j)$  is  $S$ -appropriate.  $\blacktriangleleft$

**Proof of Lemma 14.** It is not difficult to see that any item implies that there exists no  $S$ -appropriate pair in  $h$ . To prove the other direction, take a complete  $\text{scan}$  operation  $S$  such that there is no  $S$ -appropriate pair in  $h$ . We aim to prove that one of the items holds. If one of the first two items holds we are done. Otherwise, we assume that items one and two do not hold, and we prove that one of the last two items holds.

Since items one and two do not hold, there exist  $U_i \in I_i(S)$  and  $U_j \in I_j(S)$  such that  $val_h(U_i) = val_{h:i}(S)$  and  $val_h(U_j) = val_{h:j}(S)$ . Since there is no  $S$ -appropriate pair in  $h$ , by the previous lemma,  $val_{h:i}(S) \neq val_{h:j}(S)$ . Assume, without loss of generality, that  $(val_{h:i}(S), val_{h:j}(S)) = (0, 1)$ . To show that item three holds, we need to prove that  $F_i <_h F_j$ .

Let  $W_i$  be the first  $\text{update}_i$  operation in  $I_i(S)$ . Hence,  $W_i <_h S$ . Moreover,  $W_i \leq_h U_i$  thus  $val_h(W_i) = 0$ . Let  $W_j$  be the first  $\text{update}_j(1)$  operation in  $I_j(S)$ . We claim that  $W_j = F_j$ .

Towards a contradiction, assume that  $W_j \neq F_j$ , and conclude that  $F_j <_h W_j$ . As a result,  $W_j < S$ , since otherwise, we get that the  $\text{update}_j$  operation that precedes  $W_j$  is also an  $\text{update}_j(1)$  operation in  $I_j(S)$ , which contradicts the minimality of  $W_j$ . Therefore, the following hold:

- $W_i <_h S$ ,  $W_i \in I_i(S)$  and  $val_h(W_i) = 0$ .
- $W_j <_h S$ ,  $W_j \in I_j(S)$  and  $val_h(W_j) = 1$ .

As in the proof of Lemma 42, it follows that  $(W_i, W_j)$  is an  $S$ -appropriate pair, in contradiction to our assumption. Hence,  $W_j = F_j$  and in particular,  $F_j \in I_j(S)$ .

Now, by our assumption, the pair  $(W_i, F_j)$  is not  $S$ -appropriate. Hence, either there exists an  $\text{update}_i$  operation between  $W_i$  and  $F_j$ , or there exists an  $\text{update}_j$  operation between  $F_j$  and  $W_i$ . First, assume that  $W'_j$  is an  $\text{update}_j$  operation such that  $F_j <_h W'_j <_h W_i$ . Thus, since  $W_i <_h S$ , we get that  $F_j <_h W'_j <_h S$ , in contradiction to  $F_j \in I_j(S)$ . Hence, there are some  $\text{update}_i$  operations between  $W_i$  and  $F_j$ .

Let  $W'_i$  be the maximal  $\text{update}_i$  operation such that  $W_i <_h W'_i <_h F_j$ , and note that  $W'_i \in I_i(S)$ . If  $val_h(W'_i) = 0$ , the pair  $(W'_i, F_j)$  is  $S$ -appropriate. Hence,  $val_j(W'_i) = 1$ . Therefore, as  $h$  is  $(i, j)$ -simple,

$$F_i \leq_h W'_i <_h F_j,$$

as required.  $\blacktriangleleft$

**Lemma 15.** *There exists an automaton  $M_3$  such that, for any  $(i, j)$ -simple history  $h$ ,  $h$  violates Appropriateness if and only if  $h \in L(M_3)$ . Moreover,  $M_3$  has  $O(n)$  states and  $O(n^2)$  transitions.*

**Proof.** For  $k < n$  consider the languages:

$$\begin{aligned} L_{1k,i} &= L(\Sigma^*(\text{inv.update}_i(1))\Sigma^*(\text{res.update}_i)\Sigma^*(\text{inv.scan}_k) \\ &\quad \Sigma^*(\text{res.scan}_k(0, 0) + \text{res.scan}_k(0, 1))) \end{aligned}$$

$$L1_{k,j} = L(\Sigma^*(inv.update_j(1))\Sigma^*(res.update_j)\Sigma^*(inv.scan_k) \\ \Sigma^*(res.scan_k(0,0) + res.scan_k(1,0)))$$

Observe that for an  $(i,j)$ -simple history  $h$ ,  $h \in \bigcup_{k=1}^n (L1_{k,i} \cup L1_{k,j})$  if and only if the first item of Lemma 14 holds in  $h$  for some complete `scan` operation  $S$ . Note that it is possible to construct an automaton with  $O(1)$  states and  $O(n)$  transitions that recognizes the language  $L1_{k,i} \cup L1_{k,j}$ . Hence, there exists an automaton with  $O(n)$  states and  $O(n^2)$  transitions that recognizes the language  $\bigcup_{k=1}^n (L1_{k,i} \cup L1_{k,j})$ .

Similarly, consider the languages

$$L2_i = L((\Sigma - inv.update_i(1))^*(res.scan_0(1,0) + res.scan_0(1,1) + \\ \dots + res.scan_{n-1}(1,0) + res.scan_{n-1}(1,1))\Sigma^*)$$

$$L2_j = L((\Sigma - inv.update_j(1))^*(res.scan_0(0,1) + res.scan_0(1,1) + \\ \dots + res.scan_{n-1}(0,1) + res.scan_{n-1}(1,1))\Sigma^*)$$

Observe that for an  $(i,j)$ -simple history  $h$ ,  $h \in L2_i \cup L2_j$  if and only if the second item of Lemma 14 holds in  $h$  for some complete `scan` operation  $S$ . Note that it is possible to construct an automaton with  $O(1)$  states and  $O(n)$  transitions that recognizes the language  $L2_i \cup L2_j$ .

Finally, consider the languages

$$L3 = L((\Sigma - inv.update_j(1))^* inv.update_i(1) (\Sigma - inv.update_j(1))^* res.update_i) \cap \\ L(\Sigma^*(res.scan_0(0,1) + \dots + res.scan_{n-1}(0,1))\Sigma^*)$$

$$L4 = L((\Sigma - inv.update_i(1))^* inv.update_j(1) (\Sigma - inv.update_i(1))^* res.update_j) \cap \\ L(\Sigma^*(res.scan_0(1,0) + \dots + res.scan_{n-1}(1,0))\Sigma^*)$$

For a simple history  $h$  and  $m \in \{3, 4\}$ ,  $h \in L_m$  iff the  $m$ th item of Lemma 14 holds for some complete `scan` operation  $h$ . Note that  $L_m$  is accepted by an automaton with  $O(1)$  states and  $O(n)$  transitions.

As a result, there exists an automaton  $M3$  with  $O(n)$  states and  $O(n^2)$  transitions that recognizes the language  $(\bigcup_{k=1}^n (L1_{k,i} \cup L1_{k,j})) \cup L2_i \cup L2_j \cup L3 \cup L4$ . For an  $(i,j)$ -simple history  $h$ ,  $h \in L(M3)$  if and only if one of the properties of Lemma 14 holds for  $h$ . Hence,  $h \in L(M3)$  if and only if  $h$  violates appropriateness. ◀