On the Complexity of Checking Transactional Consistency

RANADEEP BISWAS, Universite de Paris, IRIF, CNRS, France
CONSTANTIN ENEA, Universite de Paris, IRIF, CNRS, France

Transactions simplify concurrent programming by enabling computations on shared data that are isolated from other concurrent computations and are resilient to failures. Modern databases provide different consistency models for transactions corresponding to different tradeoffs between consistency and availability. In this work, we investigate the problem of checking whether a given execution of a transactional database adheres to some consistency model. We show that consistency models like read committed, read atomic, and causal consistency are polynomial time checkable while prefix consistency and snapshot isolation are NP-complete in general. These results complement a previous NP-completeness result concerning serializability. Moreover, in the context of NP-complete consistency models, we devise algorithms that are polynomial time assuming that certain parameters in the input executions, e.g., the number of sessions, are fixed. We evaluate the scalability of these algorithms in the context of several production databases.

1 INTRODUCTION

Transactions simplify concurrent programming by enabling computations on shared data that are isolated from other concurrent computations and resilient to failures. Modern databases provide transactions in various forms corresponding to different tradeoffs between consistency and availability. The strongest level of consistency is achieved with *serializable* transactions [23] whose outcome in concurrent executions is the same as if the transactions were executed atomically in some order. Unfortunately, serializability carries a significant penalty on the availability of the system assuming, for instance, that the database is accessed over a network that can suffer from partitions or failures. For this reason, modern databases often provide weaker guarantees about transactions, formalized by weak consistency models, e.g., causal consistency [20] and snapshot isolation [10].

Implementations of large-scale databases providing transactions are difficult to build and test. For instance, distributed (replicated) databases must account for partial failures, where some components or the network can fail and produce incomplete results. Ensuring fault-tolerance relies on intricate protocols that are difficult to design and reason about. The black-box testing framework Jepsen [1] found a remarkably large number of subtle problems in many production distributed databases.

Testing a transactional database raises two issues: (1) deriving a suitable set of testing scenarios, e.g., faults to inject into the system and the set of transactions to be executed, and (2) deriving efficient algorithms for checking whether a given execution satisfies the considered consistency model. The Jepsen framework aims to address the first issue by using randomization, e.g., introducing faults at random and choosing the operations in a transaction randomly. The effectiveness of this approach has been proved formally in recent work [22]. The second issue is, however, largely unexplored. Jepsen checks consistency in a rather ad-hoc way, focusing on specific classes of violations to a given consistency model, e.g., dirty reads (reading values from aborted transactions). This problem is challenging because the consistency specifications are non-trivial and they cannot be checked using, for instance, standard local assertions added to the client’s code.
Besides serializability, the complexity of checking correctness of an execution w.r.t. some consistency model is unknown. Checking serializability has been shown to be NP-complete [23], and checking causal consistency in a non-transactional context is known to be polynomial time [11]. In this work, we try to fill this gap by investigating the complexity of this problem w.r.t. several consistency models and, in case of NP-completeness, devising algorithms that are polynomial time assuming fixed bounds for certain parameters of the input executions, e.g., the number of sessions.

We consider several consistency models that are the most prevalent in practice. The weakest of them, Read Committed (RC) [10], requires that every value read in a transaction is written by a committed transaction. Read Atomic (RA) [14] requires that successive reads of the same variable in a transaction return the same value (also known as Repeatable Reads [10]), and that a transaction “sees” the values written by previous transactions in the same session. In general, we assume that transactions are organized in sessions [24], an abstraction of the sequence of transactions performed during the execution of an application. Causal Consistency (CC) [20] requires that if a transaction \( t_1 \) “affects” another transaction \( t_2 \), e.g., \( t_1 \) is ordered before \( t_2 \) in the same session or \( t_2 \) reads a value written by \( t_1 \), then these two transactions are observed by any other transaction in this order. Prefix Consistency (PC) [13] requires that there exists a total commit order between all the transactions such that each transaction observes a prefix of this sequence. Snapshot Isolation (SI) [10] further requires that two different transactions observe different prefixes if they both write to a common variable. Finally, we also provide new results concerning the problem of checking serializability (SER) that complement the known result about its NP-completeness.

The algorithmic issues we explore in this paper have led to a new specification framework for these consistency models that relies on the fact that the write-read relation in an execution (also known as read-from), relating reads with the transactions that wrote their value, can be defined effectively. The write-read relation can be extracted easily from executions where each value is written at most once (a variable can be written an arbitrary number of times). This can be easily enforced by tagging values with unique identifiers (e.g., a local counter that is incremented with every new write coupled with a client/session identifier). Since practical database implementations are data-independent [25], i.e., their behavior doesn’t depend on the concrete values read or written in the transactions, any potential buggy behavior can be exposed in executions where each value is written at most once. Therefore, this assumption is without loss of generality.

Previous work [11, 12, 14] has formalized such consistency models using two auxiliary relations: a visibility relation defining for each transaction the set of transactions it observes, and a commit order defining the order in which transactions are committed to the “global” memory. An execution satisfying some consistency model is defined as the existence of a visibility relation and a commit order obeying certain axioms. In our case, the write-read relation derived from the execution plays the role of the visibility relation. This simplification allows us to state a series of axioms defining these consistency models, which have a common shape. Intuitively, they define lower bounds on the set of transactions \( t_1 \) that must precede in commit order a transaction \( t_2 \) that is read in the execution. Besides shedding a new light on the differences between these consistency models, these axioms are essential for the algorithmic issues we investigate afterwards.

We establish that checking whether an execution satisfies RC, RA, or CC is polynomial time, while the same problem is NP-complete for PC and SI. Moreover, in the case of the NP-complete consistency models (PC, SI, SER), we show that their verification problem becomes polynomial time provided that, roughly speaking, the number of sessions in the input executions is considered to be fixed (i.e., not counted for in the input size). In more detail, we establish that checking SER reduces to a search problem in a space that has polynomial size when the number of sessions is

\[1\]This is also used in Jepsen, e.g., checking dirty reads in Galera [2].
fixed. (This algorithm applies to arbitrary executions, but its complexity would be exponential in the number of sessions in general.) Then, we show that checking PC or SI can be reduced in polynomial time to checking SER using a transformation of executions that, roughly speaking, splits each transaction in two parts: one part containing all the reads, and one part containing all the writes (SI further requires adding some additional variables in order to deal with transactions writing on a common variable). We extend these results even further by relying on an abstraction of executions called communication graphs [15]. Roughly speaking, the vertices of a communication graph correspond to sessions, and the edges represent the fact that two sessions access (read or write) the same variable. We show that all these criteria are polynomial-time checkable provided that the biconnected components of the communication graph are of fixed size.

We provide an experimental evaluation of our algorithms on executions of CockroachDB [3], which claims to implement serializability [4] acknowledging however the possibility of anomalies, Galera [5], whose documentation contains contradicting claims about whether it implements snapshot isolation [6, 7], and AntidoteDB [8], which claims to implement causal consistency [9]. Our implementation reports violations of these criteria in all cases. The consistency violations we found for AntidoteDB are novel and have been confirmed by its developers. We show that our algorithms are efficient and scalable. In particular, we show that, although the asymptotic complexity of our algorithms is exponential in general (w.r.t. the number of sessions), the worst-case behavior is not exercised in practice.

To summarize, the contributions of this work are fourfold:
- We develop a new specification framework for describing common transactional-consistency criteria (Âğ2);
- We show that checking RC, RA, and CC is polynomial time while checking PC and SI is NP-complete (Âğ3);
- We show that PC, SI, and SER are polynomial-time checkable assuming that the communication graph of the input execution has fixed-size biconnected components (Âğ4 and Âğ5);
- We perform an empirical evaluation of our algorithms on executions generated by production databases (Âğ6);

Combined, these contributions form an effective algorithmic framework for the verification of transactional-consistency models. To the best of our knowledge, we are the first to investigate the asymptotic complexity for most of these consistency models, despite their prevalence in practice.

2 CONSISTENCY CRITERIA

2.1 Histories

We consider a transactional database storing a set of variables $\text{Var} = \{x, y, \ldots\}$. Clients interact with the database by issuing transactions formed of read and write operations. Assuming an unspecified set of values $\text{Val}$ and a set of operation identifiers $\text{OpId}$, we let

$$\text{Op} = \{\text{read}_i(x, v), \text{write}_i(x, v) : i \in \text{OpId}, x \in \text{Var}, v \in \text{Val}\}$$

be the set of operations reading a value $v$ or writing a value $v$ to a variable $x$. We omit operation identifiers when they are not important.

**Definition 2.1.** A transaction $\langle O, \text{po} \rangle$ is a finite set of operations $O$ along with a strict total order $\text{po}$ on $O$, called program order.

We use $t$, $t_1$, $t_2$, $\ldots$ to range over transactions. The set of read, resp., write, operations in a transaction $t$ is denoted by $\text{reads}(t)$, resp., $\text{writes}(t)$. The extension to sets of transactions is
writes to the same variable in the same transaction.

When write

4 Ranadeep Biswas and Constantin Enea, Vol. 1, No. 1, Article . Publication date: August 2018.

that ⟨

2

behavior does not depend on the concrete values read or written in the transactions, any potential each value is written at most once. Since in practice, databases are data-independent [25], i.e., their execution. As mentioned before, such a relation can be extracted easily from executions where write-read relation that identifies the transaction writing the value returned by each read in the session union of sequences, each sequence being called a session order so represents ordering constraints imposed by the applications using the database. Most often, they can be ignored. For instance, the read(x) in Figure 1a should not return 1 because this is not the last value written to x by the other transaction. It can return the initial value or 2. Also, if a read would be preceded by a write to the same variable in the same transaction, then it should return a value written in the same transaction (i.e., the value written by the latest write to x in that transaction). For instance, the read(x) in Figure 1b can only return 2 (assuming that there are no other writes on x in the same transaction). These two properties can be verified easily (in a syntactic manner) on a given execution. Beyond these two properties, the various consistency criteria used in practice constrain only the last writes to each variable in each transaction and the reads that are not preceded by writes to the same variable in the same transaction.

Consistency criteria are formalized on an abstract view of an execution called history. A history includes only successful or committed transactions. In the context of databases, it is always assumed that the effect of aborted transactions should not be visible to other transactions, and therefore, they can be ignored. For instance, the read(x) in Figure 1c should not return the value 1 written by the aborted transaction. The transactions are ordered according to a (partial) session order so which represents ordering constraints imposed by the applications using the database. Most often, so is a union of sequences, each sequence being called a session. We assume that the history includes a write-read relation that identifies the transaction writing the value returned by each read in the execution. As mentioned before, such a relation can be extracted easily from executions where each value is written at most once. Since in practice, databases are data-independent [25], i.e., their behavior does not depend on the concrete values read or written in the transactions, any potential buggy behavior can be exposed in such executions.

Definition 2.2. A history ⟨T, so, wr⟩ is a set of transactions T along with a strict partial order so called session order, and a relation wr ⊆ T × reads(T) called write-read relation, s.t.

• the inverse of wr is a total function, and if (t, read(x, v)) ∈ wr, then write(x, v) ∈ t, and
• so ∪ wr is acyclic.

That is, for every transaction t, and every write(x, v), write(y, v′) ∈ writes(t), we have that x ≠ y.

That is, for every transaction t = ⟨O, po⟩, if write(x, v) ∈ writes(t) and there exists read(x, v) ∈ reads(t), then we have that ⟨read(x, v), write(x, v)⟩ ∈ po
We describe an axiomatic framework to characterize the set of histories satisfying a certain consistency criterion. The overarching principle is to say that a history satisfies a certain criterion if there exists a strict total order on its transactions, called commit order and denoted by \( \text{co} \), which extends the write-read relation and the session order, and which satisfies certain properties. These properties are expressed by a set of axioms that relate the commit order with the session-order and the write-read relation in the history.

![Fig. 2. Definitions of consistency axioms. The reflexive and transitive, resp., transitive, closure of a relation \( \text{rel} \) is denoted by \( \text{rel}^{*} \), resp., \( \text{rel}^{+} \). Also, \( \circ \) denotes the composition of two relations, i.e., \( \text{rel}_1 \circ \text{rel}_2 = \{ (a, b) | \exists c. (a, c) \in \text{rel}_1 \land (c, b) \in \text{rel}_2 \} \).

To simplify the technical exposition, we assume that every history includes a distinguished transaction writing the initial values of all variables. This transaction precedes all the other transactions in \( \text{so} \). We use \( h, h_1, h_2, \ldots \) to range over histories.

We say that the read operation \( \text{read}(x, v) \) reads value \( v \) from variable \( x \) written by \( t \) when \( (t, \text{read}(x, v)) \in \text{wr} \). For a given variable \( x \), \( \text{wr}_x \) denotes the restriction of \( \text{wr} \) to reads of variable \( x \), i.e., \( \text{wr}_x = \text{wr} \cap (T \times \{ \text{read}(x, v) | v \in \text{Val} \}) \). Moreover, we extend the relations \( \text{wr} \) and \( \text{wr}_x \) to pairs of transactions as follows: \( \langle t_1, t_2 \rangle \in \text{wr} \), resp., \( \langle t_1, t_2 \rangle \in \text{wr}_x \), iff there exists a read operation \( \text{read}(x, v) \in \text{reads}(t_2) \) such that \( \langle t_1, \text{read}(x, v) \rangle \in \text{wr}_x \), resp., \( \langle t_1, \text{read}(x, v) \rangle \in \text{wr}_x \). We say that the transaction \( t_1 \) is read by the transaction \( t_2 \) when \( \langle t_1, t_2 \rangle \in \text{wr}_x \), and that it is read when it is read by some transaction \( t_2 \).

### 2.2 Axiomatic Framework

We describe an axiomatic framework to characterize the set of histories satisfying a certain consistency criterion. The overarching principle is to say that a history satisfies a certain criterion if there exists a strict total order on its transactions, called commit order and denoted by \( \text{co} \), which extends the write-read relation and the session order, and which satisfies certain properties. These properties are expressed by a set of axioms that relate the commit order with the session-order and the write-read relation in the history.
The axioms we use have a uniform shape: they define mandatory co predecessors $t_2$ of a transaction $t_1$ that is read in the history. For instance, the criterion called Read Committed (RC) [10] requires that every value read in the history was written by a committed transaction, and also, that the reads in the same transaction are “monotonic” in the sense that they do not return values that are older, w.r.t. the commit order, than other values read in the past\textsuperscript{4}. While the first condition holds for any history (because of the surjectivity of wr), the second condition is expressed by the axiom Read Committed in Figure 2a. This axiom states that for any transaction $t_1$ writing a variable $x$ that is read in a transaction $t$, the set of transactions $t_2$ writing $x$ and read previously in the same transaction must precede $t_1$ in commit order. For instance, Figure 3a shows a history and a (partial) commit order that does not satisfy this axiom because read($x$) returns the value written in a transaction “older” than the transaction read in the previous read($y$). An example of a history and commit order satisfying this axiom is given in Figure 3b.

More precisely, the axioms are first-order formulas\textsuperscript{5} of the following form:

$$\forall x, \forall t_1, t_2, \forall \alpha. t_1 \neq t_2 \land \langle t_1, \alpha \rangle \in \text{wr}_x \land t_2 \text{ writes } x \land \phi(t_2, \alpha) \Rightarrow \langle t_2, t_1 \rangle \in \text{co}$$

where $\phi$ is a property relating $t_2$ and $\alpha$ (i.e., the read or the transaction reading from $t_1$) that varies from one axiom to another. Intuitively, this axiom schema states the following: in order for $\alpha$ to read specifically $t_1$’s write on $x$, it must be the case that every $t_2$ that also writes $x$ and satisfies

\textsuperscript{4}This monotonicity property corresponds to the fact that in the original formulation of Read Committed [10], every write is guarded by the acquisition of a lock on the written variable, that is held until the end of the transaction.

\textsuperscript{5}These formulas are interpreted on tuples $\langle h, \text{co} \rangle$ of a history $h$ and a commit order $\text{co}$ on the transactions in $h$ as usual.

Fig. 3. Examples of histories used to explain the axioms in Figure 2. For readability, the wr relation is defined by the values written in comments with each read.
\( \phi(t_2, \alpha) \) was committed before \( t_1 \). Note that in all cases we consider, \( \phi(t_2, \alpha) \) already ensures that \( t_2 \) is committed before the read \( \alpha \), so this axiom schema ensures that \( t_2 \) is furthermore committed before \( t_1 \)'s write.

The axioms used throughout the paper are given in Figure 2. The property \( \phi \) relates \( t_2 \) and \( \alpha \) using the write-read relation and the session order in the history, and the commit order.

In the following, we explain the rest of the consistency criteria we consider and the axioms defining them. \textsc{Read Atomic} (RA) [14] is a strengthening of \textsc{Read Committed} defined by the axiom \textsc{Read Atomic}, which states that for any transaction \( t_1 \) writing a variable \( x \) that is read in a transaction \( t_3 \), the set of \( \text{wr} \) or \( \text{so} \) predecessors of \( t_3 \) writing \( x \) must precede \( t_1 \) in commit order. The case of \( \text{wr} \) predecessors corresponds to the Repeatable Read criterion in [10] which requires that successive reads of the same variable in the same transaction return the same value, Figure 3b showing a violation, and also that every read of a variable \( x \) in a transaction \( t \) returns the value written by the maximal transaction \( t' \) (w.r.t. the commit order) that is read by \( t \), Figure 3d showing a violation (for any commit order between the transactions on the left, either \( \text{read}(x) \) or \( \text{read}(y) \) will return a value not written by the maximal transaction). The case of \( \text{so} \) predecessors corresponds to the “read-my-writes” guarantee [24] concerning sessions, which states that a transaction \( t \) must observe previous writes in the same session. For instance, \( \text{read}(y) \) returning 1 in Figure 3c shows that the last transaction on the right does not satisfy this guarantee: the transaction writing 1 to \( y \) was already visible to that session before it wrote 2 to \( y \), and therefore the value 2 should have been read. \text{Read Atomic} requires that the \( \text{so} \) predecessor of the transaction reading \( y \) be ordered in \( \text{co} \) before the transaction writing 1 to \( y \), which makes the union \( \text{co} \cup \text{wr} \) cyclic.

The following lemma shows that for histories satisfying \text{Read Atomic}, the inverse of \( \text{wr} \), extended to transactions is a total function (see Appendix A for the proof).

**Lemma 2.3.** Let \( h = (T, \text{so}, \text{wr}) \) be a history. If \( \langle h, \text{co} \rangle \) satisfies \text{Read Atomic}, then for every transaction \( t \) and two reads \( \text{read}_i(x, v_1), \text{read}_i(x, v_2) \in \text{reads}(t) \), \( \text{wr}^{-1}(\text{read}_i(x, v_1)) = \text{wr}^{-1}(\text{read}_i(x, v_2)) \) and \( v_1 = v_2 \).

**Causal Consistency** (CC) [20] is defined by the axiom Causal, which states that for any transaction \( t_1 \) writing a variable \( x \) that is read in a transaction \( t_3 \), the set of \( (\text{wr} \cup \text{so})^+ \) predecessors of \( t_3 \) writing \( x \) must precede \( t_1 \) in commit order (\( (\text{wr} \cup \text{so})^+ \) is usually called the causal order). A violation of this axiom can be found in Figure 3e: the transaction \( t_2 \) writing 2 to \( x \) is a \( (\text{wr} \cup \text{so})^+ \) predecessor of the transaction \( t_3 \) reading 1 from \( x \) because the transaction \( t_4 \), writing 1 to \( y \), reads \( x \) from \( t_2 \) and \( t_3 \) reads \( y \) from \( t_4 \). This implies that \( t_2 \) should precede in commit order the transaction \( t_1 \) writing 1 to \( x \), which again, is inconsistent with the write-read relation \( t_2 \) reads from \( t_1 \).

**Prefix Consistency** (PC) [13] is a strengthening of CC, which requires that every transaction observes a prefix of a commit order between all the transactions. With the intuition that the observed transactions are \( \text{wr} \cup \text{so} \) predecessors, the axiom Prefix defining PC, states that for any transaction \( t_1 \) writing a variable \( x \) that is read in a transaction \( t_3 \), the set of \( \text{co}^+ \) predecessors of
transactions observed by \( t_3 \) writing \( x \) must precede \( t_1 \) in commit order (we use \( \text{co}^* \) to say that even the transactions observed by \( t_3 \) must precede \( t_1 \)). This ensures the prefix property stated above. An example of a PC violation can be found in Figure 3f: the two transactions on the bottom read from the three transactions on the top, but any serialization of those three transactions will imply that one of the combinations \( x=1, y=2 \) or \( x=2, y=1 \) cannot be produced at the end of a prefix in this serialization.

**Snapshot Isolation (SI)** [10] is a strengthening of PC that disallows two transactions to observe the same prefix of a commit order if they conflict, i.e., write to a common variable. It is defined by the conjunction of Prefix and another axiom called Conflict, which requires that for any transaction \( t_1 \) writing a variable \( x \) that is read in a transaction \( t_3 \), the set of \( \text{co}^* \) predecessors writing \( x \) of transactions conflicting with \( t_3 \) and before \( t_3 \) in commit order, must precede \( t_1 \) in commit order. Figure 3g shows a Conflict violation.

Finally, **Serializability (SER)** [23] is defined by the axiom with the same name, which requires that for any transaction \( t_1 \) writing to a variable \( x \) that is read in a transaction \( t_3 \), the set of \( \text{co} \) predecessors of \( t_3 \) writing \( x \) must precede \( t_1 \) in commit order. This ensures that each transaction observes the effects of all the \( \text{co} \) predecessors. Figure 3h shows a Serializability violation.

**Lemma 2.4.** The following entailments hold:

- \( \text{Causal} \Rightarrow \text{Read Atomic} \Rightarrow \text{Read Committed} \)
- \( \text{Prefix} \Rightarrow \text{Causal} \)
- \( \text{Serializability} \Rightarrow \text{Prefix} \land \text{Conflict} \)

**Definition 2.5.** Given a set of axioms \( X \) defining a criterion \( C \) like in Table 1, a history \( h = \langle T, \text{so}, \text{wr} \rangle \) satisfies \( C \) iff there exists a strict total order \( \text{co} \) such that \( \text{wr} \cup \text{so} \subseteq \text{co} \) and \( \langle h, \text{co} \rangle \) satisfies \( X \).

Definition 2.5 and Lemma 2.4 imply that each consistency criterion in Table 1 is stronger than its predecessors (reading them from top to bottom), e.g., CC is stronger than RA and RC. This relation is strict, e.g., RA is not stronger than CC. These definitions are equivalent with previous formalizations by Cerone et al. [14] (see Appendix E).

## 3 CHECKING CONSISTENCY CRITERIA

This section establishes the complexity of checking the different consistency criteria in Table 1 for a given history. More precisely, we show that \( \text{READ COMMITTED}, \text{READ ATOMIC}, \text{AND CAUSAL CONSISTENCY} \) can be checked in polynomial time while the problem of checking the rest of the criteria is NP-complete.
On the Complexity of Checking Transactional Consistency

Input: A history $h = \langle T, so, wr \rangle$

Output: $true$ iff $h$ satisfies Causal consistency

1. if $so \cup wr$ is cyclic then return $false$;
2. $co \leftarrow so \cup wr$;
3. foreach $x \in \text{vars}(h)$ do
   4. if $\exists t_1, t_2 \in T$ s.t. $t_1$ and $t_2$ write $x$ do
      5. $co \leftarrow co \cup \{ \langle t_2, t_1 \rangle \}$;
   6. if $co$ is cyclic then return $false$;
7. else return $true$;

Algorithm 1: Checking Causal consistency

Intuitively, the polynomial time results are based on the fact that the axioms defining those consistency criteria do not contain the commit order ($co$) on the left-hand side of the entailment. Therefore, proving the existence of a commit order satisfying those axioms can be done using a saturation procedure that builds a “partial” commit order based on instantiating the axioms on the write-read relation and the session order in the given history. Since the commit order must be an extension of the write-read relation and the session order, it contains those two relations from the beginning. This saturation procedure stops when the order constraints derived this way become cyclic. For instance, let us consider applying such a procedure corresponding to RA on the histories in Figure 4a and Figure 4b. Applying the axiom in Figure 2b on the first history, since the transaction on the right reads 2 from $y$, we get that its $wr_x$ predecessor (i.e., the first transaction on the left) must precede the transaction writing 2 to $y$ in commit order (the red edge). This holds because the $wr_x$ predecessor writes on $y$. Similarly, since the same transaction reads 1 from $x$, we get that its $wr_y$ predecessor must precede the transaction writing 1 to $x$ in commit order (the blue edge). This already implies a cyclic commit order, and therefore, this history does not satisfy RA. On the other hand, for the history in Figure 4b, all the axiom instantiations are vacuous, i.e., the left part of the entailment is false, and therefore, it satisfies RA. Checking CC on the history in Figure 4c requires a single saturation step: since the transaction on the bottom right reads 1 from $x$, its $wr_x; wr_y$ predecessor that writes on $x$ (the transaction on the bottom left) must precede in commit order the transaction writing 1 to $x$. Since this is already inconsistent with the session order, we get that this history violates CC.

Algorithm 1 lists our procedure for checking CC. As explained above, $co$ is initially set to $so \cup wr$, and then, it is saturated with other ordering constraints implied by non-vacuous instantiations of the axiom Causal (where the left-hand side of the implication evaluates to true). The algorithms concerning RC and RA are defined in a similar way by essentially changing the test at line 6 so that it corresponds to the left-hand side of the implication in the corresponding axiom. Algorithm 1 can be rewritten as a Datalog program containing straightforward Datalog rules for computing transitive closures and relation composition, and a rule of the form

$\langle t_2, t_1 \rangle \in co : t_1 \neq t_2, \langle t_1, t_3 \rangle \in wr_x, \langle t_2, t_3 \rangle \in (so \cup wr)^+$

---

We write Datalog rules using a standard notation $head :- body$ where $head$ is a relational atom (written as $\langle a, b \rangle \in R$ where $a, b$ are elements and $R$ a binary relation) and $body$ is a list of relational atoms.

Vol. 1, No. 1, Article . Publication date: August 2018.
to represent the Causal axiom. The following is a consequence of the fact that these algorithms run in polynomial time (or equivalently, the Datalog programs can be evaluated in polynomial time over a database that contains the \textit{wr} and \textit{so} relations in a given history).

**Theorem 3.1.** For any criterion \( C \in \{\text{Read Committed, Read Atomic, Causal consistency}\}, the problem of checking whether a given history satisfies \( C \) is polynomial time.

On the other hand, checking PC, SI, and SER is NP-complete in general. We show this using a reduction from boolean satisfiability (SAT) that covers uniformly all the three cases. In the case of SER, it provides a new proof of the NP-completeness result by Papadimitriou [23] which uses a reduction from boolean satisfiability (SAT) that covers uniformly all the three cases. In the case of SER, it provides a new proof of the NP-completeness result by Papadimitriou [23] which uses a reduction from boolean satisfiability (SAT) that covers uniformly all the three cases.

**Theorem 3.2.** For any criterion \( C \in \{\text{Prefix Consistency, Snapshot Isolation, Serializability}\} the problem of checking whether a given history satisfies \( C \) is NP-complete.

**Proof.** Given a history, any of these three criteria can be checked by guessing a total commit order on its transactions and verifying whether it satisfies the corresponding axioms. This shows that the problem is in NP.

To show NP-hardness, we define a reduction from boolean satisfiability. Therefore, let \( \varphi = D_1 \land \ldots \land D_m \) be a CNF formula over the boolean variables \( x_1, \ldots, x_n \) where each \( D_i \) is a disjunctive clause with \( m_i \) literals. Let \( \lambda_{ij} \) denote the \( j \)-th literal of \( D_i \).

We construct a history \( h_{\varphi} \) such that \( \varphi \) is satisfiable if and only if \( h_{\varphi} \) satisfies PC, SI, or SER. Since \( \text{SER} \Rightarrow \text{SI} \Rightarrow \text{PC} \), we show that (1) if \( h_{\varphi} \) satisfies PC, then \( \varphi \) is satisfiable, and (2) if \( \varphi \) is satisfiable, then \( h_{\varphi} \) satisfies SER.

The main idea of the construction is to represent truth values of each of the variables and literals in \( \varphi \) with the polarity of the commit order between corresponding transaction pairs. For each variable \( x_k \), \( h_{\varphi} \) contains a pair of transactions \( a_k \) and \( b_k \), and for each literal \( \lambda_{ij} \), \( h_{\varphi} \) contains a set of transactions \( w_{ij}, y_{ij} \) and \( z_{ij} \).\footnote{We assume that the transactions \( a_k \) and \( b_k \) associated to a variable \( x_k \) are distinct and different from the transactions associated to another variable \( x_k’ \neq x_k \) or to a literal \( \lambda_{ij} \). Similarly, for the transactions \( w_{ij}, y_{ij} \) and \( z_{ij} \) associated to a literal \( \lambda_{ij} \).}

We want to have that \( \lambda_{ij} \) is false if and only if \( h_{\varphi} \) satisfies PC, then \( \varphi \) is satisfiable, and (2) if \( \varphi \) is satisfiable, then \( h_{\varphi} \) satisfies SER.

The history \( h_{\varphi} \) should ensure that the \textit{co} ordering constraints corresponding to an assignment that falsifies the formula (i.e., one of its clauses) form a cycle. To achieve that, we add all pairs \( (z_{ij}, y_{i,(j+1)\%m_i}) \) in the session order \textit{so}. An unsatisfied clause \( D_i \), i.e., every \( \lambda_{ij} \) is false, leads to a cycle of the form \( y_{i1} \rightarrow z_{i1} \rightarrow y_{i2} \rightarrow z_{i2} \ldots z_{i m_i} \rightarrow y_{i1} \).

The most complicated part of the construction is to ensure the consistency between the truth value of the literals and the truth value of the variables, e.g., \( \lambda_{ij} = x_k \) is false iff \( x_k \) is false. We use
special sub-histories to enforce that if history \( h_\phi \) satisfies PC (i.e., the axiom Prefix), then there exists a commit order \( \text{co} \) such that \( \langle h_\phi, \text{co} \rangle \) satisfies Prefix (Figure 2d) and:

\[
\langle a_k, b_k \rangle \in \text{co} \iff \langle y_{ij}, z_{ij} \rangle \in \text{co} \text{ when } \lambda_{ij} = x_k, \quad \text{and} \quad (1)
\]

\[
\langle a_k, b_k \rangle \in \text{co} \iff \langle z_{ij}, y_{ij} \rangle \in \text{co} \text{ when } \lambda_{ij} = \neg x_k.
\]

Figure 5a shows the sub-history associated to a positive literal \( \lambda_{ij} = x_k \) while Figure 5b shows the case of a negative literal \( \lambda_{ij} = \neg x_k \).

For a positive literal \( \lambda_{ij} = x_k \) (Figure 5a), (1) we enrich session order with the pairs \( \langle y_{ij}, a_k \rangle \) and \( \langle b_k, w_{ij} \rangle \), (2) we include writes to a variable \( v_{ij} \) in the transactions \( y_{ij} \) and \( z_{ij} \), and (3) we make \( w_{ij} \) read from \( z_{ij} \), i.e., \( \langle z_{ij}, w_{ij} \rangle \in \text{wr}_{v_{ij}} \). The case of a negative literal is similar, switching the roles of \( a_k \) and \( b_k \).

This construction ensures that if the \( \text{co} \) goes downwards on the right-hand side (\( \langle a_k, b_k \rangle \in \text{co} \) in the case of a positive literal, and \( \langle b_k, a_k \rangle \in \text{co} \) in the case of a negative literal), then it must also go downwards on the left-hand side (\( \langle y_{ij}, z_{ij} \rangle \in \text{co} \) to satisfy Prefix. For instance, in the case of a positive literal, note that if \( \langle a_k, b_k \rangle \in \text{co} \), then \( \langle y_{ij}, w_{ij} \rangle \in \text{so} ; \text{co} ; \text{so} \). Therefore, for every commit order \( \text{co} \) such that \( \langle h_\phi, \text{co} \rangle \) satisfies Prefix, \( \langle a_k, b_k \rangle \in \text{co} \) implies \( \langle y_{ij}, z_{ij} \rangle \in \text{co} \). Indeed, if \( \langle a_k, b_k \rangle \in \text{co} \), instantiating the Prefix axiom where \( y_{ij} \) plays the role of \( t_2 \), \( z_{ij} \) plays the role of \( t_1 \), and \( w_{ij} \) plays the role of \( t_3 \), we obtain that \( \langle y_{ij}, z_{ij} \rangle \in \text{co} \).

In contrast, when the \( \text{co} \) goes upwards on the right-hand side (\( \langle b_k, a_k \rangle \in \text{co} \) in the case of a positive literal, and \( \langle a_k, b_k \rangle \in \text{co} \) in the case of a negative literal) then it imposes no constraint on the direction of \( \text{co} \) on the left-hand side. Therefore, any commit order \( \text{co} \) satisfying Prefix that goes upwards on the right-hand side (e.g., \( \langle b_k, a_k \rangle \in \text{co} \) in the case of a positive literal) and downwards on the left-hand side (\( \langle y_{ij}, z_{ij} \rangle \in \text{co} \) in some sub-history (associated to some literal), thereby contradicting Property (1), can be modified into another commit order satisfying Prefix that goes upwards on the left-hand side as well. Formally, let \( \text{co} \) be a commit order such that \( \langle h_\phi, \text{co} \rangle \) satisfies Prefix and

\[
\langle b_k, a_k \rangle \in \text{co} \wedge \langle y_{ij}, z_{ij} \rangle \in \text{co}
\]

for some literal \( \lambda_{ij} = x_k \) (the case of negative literals can be handled in a similar manner). Let \( \text{co}_1 \) be the restriction of \( \text{co} \) on the set of tuples

\[
\{(a_{k'}, b_{k'}) ; (b_{k'}, a_{k'}) | 1 \leq k' \leq n \} \cup \{(y_{i'j'}, z_{i'j'}) ; (z_{i'j'}, y_{i'j'}) \} \text{ for each } i', j' \} \cup \text{so} \cup \text{wr}.
\]

Since \( \text{co}_1 \subseteq \text{co} \), we have that \( \text{co}_1 \) is acyclic. Let \( \text{co}_2 \) be a relation obtained from \( \text{co}_1 \) by flipping the order between \( y_{ij} \) and \( z_{ij} \) (i.e., \( \text{co}_2 = \text{co}_1 \setminus \{(y_{ij}, z_{ij}) \} \cup \{(z_{ij}, y_{ij}) \} \)). This flipping does not introduce any cycle because \( \text{co}_2 \) contains no path ending in \( z_{ij} \) (see Fig 5a). Also, \( \text{co}_2 \) still satisfies the Prefix axiom (since \( \langle b_k, a_k \rangle \in \text{co}_2 \) there is no path from \( y_{ij} \) to \( w_{ij} \) satisfying the constraints in the Prefix axiom). Since \( \text{co}_2 \) is acyclic, it can be extended to a total commit order \( \text{co}_3 \) that satisfies Prefix. This is a consequence of the following lemma whose proof follows easily from definitions (the part of this lemma concerning Serializability will be used later).

**Lemma 3.3.** Let \( \text{co} \) be an acyclic relation that includes \( \text{so} \cup \text{wr} \), \( \langle a_k, b_k \rangle \) or \( \langle b_k, a_k \rangle \), for each \( k \), and \( \langle y_{ij}, z_{ij} \rangle \) or \( \langle z_{ij}, y_{ij} \rangle \), for each \( i, j \). For each axiom \( A \in \{ \text{Prefix}, \text{Serializability} \} \), if \( \langle h_\phi, \text{co} \rangle \) satisfies \( A \), then there exists a total commit order \( \text{co}' \) such that \( \text{co} \subseteq \text{co}' \) and \( \langle h_\phi, \text{co}' \rangle \) satisfies \( A \).

Therefore, \( \langle h_\phi, \text{co}_3 \rangle \) satisfies Prefix, and \( \langle b_k, a_k \rangle \in \text{co}_3 \wedge \langle z_{ij}, y_{ij} \rangle \in \text{co}_3 \) (\( \text{co}_3 \) goes upwards on both sides of a sub-history like in Figure 5a). This transformation can be applied iteratively until obtaining a commit order that satisfies both Prefix and Property (1).
Next, we complete the correctness proof of this reduction. For the “if” direction, if \( h_\varphi \) satisfies PC, then there exists a total commit order co between the transactions described above, which together with \( h_\varphi \) satisfies Prefix. The assignment of the variables \( x_k \) explained above (defined by the co order between \( a_k \) and \( b_k \), for each \( k \)) satisfies the formula \( \varphi \) since there exists no cycle between the transactions \( y_{ij} \) and \( z_{ij} \), which implies that for each clause \( D_i \), there exists a \( j \) such that \( \langle y_{ij}, z_{ij} \rangle \notin \text{co} \) which means that \( \lambda_{ij} \) is satisfied. For the “only-if” direction, let \( y \) be a satisfying assignment for \( \varphi \). Also, let \( \text{co}' \) be a binary relation that includes so and wr such that if \( y(x_k) = \text{false} \), then \( \langle a_k, b_k \rangle \in \text{co}' \) and \( \langle y_{ij}, z_{ij} \rangle \in \text{co}' \) for each \( \lambda_{ij} = x_k \), and \( \langle z_{ij}, y_{ij} \rangle \in \text{co}' \) for each \( \lambda_{ij} = \neg x_k \), and if \( y(x_k) = \text{true} \), then \( \langle y_{ij}, z_{ij} \rangle \in \text{co}' \) for each \( \lambda_{ij} = x_k \), and \( \langle y_{ij}, z_{ij} \rangle \in \text{co}' \) for each \( \lambda_{ij} = \neg x_k \). Note that \( \text{co}' \) is acyclic: no cycle can contain \( w_{ij} \) because \( w_{ij} \) has no “outgoing” dependency (i.e., \( \text{co}' \) contains no pair with \( w_{ij} \) as a first component), there is no cycle including some pair of transactions \( a_k, b_k \) and some pair \( y_{ij}, z_{ij} \) because there is no way to reach \( y_{ij} \) or \( z_{ij} \) from \( a_k \) or \( b_k \), there is no cycle including only transactions \( a_k \) and \( b_k \) because \( a_k \) and \( b_k \) are not related to \( a_{k'} \) and \( b_{k'} \), for \( k_1 \neq k_2 \), there is no cycle including transactions \( y_{i_{k_1}, j_1}, z_{i_{k_2}, j_2} \) and \( y_{i_{k_2}, h}, z_{i_{k_1}, h} \), for \( i_1 \neq i_2 \) since these are disconnected as well, and finally, there is no cycle including only transactions \( y_{ij} \) and \( z_{ij} \), for a fixed \( i \), because \( \varphi \) is satisfiable. By Lemma 3.3, the acyclic relation \( \text{co}' \) can be extended to a total commit order co which together with \( h_\varphi \) satisfies the Serializability axiom. Therefore, \( h_\varphi \) satisfies SER.

4 CHECKING CONSISTENCY OF BOUNDED-WIDTH HISTORIES

In this section, we show that checking prefix consistency, snapshot isolation, and serializability becomes polynomial time under the assumption that the width of the given history, i.e., the maximum number of mutually-unordered transactions w.r.t. the session order, is bounded by a fixed constant. If we consider the standard case where the session order is a union of transaction sequences (modulo the fictitious transaction writing the initial values), i.e., a set of sessions, then the width of the history is the number of sessions. We start by presenting an algorithm for checking serializability which is polynomial time when the width is bounded by a fixed constant. In general, the asymptotic complexity of this algorithm is exponential in the width of the history, but this worst-case behavior is not exercised in practice as shown in Section 6. Then, we prove that checking prefix consistency and snapshot isolation can be reduced in polynomial time to the problem of checking serializability.

4.1 Checking Serializability

We present an algorithm for checking serializability of a given history which constructs a valid commit order (satisfying Serialization), if any, by “linearizing” transactions one by one in an order consistent with the session order. At any time, the set of already linearized transactions is uniquely determined by an antichain of the session order (i.e., a set of mutually-unordered transactions w.r.t. so), and the next transaction to linearize is chosen among the immediate so successors of the transactions in this antichain. The crux of the algorithm is that the next transaction to linearize can be chosen such that it does not produce violations of Serialization in a way that does not depend on the order between the already linearized transactions. Therefore, the algorithm can be seen as a search in the space of so antichains. If the width of the history is bounded (by a fixed constant), then the number of possible so antichains is polynomial in the size of the history, which implies that the search can be done in polynomial time.

A prefix of a history \( h = (T, \text{so}, \text{wr}) \) is a set of transactions \( T' \subseteq T \) such that all the so predecessors of transactions in \( T' \) are also in \( T' \), i.e., \( \forall t \in T. so^{-1}(t) \in T \). A prefix \( T' \) is uniquely determined by the set of transactions in \( T' \) which are maximal w.r.t. so. This set of transactions forms an antichain.
so, i.e., any two elements in this set are incomparable w.r.t. so. Given an antichain \( \{t_1, \ldots, t_n\} \) of so, we say that \( \{t_1, \ldots, t_n\} \) is the boundary of the prefix \( T' = \{t : \exists i. \langle t, t_i \rangle \in so \lor t = t_1\} \). For instance, given the history in Figure 6a, the set of transactions \( \{t_0, t_1, t_2\} \) is a prefix with boundary \( \{t_1, t_2\} \) (the latter is an antichain of the session order).

A prefix \( T' \) of a history \( h \) is called serializable iff there exists a partial commit order \( co \) on the transactions in \( h \) such that the following hold:

- \( co \) does not contradict the session order and the write-read relation in \( h \), i.e., \( wr \cup so \cup co \) is acyclic,
- \( co \) is a total order on transactions in \( T' \),
- \( co \) orders transactions in \( T' \) before transactions in \( T \setminus T' \), i.e., \( \langle t_1, t_2 \rangle \in co \) for every \( t_1 \in T' \) and \( t_2 \in T \setminus T' \),
- \( co \) does not order any two transactions \( t_1, t_2 \in T' \)
- the history \( h \) along with the commit order \( co \) satisfies the axiom defining serializability, i.e., \( \langle h, co \rangle \models \text{Serialization} \).

For the history in Figure 6a, the prefix \( \{t_0, t_1, t_2\} \) is serializable since there exists a partial commit order \( co \) which orders \( t_0 \), \( t_1 \), \( t_2 \) in this order, and both \( t_1 \) and \( t_2 \) before \( t_3 \) and \( t_4 \). The axiom Serialization is satisfied trivially, since the prefix contains a single transaction writing \( x \) and all the transactions outside of the prefix do not read \( x \).

A prefix \( T' \uplus \{t\} \) of \( h \) is called a valid extension of a serializable prefix \( T' \) of \( h \), denoted by \( T' \triangleright T' \uplus \{t\} \) if:

- \( t \) does not read from a transaction outside of \( T' \), i.e., for every \( t' \in T \setminus T' \), \( \langle t', t \rangle \notin wr \), and
- for every variable \( x \) written by \( t \), there exists no transaction \( t_2 \neq t \) outside of \( T' \) which reads a value of \( x \) written by a transaction \( t_3 \) in \( T' \), i.e., for every \( x \) written by \( t \) and every \( t_1 \in T' \) and \( t_2 \in T \setminus (T' \uplus \{t\}) \), \( \langle t_1, t_2 \rangle \notin wr \).

For the history in Figure 6a, we have \( \{t_0, t_1\} \triangleright \{t_0, t_1\} \uplus \{t_2\} \) because \( t_2 \) reads from \( t_0 \) and it does not write any variable. On the other hand \( \{t_0, t_1\} \not\triangleright \{t_0, t_1\} \uplus \{t_3\} \) because \( t_3 \) writes \( x \) and the transaction \( t_2 \), outside of this prefix, reads from the transaction \( t_0 \) included in the prefix.

Let \( \triangleright^* \) denote the reflexive and transitive closure of \( \triangleright \).

The following lemma is essential in proving that iterative valid extensions of the initial empty prefix can be used to show that a given history is serializable.

\[ \text{We assume that } t \notin T' \text{ which is implied by the use of the disjoint union } \uplus. \]
We extend co = h, a serializable prefix T’ of h, A set, in global scope, seen of prefixes of h which are not serializable Output: true iff T’ ⊑∗ h

Algorithm 2: The algorithm checkSER for checking serializability

Lemma 4.1. For a serializable prefix T’ of a history h, a prefix T’ ∪ {t} is serializable if it is a valid extension of T’.

Proof. Let co’ be the partial commit order for T’ which satisfies the serializable prefix conditions. We extend co’ to a partial order co = co’ ∪ \{⟨t, t’⟩|t’ ∉ T’ ∪ {t’}\}. We show that ⟨h, co⟩ |= Serialization. The other conditions for T’ ∪ {t} being a serializable prefix are satisfied trivially by co.

Assume by contradiction that ⟨h, co⟩ does not satisfy the axiom Serialization. Then, there exists t₁, t₂, t₃, x ∈ vars(h) s.t. ⟨t₁, t₂⟩ ∈ wrₓ and t₂ writes on x and ⟨t₁, t₂⟩, ⟨t₂, t₃⟩ ∈ co. Since ⟨h, co’⟩ satisfies this axiom, at least one of these two co ordering constraints are of the form ⟨t, t’⟩ where t’ ∉ T’ ∪ {t}:

- the case t₁ = t and t₂ ∉ T’ ∪ {t} is not possible because co’ contains no pair of the form ⟨t’, _⟩ ∈ co’ with t’ ∉ T’ (recall that ⟨t₂, t₃⟩ should be also included in co).
- If t₂ = t then, ⟨t₁, t₂⟩ ∈ co’ and ⟨t₂, t₃⟩ for some t₃ ∉ T’ ∪ {t}. But, by the definition of valid extension, for all variables x written by t, there exists no transaction t₃ ∉ T’ ∪ {t} such that it reads x from t₁ ∈ T’. Therefore, this is also a contradiction.

Algorithm 2 lists our algorithm for checking serializability. It is defined as a recursive procedure that searches for a sequence of valid extensions of a given prefix (initially, this prefix is empty) until covering the whole history. Figure 6b pictures this search on the history in Figure 6a. The right branch (containing blue edges) contains only valid extensions and it reaches a prefix that includes all the transactions in the history.

Theorem 4.2. A history h is serializable iff checkSER(h, ∅, ∅) returns true.

Proof. The “if” direction is a direct consequence of Lemma 4.1. For the reverse, assume that h = ⟨T, so, wr⟩ is serializable with a (total) commit order co. Let coᵢ be the set of transactions in the prefix of co of length i. Since co is consistent with so, we have that coᵢ is a prefix of h, for any i. We show by induction that coᵢ₊₁ is a valid extension of coᵢ. The base case is trivial. For the induction step, let t be the last transaction in the prefix of co of length i + 1. Then,

- t cannot read from a transaction outside of coᵢ because co is consistent with the write-read relation wr,
- also, for every variable x written by t, there exists no transaction t₂ ≠ t outside of coᵢ which reads a value of x written by a transaction t₁ ∈ coᵢ. Otherwise, ⟨t₁, t₂⟩ ∈ wrₓ, ⟨t, t₂⟩ ∈ co, and ⟨t₁, t⟩ ∈ co which implies that ⟨h, co⟩ does not satisfy Serializability.
This implies that checkSER(h, ∅, ∅) returns true.

By definition, the size of each antichain of a history h is smaller than the width of h. Therefore, the number of possible antichains of a history h is \(O(\text{size}(h)^{\text{width}(h)})\) where size(h), resp., width(h), is the number of transactions, resp., the width, of h. Since the valid extension property can be checked in quadratic time, the asymptotic time complexity of the algorithm defined by checkSER is upper bounded by \(O(\text{size}(h)^{\text{width}(h)} \cdot \text{size}(h)^3)\). The following corollary is a direct consequence of this observation.

**Corollary 4.3.** For an arbitrary but fixed constant \(k \in \mathbb{N}\), the problem of checking serializability for histories of width at most \(k\) is polynomial time.

### 4.2 Reducing Prefix Consistency to Serializability

We describe a polynomial time reduction of checking prefix consistency of bounded-width histories that we prove that they are acyclic and that any linearization is serializable. Thus, let checkSER want to check prefix consistency, we define a new history (the history co of the transaction that is serializable while the one corresponding to “lost update” is not serializable. We transform on the two histories in Figure 7a and Figure 7c, which represent typical anomalies known as “long fork” and “lost update”, respectively. The former is not admitted by PC while the latter is allowed. It can be easily seen that the transformed history corresponding to the “long fork” anomaly is not serializable while the one corresponding to “lost update” is serializable. We show that this transformation leads to a history of the same width, which by Corollary 4.3, implies that checking prefix consistency of bounded-width histories is polynomial time.

Thus, given a history \(h = (T, \text{wr}, \text{so})\), we define the history \(h_{R|W} = (T', \text{wr}', \text{so}')\) as follows:

- **T'** contains a transaction \(R_t\), called a *read* transaction, and a transaction \(W_t\), called a *write* transaction, for each transaction \(t\) in the original history, i.e., \(T' = \{R_t | t \in T\} \cup \{W_t | t \in T\}\)
- the write transaction \(W_t\) writes exactly the same set of variables as \(t\), i.e., for each variable \(x\), \(W_t\) writes to \(x\) if \(t\) writes to \(x\).
- the read transaction \(R_t\) reads exactly the same values and the same variables as \(t\), i.e., for each variable \(x, \text{wr}_x' = \{(W_{t_1}, R_{t_2}) | (t_1, t_2) \in \text{wr}_x\}\}
- the session order between the read and the write transactions corresponds to that of the original transactions and read transactions precede their write counterparts, i.e.,

\[
\text{so}' = \{(R_t, W_t) | t \in T\} \cup \{\langle R_{t_1}, R_{t_2}\rangle, \langle R_{t_1}, W_{t_2}\rangle, \langle W_{t_1}, R_{t_2}\rangle, \langle W_{t_1}, W_{t_2}\rangle | (t_1, t_2) \in \text{so}\}
\]

The following lemma is a straightforward consequence of the definitions (see Appendix C).

**Lemma 4.4.** The histories \(h\) and \(h_{R|W}\) have the same width.

Next, we show that \(h_{R|W}\) is serializable if \(h\) is prefix consistent. Formally, we show that

\(\forall co. \exists co'. \langle h, co \rangle \models \text{Prefix} \Rightarrow \langle h_{R|W}, co' \rangle \models \text{Serializability}\)

Thus, let \(co\) be a commit (total) order on transactions of \(h\) which together with \(h\) satisfies the prefix consistency axiom. We define two partial commit orders \(co'_1\) and \(co'_2\), \(co'_2\), \(co'_3\), a strengthening of \(co'_1\), which we prove that they are acyclic and that any linearization \(co'\) of \(co'_2\) is a valid witness for \(h_{R|W}\) satisfying serializability.
Thus, let $\text{co}'_1$ be a partial commit order on transactions of $h_{R\mid W}$ defined as follows:

$$\text{co}'_1 = \{ \langle R_t, W_t \rangle | t \in T \} \cup \{ \langle W_{t_1}, W_{t_2} \rangle | (t_1, t_2) \in \text{co} \} \cup \{ \langle W_{t_1}, R_{t_2} \rangle | (t_1, t_2) \in \text{wr} \cup \text{so} \}$$

We show that if $\text{co}'_1$ were to be cyclic, then it contains a minimal cycle with one read transaction, and at least one but at most two write transactions. Then, we show that such cycles cannot exist.

**Lemma 4.5. The relation $\text{co}'_1$ is acyclic.**

**Proof.** We first show that if $\text{co}'_1$ were to be cyclic, then it contains a minimal cycle with one read transaction, and at least one but at most two write transactions. Then, we show that such cycles cannot exist. Therefore, let us assume that $\text{co}'_1$ is cyclic. Then,

- Since $\langle W_{t_1}, W_{t_2} \rangle \in \text{co}'_1$ implies $\langle t_1, t_2 \rangle \in \text{co}$, for every $t_1$ and $t_2$, a cycle in $\text{co}'_1$ cannot contain only write transactions. Otherwise, it will imply a cycle in the original commit order $\text{co}$. Therefore, a cycle in $\text{co}'_1$ must contain at least one read transaction.

- Assume that a cycle in $\text{co}'_1$ contains two write transactions $W_{t_1}$ and $W_{t_2}$ which are not consecutive, like in Figure 8. Since either $\langle W_{t_1}, W_{t_2} \rangle \in \text{co}'_1$, or $\langle W_{t_1}, W_{t_2} \rangle \in \text{co}'_2$, there exists a smaller cycle in $\text{co}'_1$ where these two write transactions are consecutive.

- If a minimal cycle were to contain three write transactions, then all of them cannot be consecutive unless they all three form a cycle, which is not possible. So a minimal cycle contains at most two write transactions.

- Since $\text{co}'_1$ contains no direct relation between read transactions, it cannot contain a cycle with two consecutive read transactions, or only read transactions.

This shows that a minimal cycle of $\text{co}'_1$ would include a read transaction and a write transaction, and at most one more write transaction. We prove that such cycles are however impossible:

- if the cycle is of size 2, then it contains two transactions $W_{t_1}$ and $R_{t_2}$ such that $\langle W_{t_1}, R_{t_2} \rangle \in \text{co}'_1$ and $\langle R_{t_2}, W_{t_1} \rangle \in \text{co}'_1$. Since all the $\langle R \cdot W \rangle$ dependencies in $\text{co}'_1$ are of the form $\langle R_t, W_t \rangle$, it follows that $t_1 = t_2$. Then, we have $\langle W_{t_1}, R_{t_1} \rangle \in \text{co}'_1$ which implies $\langle t_1, t_1 \rangle \in \text{wr} \cup \text{so}$, a contradiction.
• if the cycle is of size 3, then it contains three transactions \(W_{t_1}, W_{t_2},\) and \(R_{t_3}\) such that \(\langle W_{t_1}, W_{t_2} \rangle \in co^*_1,\) \(\langle W_{t_2}, R_{t_3} \rangle \in co^*_1,\) and \(\langle R_{t_3}, W_{t_1} \rangle \in co^*_1.\) Using a similar argument as in the previous case, \(\langle R_{t_3}, W_{t_1} \rangle \in co^*_1\) implies \(t_3 = t_1.\) Therefore, \(\langle t_1, t_2 \rangle \in co\) and \(\langle t_2, t_1 \rangle \in wr \cup so,\) which contradicts the fact that \(wr \cup so \subseteq co.\)

We define a strengthening of \(co^*_1\) where intuitively, we add all the dependencies from read transactions \(t_3\) to write transactions \(t_2\) that “overwrite” values read by \(t_3.\) Formally, \(co^*_2 = co^*_1 \cup RW(co^*_1)\) where

\[
RW(co^*_1) = \{ \langle t_3, t_2 \rangle | \exists x \in \text{vars}(h). \exists t_1 \in T'. \langle t_1, t_3 \rangle \in wr_x', \langle t_1, t_2 \rangle \in co^*_1, t_2 \text{ writes } x \}.
\]

It can be shown that any cycle in \(co^*_2\) would correspond to a Prefix violation in the original history. Therefore,

**Lemma 4.6.** The relation \(co^*_2\) is acyclic.

**Proof.** Assume that \(co^*_2\) is cyclic. Any minimal cycle in \(co^*_2\) still satisfies the properties of minimal cycles of \(co^*_1\) proved in Lemma 4.5 (because all write transactions are still totally ordered and \(co^*_2\) doesn’t relate directly read transactions). So, a minimal cycle in \(co^*_2\) contains a read transaction and a write transaction, and at most one more write transaction.

Since \(co^*_1\) is acyclic, a cycle in \(co^*_2,\) and in particular a minimal one, must necessarily contain a dependency from \(RW(co^*_1).\) Note that a minimal cycle cannot contain two such dependencies since this would imply that it contains two non-consecutive write transactions. The red edges in Figure 9a show a minimal cycle of \(co^*_2\) satisfying all the properties mentioned above. This cycle contains a dependency \(\langle R_{t_3}, W_{t_2} \rangle \in RW(co^*_1)\) which implies the existence of a write transaction \(W_{t_1}\) in \(h_{R|W}\) s.t. \(\langle W_{t_1}, R_{t_3} \rangle \in wr_x'\) and \(\langle W_{t_1}, W_{t_2} \rangle \in co^*_1\) and \(W_{t_1}, W_{t_2}\) write on \(x\) (these dependencies are represented by the black edges in Figure 9a). The relations between these transactions of \(h_{R|W}\) imply that the corresponding transactions of \(h\) are related as shown in Figure 9b: \(\langle W_{t_1}, W_{t_2} \rangle \in co^*_1\) and \(\langle W_{t_2}, W_{t_3} \rangle \in co^*_1\) imply \(\langle t_1, t_2 \rangle \in co\) and \(\langle t_2, t_3 \rangle \in co^*,\) respectively, \(\langle W_{t_1}, W_{t_2} \rangle \in wr_x'\) implies \(\langle t_1, t_3 \rangle \in wr_x,\) and \(\langle W_{t_1}, R_{t_3} \rangle \in co^*_1\) implies \(\langle t_4, t_3 \rangle \in wr \cup so.\) This implies that \(\langle h, co\rangle\) doesn’t satisfy the Prefix axiom, a contradiction.

**Lemma 4.7.** If a history \(h\) satisfies prefix consistency, then \(h_{R|W}\) is serializable.

**Proof.** Let \(co'\) be any total order consistent with \(co^*_2.\) Assume by contradiction that \(h_{R|W}, co'\) doesn’t satisfy Serializability. Then, there exist \(t'_1, t'_2, t'_3 \in T'\) such that \(\langle t'_1, t'_2 \rangle, \langle t'_2, t'_3 \rangle \in co'\) and \(t'_1, t'_2\) write on some variable \(x\) and \(\langle t'_1, t'_3 \rangle \in wr_x'.\) But then \(t'_1, t'_2\) are write transactions and \(co^*_1\) must contain \(\langle t'_1, t'_2 \rangle.\) Therefore, \(RW(co^*_1)\) and \(co^*_2\) should contain \(\langle t'_1, t'_2 \rangle,\) a contradiction with \(co'\) being consistent with \(co^*_2.\)

Finally, it can be proved that any linearization \(co'\) of \(co^*_2\) satisfies Serializability (together with \(h_{R|W}\)). Moreover, it can also be shown that the serializability of \(h_{R|W}\) implies that \(h\) satisfies PC. Therefore,

**Theorem 4.8.** A history \(h\) satisfies prefix consistency iff \(h_{R|W}\) is serializable.

**Proof.** The “only-if” direction is proven by Lemma 4.7. For the reverse, we show that \(\forall co'. \exists co. \langle h_{R|W}, co' \rangle \models \text{Serializability} \Rightarrow \langle h, co \rangle \models \text{Prefix}\)
Thus, let $\text{co}'$ be a commit (total) order on transactions of $h_{R|W}$ which together with $h_{R|W}$ satisfies the serializability axiom. Let $\text{co}$ be a commit order on transactions of $h$ defined by $\text{co} = \{(t_1, t_2) | \langle W_{t_1}, W_{t_2} \rangle \in \text{co}' \}$ ($\text{co}$ is clearly a total order). If $\text{co}$ were not to be consistent with $\text{wr} \cup \text{so}$, then there would exist transactions $t_1$ and $t_2$ such that $\langle t_1, t_2 \rangle \in \text{wr} \cup \text{so}$ and $\langle t_2, t_1 \rangle \in \text{co}$, which would imply that $\langle W_{t_1}, R_{t_2} \rangle, \langle R_{t_2}, W_{t_1} \rangle \in \text{wr} \cup \text{so}$ and $\langle W_{t_2}, W_{t_1} \rangle \in \text{co}'$, which violates the acyclicity of $\text{co}'$. We show that $\langle h, \text{co} \rangle$ satisfies Prefix. Assume by contradiction that there exists a Prefix violation between $t_1, t_2, t_3, t_4$ (shown in Figure 10a), i.e., for some $x \in \text{vars}(h)$, $\langle t_1, t_3 \rangle \in \text{wr}_x$ and $t_2$ writes $x$, $\langle t_1, t_2 \rangle \in \text{co}$, $\langle t_2, t_4 \rangle \in \text{co}'$ and $\langle t_4, t_3 \rangle \in \text{wr} \cup \text{so}$. Then, the corresponding transactions $W_{t_1}, W_{t_2}, W_{t_3}, R_{t_3}$ in $h_{R|W}$ would be related as follows: $\langle W_{t_1}, W_{t_2} \rangle \in \text{co}'$ and $\langle W_{t_1}, R_{t_3} \rangle \in \text{wr}_x'$ because $\langle t_1, t_3 \rangle \in \text{wr}_x$ and $\langle t_1, t_2 \rangle \in \text{co}$. Since $\text{co}'$ satisfies Serializability, then $\langle R_{t_1}, W_{t_2} \rangle \in \text{co}'$. But $\langle t_2, t_4 \rangle \in \text{co}'$ and $\langle t_4, t_3 \rangle \in \text{wr} \cup \text{so}$ imply that $\langle W_{t_2}, W_{t_1} \rangle \in \text{co}''$ and $\langle W_{t_4}, R_{t_3} \rangle \in \text{wr}' \cup \text{so}'$, which show that $\text{co}'$ is cyclic (the red cycle in Figure 10b), a contradiction.

Since the history $h_{R|W}$ can be constructed in linear time, Lemma 4.4, Theorem 4.8, and Corollary 4.3 imply the following result.

**Corollary 4.9.** For an arbitrary but fixed constant $k \in \mathbb{N}$, the problem of checking prefix consistency for histories of width at most $k$ is polynomial time.

### 4.3 Reducing Snapshot Isolation to Serializability

We extend the reduction of prefix consistency to serializability to the case of snapshot isolation. Compared to prefix consistency, snapshot isolation disallows transactions that read the same snapshot of the database to commit together if they write on a common variable (stated by the Conflict axiom). More precisely, for any pair of transactions $t_1$ and $t_2$ writing to a common variable, $t_1$ must observe the effects of $t_2$ or vice-versa. We refine the definition of $h_{R|W}$ such that any “serialization” (i.e., commit order satisfying Serializability) disallows that the read transactions corresponding to such two transactions are ordered both before their write counterparts. We do this by introducing auxiliary variables that are read or written by these transactions. For instance, Figure 11 shows this transformation on the two histories in Figure 11a and Figure 11c, which represent the anomalies known as “lost update” and “write skew”, respectively. The former is not admitted by SI while the latter is admitted. Concerning “lost update”, the read counterpart of the transaction on the left writes to a variable $x12$ which is read by its write counterpart, but also written by the write counterpart of the other transaction. This forbids that the latter is serial in between the read and write counterparts of the transaction on the left. A similar scenario is imposed on the transaction on the right, which makes that the transformed history is not serializable. Concerning the “write skew” anomaly, the transformed history is exactly as for the PC reduction since the two transactions don’t write on a common variable. It is clearly serializable.

For a history $h = \langle T, \text{wr}, \text{so} \rangle$, the history $h_{R|W}^c = \langle T', \text{wr}', \text{so}' \rangle$ is defined as $h_{R|W}$ with the following additional construction: for every two transactions $t_1$ and $t_2 \in T$ that write on a common variable,

- $R_{t_1}$ and $W_{t_2}$ (resp., $R_{t_2}$ and $W_{t_1}$) write on a variable $x_{1,2}$ (resp., $x_{2,1}$),
- the write transaction of $t_i$ reads $x_{i,j}$ from the read transaction of $t_i$, for all $i \neq j \in \{1, 2\}$, i.e., $\text{wr}_{x_{1,2}} = \{(R_{t_1}, W_{t_2})\}$ and $\text{wr}_{x_{2,1}} = \{(R_{t_2}, W_{t_1})\}$.
On the Complexity of Checking Transactional Consistency

Fig. 11. Reducing SI to SER.

Note that \( h_{R \mid W} \) and \( h^c_{R \mid W} \) have the same width (the session order is defined exactly in the same way), which implies, by Lemma 4.4, that \( h \) and \( h^c_{R \mid W} \) have the same width.

The following result can be proved using similar reasoning as in the case of prefix consistency (see Appendix D).

**Theorem 4.10.** A history \( h \) satisfies snapshot isolation iff \( h^c_{R \mid W} \) is serializable.

Note that \( h^c_{R \mid W} \) and \( h \) have the same width, and that \( h^c_{R \mid W} \) can be constructed in linear time. Therefore, Theorem 4.10, and Corollary 4.3 imply the following result.

**Corollary 4.11.** For an arbitrary but fixed constant \( k \in \mathbb{N} \), the problem of checking snapshot isolation for histories of width at most \( k \) is polynomial time.

### 5 Communication Graphs

In this section, we present an extension of the polynomial time results for PC, SI, and SER, which allows to handle histories where the sharing of variables between different sessions is sparse. For the results in this section, we take the simplifying assumption that the session order is a union of transaction sequences (modulo the fictitious transaction writing the initial values), i.e., each transaction sequence corresponding to the standard notion of session 9. We represent the sharing of variables between different sessions using an undirected graph called a communication graph.

For instance, the communication graph of the history in Figure 12a is given in Figure 12b. For readability, the edges are marked with the variables accessed by the two sessions.

We show that the problem of checking PC, SI, or SER is polynomial time when the size of every biconnected component of the communication graph is bounded by a fixed constant. This is stronger than the results in Section 4 because the number of biconnected components can be arbitrarily large which means that the total number of sessions is unbounded. In general, we prove that the time complexity of these consistency criteria is exponential only in the maximum size of such a biconnected component, and not the whole number of sessions.

An undirected graph is biconnected if it is connected and if any one vertex were to be removed, the graph will remain connected, and a biconnected component of a graph \( G \) is a maximal biconnected subgraph of \( G \). Figure 12b shows the decomposition in biconnected components of a communication graph. This graph contains 5 sessions while every biconnected component is of size at most 3. Intuitively, any potential cycle in the commit order associated to a history will contain a cycle that passes only through sessions in the same biconnected component. Therefore, checking any of these criteria can be done in isolation for each biconnected component (more precisely, on sub-histories that contain only sessions in the same biconnected component). Actually, this decomposition argument works even for RC, RA, and CC. For instance, in the case of the history in Figure 12a, any consistency criterion can be checked looking in isolation at three sub-histories: a sub-history with \( S_1 \) and \( S_2 \), a sub-history with \( S_2, S_3, \) and \( S_4 \), and a sub-history with \( S_4 \) and \( S_5 \).

9The results can be extended to arbitrary session orders by considering maximal transaction sequences in session order instead of sessions.
Formally, a communication graph of a history \( h \) is an undirected graph \( \text{Comm}(h) = (V, E) \) where the set of vertices \( V \) is the set of sessions in \( h \), and \((v, v') \in E\) iff the sessions \( v \) and \( v' \) contain two transactions \( t_1 \) and \( t_2 \), respectively, such that \( t_1 \) and \( t_2 \) read or write a common variable \( x \).

**Lemma 5.1.** Let \( C_1, \ldots, C_n \) be the biconnected components of \( \text{Comm}(h) \) for a history \( h = \langle T, \text{wr}, \text{so} \rangle \). Let \( P_A \) be a path of the form of type A connecting two transactions of \( C_i \). Then, there is a path \( P_B \) of the form of type B connecting the same two transactions and \( P_B \) never leaves \( C_i \).

**Proof.** Type A and B are both of the form \( \text{co}^+ \). Consider a minimal path \( \pi = t_0, \ldots, t_n \in \bigcup_j \text{co}_j \) between two transactions \( t_0 \) and \( t_n \) of the same biconnected component \( C \) of \( \text{Comm}(h) \) (i.e., from sessions in \( C \)). We define a path \( \pi_z = v_0, \ldots, v_m \) between sessions, i.e., vertices of \( \text{Comm}(h) \), which contains an edge \((v_j, v_{j+1})\) iff \( \pi \) contains an edge \((t_i, t_{i+1})\) with \( t_i \) a transaction of session \( v_j \) and \( t_{i+1} \) a transaction of session \( v_{j+1} \neq v_j \). Since any graph decomposes to a forest of biconnected components, this path must necessarily leave and enter some biconnected component \( C_1 \) to and from the same biconnected component \( C_2 \), i.e., \( \pi_z \) must contain two vertices \( v_{j_1} \) and \( v_{j_2} \) in \( C_1 \) such that the successor \( v_{j_1+1} \) of \( v_{j_1} \) and the predecessor \( v_{j_2-1} \) of \( v_{j_2} \) are from \( C_2 \). Let \( t_1, t_2, t_3, t_4 \) be the transactions in the path \( \pi \) corresponding to \( v_{j_1}, v_{j_2}, v_{j_1+1}, \) and \( v_{j_2-1}, \) respectively. Now, since any two biconnected components share at most one vertex, it follows that \( t_3 \) and \( t_4 \) are from the same session and

- if \( \langle t_3, t_4 \rangle \in \text{so} \), then there exists a smaller path between \( t_0 \) and \( t_1 \) that uses the so relation between \( \langle t_3, t_4 \rangle \) (we recall that so \( \subseteq \bigcup_j \text{co}_j \)) instead of the transactions in \( C_2 \), pictured in Figure 13a, which is a contradiction to the minimality of \( \pi \),

- if \( \langle t_4, t_3 \rangle \notin \text{so} \), there is a cycle in \( \bigcup_j \text{co}_j \cup \text{so} \), pictured in Figure 13b, which is also a contradiction.

Type A and B are of the form \((\text{wr} \cup \text{so})^+\). “shortening” a bigger \((\text{wr} \cup \text{so})^+\) path (they are also a path in \( \text{co}^+ \) since \((\text{wr} \cup \text{so})^+ \subseteq \text{co} \)) will introduce only so dependencies. So a minimal \((\text{wr} \cup \text{so})^+\) never leaves a bicomponent.

Type A and B are of the form \( \text{co}^+ \); \( \text{wr} \cup \text{so} \). Similar to last the case, “shortening” a bigger path will introduce only so dependencies. If the new so is at the end of the path then the new path is still of the form \( \text{co}^+ \); \( \text{wr} \cup \text{so} \). Else, we can replace so with co to make a path of the form \( \text{co}^+ \); \( \text{wr} \cup \text{so} \). So a minimal \( \text{co}^+ \); \( \text{wr} \cup \text{so} \) never leaves a bicomponent.

Type A is of the form \( \text{co}^+ \); co where the last co dependency is between two transactions writing on same variable and type B is of the same form of type A or \( \text{co}^+ \); so. Similar to the previous cases, “shortening” a bigger path will introduce only so dependencies. If the new so is at the end, then it

---

\(^{10}\)The transaction writing the initial values is considered as a distinguished session.

\(^{11}\)That is, transactions that are included in the sessions in \( C_i \).

---
becomes of the form of $co^*; so$. Else, we can replace $so$ with $co$ to make a path of the form $co^*; co$ where the last $co$ dependency is the one from the original path. So a minimal path of type $A$ never leaves a bicomponent or it can be “shortened” to a minimal path of the form $co^*; so$ which never leaves a bicomponent.

For a history $h = (T, so, wr)$ and biconnected component $C$ of $Comm(h)$, the projection of $h$ over transactions in sessions of $C$ is denoted by $h \downarrow C$, i.e., $h \downarrow C = (T', so', wr')$ where $T'$ is the set of transactions in sessions of $C$, $so'$ and $wr'$ are the projections of $so$ and $wr$, respectively, on $T'$.

**Theorem 5.2.** For any criterion $X \in \{RA, RC, CC, PC, SI, SER\}$, a history $h$ satisfies $X$ iff for every biconnected component $C$ of $Comm(h)$, $h \downarrow C$ satisfies $X$.

**Proof.** The “only-if” direction is obvious. For the “if” direction, let $C_1, \ldots, C_n$ be the biconnected components of $Comm(h)$. Also, let $co_j$ be the commit order that witnesses that $h \downarrow C_j$ satisfies $X$, for each $1 \leq i \leq n$. The union $\bigcup_j co_j$ is acyclic since otherwise, any minimal cycle would be a minimal path between transactions of the same biconnected component $C_j$, and, by Lemma 5.1, it will include only transactions of $C_j$ which is a contradiction to $co_j$ being a total order. We show that any linearization $co$ of $\bigcup_j co_j$ along with $h$ satisfies the axioms of $X$, for every consistency model $X$.

The axioms defining $RA$, $RC$, $CC$, $PC$, and $SER$ involve transactions that write or read a common variable, which implies that they belong to the same biconnected component. For $CC$, resp., $PC$, $SER$ using the result from Lemma 5.1, a minimal $(wr \cup so)^+$, resp., $co^*;(wr \cup so)^+$, $co$ path from $t_2$ to $t_3$ in Figure 2c, resp., Figure 2d, Figure 2f will include transactions in the same biconnected component as $t_2$ and $t_3$, since “shortening” a bigger path will introduce only $so$ dependencies. Therefore, they must be satisfied by $co$.

For $SI$, it’s only necessary to discuss the axiom $Conflict$ (the satisfaction of Prefix is proved as for $PC$). Following Figure 2e and Lemma 5.1, any $co^*; co$ path connecting $t_2$ and $t_3$ where the last $co$ dependency is between two transactions writing on same variables, has either a minimal path of the same form that never leaves the same bicomponent as $t_2$, $t_3$, or a minimal path of the form $co^*; so$. Since the bicomponent satisfies $SI$ or particularly Prefix and $Conflict$, for all possible $t_1$, $t_1, t_2, t_3$, it must satisfy $Conflict$. Note that $t_3$ cannot be the first transaction in its session because a path from $t_2$ to $t_3$ passing through $t_4$ (which belongs to a different biconnected component) will necessarily have to pass twice through $t_3$ which would imply that $co$ is cyclic. Thus, $Conflict$ must be satisfied by $co$.

Since the decomposition of a graph into biconnected components can be done in linear time, Theorem 5.2 implies that any of the criteria $PC$, $SI$, or $SER$ can be checked in time $O(size(h)^{bi-size(h)} \cdot size(h)^3 \cdot bi-nb(h))$ where $bi-size(h)$ and $bi-nb(h)$ are the maximum size of a biconnected component in $Comm(h)$ and the number of biconnected components of $Comm(h)$, respectively. The following corollary is a direct consequence of this observation.

**Corollary 5.3.** For an arbitrary but fixed constant $k \in \mathbb{N}$ and any criterion $X \in \{PC, SI, SER\}$, the problem of checking if a history $h$ satisfies $X$ is polynomial time, provided that the size of every biconnected component of $Comm(h)$ is bounded by $k$.

**6 EXPERIMENTAL EVALUATION**

To demonstrate the practical value of the theory developed in the previous sections, we argue that our algorithms:

- are efficient and scalable, and they outperform a SAT encoding of the axioms in Section 2,
- enable an effective testing framework allowing to expose consistency violations in production databases.
The SAT encoding we considered is based on the axioms we presented on this paper. We represent each binary relation with a propositional variable and encode the axioms using clauses to create a 3-SAT formula, which is passed to a SAT solver.

For each ordered pair of transactions $t_1, t_2$ we add two propositional variables representing $\langle t_1, t_2 \rangle \in (\text{wr} \cup \text{so})^+$ and $\langle t_1, t_2 \rangle \in \text{co}$, respectively. Then we generate clauses corresponding to:

- Singleton clauses defining the relation $\text{wr} \cup \text{so}$ (extracted from the input history),
- $\langle t_1, t_2 \rangle \in \text{wr} \cup \text{so}$ implies $\langle t_1, t_2 \rangle \in \text{co}$.
- $\text{co}$ being a total order.
- The axioms corresponding to the considered consistency model.

This is an optimization that does not encode $\text{wr}$ and $\text{so}$ separately, which is sound because of the shape of our axioms (and because these relations are fixed apriori).

As for the implementation of our algorithms, we used standard programming optimizations, e.g., efficient data structures, to avoid unnecessary runtime and memory usage. Few examples include:

- using efficient hashsets for searching in a set,
- grouping transactions which access the same variable (because our algorithms usually iterate over transactions accessing the same variable).
- reducing PCSI to SER on-the-fly while traversing the history.

We focus on three of the criteria introduced in Section 2: serializability which is NP-complete in general and polynomial time when the number of sessions is considered to be a constant, snapshot isolation which can be reduced in linear time on-the-fly to serializability, and causal consistency which is polynomial-time in general\textsuperscript{12}. As benchmark, we consider histories extracted from three distributed databases: CockroachDB [3], Galera [5], and AntidoteDB [8]. Following the approach

\textsuperscript{12}Our implementation is publicly available. URL omitted to maintain anonymity.
in Jepsen [1], histories are generated with random clients. For the experiments described hereafter, the randomization process is parametrized by: (1) the number of sessions ($#\text{sess}$), (2) the number of transactions per session ($#\text{trs}$), (3) the number of operations per transaction ($#\text{ops}$), and (4) an upper bound on the number of used variables ($#\text{vars}$). For any valuation of these parameters, half of the histories generated with CockroachDB and Galera are restricted such that the sets of variables written by any two sessions are disjoint (the sets of read variables are not constrained). This restriction is used to increase the frequency of valid histories.

In a first experiment, we investigated the efficiency of our serializability checking algorithm (Section 4.1) and we compared its performance with a direct SAT encoding of the serializability definition in Section 2 (we used MiniSAT [16] to solve the SAT queries). We used histories extracted from CockroachDB which claims to implement serializability, acknowledging however the possibility of anomalies [4]. The sessions of a history are uniformly distributed among 3 nodes of a single cluster. To evaluate scalability, we fix a reference set of parameter values: $#\text{sess}=6$, $#\text{trs}=30$, $#\text{ops}=20$, and $#\text{vars} = 60 \times #\text{sess}$, and vary only one parameter at a time. For instance, the number of sessions varies from 3 to 15 in increments of 3. We consider 100 histories for each combination of parameter values. The experimental data is reported in Figure 14. Our algorithm scales well even when increasing the number of sessions, which is not guaranteed by its worst-case complexity (in general, this is exponential in the number of sessions). Also, our algorithm is at least two orders of magnitude more efficient than the SAT encoding. We have fixed a 10 minutes timeout, a limit of 10GB of memory, and a limit of 10GB on the files containing the formulas to be passed to the SAT solver. The blue dots represent resource exhausted instances. The SAT encoding reaches the file limit for 148 out of 200 histories with at least 12 sessions (Figure 14a) and for 50 out of 100 histories with 60 transactions per session (Figure 14b), the other parameters being fixed as explained above.

We have found a large number of violations, whose frequency increases with the number of sessions, transactions per session, or operations per transaction, and decreases when allowing more variables. This is expected since increasing any of the former parameters increases the chance of interference between different transactions while increasing the latter has the opposite effect. The second and third column of Table 2 give a more precise account of the kind of violations we found by identifying for each criterion X, the number of histories which violate X but no other criterion weaker than X, e.g., there is only one violation to SI which satisfies PC.

The second experiment measures the scalability of the SI checking algorithm obtained by applying the reduction to SER described in Section 4.3 followed by the SER checking algorithm in Section 4.1, and its performance compared to a SAT encoding of SI. We focus on its behavior when increasing the number of sessions (varying the other parameters leads to similar results). As benchmark, we used the same CockroachDB histories as in Figure 14a and a number of histories extracted

\[13\text{We ensure that every value is written at most once.}\]
from Galera\textsuperscript{14} whose documentation contains contradicting claims about whether it implements snapshot isolation \cite{6,7}. We use 100 histories per combination of parameter values as in the previous experiment. The results are reported in Figure 15a and Figure 15b. We observe the same behavior as in the case of SER. In particular, the SAT encoding reaches the file limit for 150 out of 200 histories with at least 12 sessions in the case of the CockroachDB histories, and for 162 out of 300 histories with at least 9 sessions in the case of the Galera histories. The last two columns in Table 2 classify the set of violations depending on the weakest criterion that they violate.

We also evaluated the performance of the CC checking algorithm in Section 3 when increasing the number of sessions, on histories extracted from AntidoteDB, which claims to implement causal consistency \cite{9}. The results are reported in Figure 15c. In this case, the SAT encoding reaches the file limit for 150 out of 300 histories with at least 9 sessions. All the histories considered in this experiment are valid. However, when experimenting with other parameter values, we have found several violations. The smallest parameter values for which we found violations were 3 sessions, 14 transactions per session, 14 operations per transaction, and 5 variables. The violations we found are also violations of Read Atomic. For instance, one of the violations contains two transactions \(t_1\) and \(t_2\), each of them writing to two variables \(x_1\) and \(x_2\), and another transaction \(t_3\) which reads \(x_1\) from \(t_1\) and \(x_2\) from \(t_2\) (\(t_1\) and \(t_2\) are from different sessions while \(t_3\) is an \textit{so} successor of \(t_1\) in the same session). These violations are novel and they were confirmed by the developers of AntidoteDB.

The refinement of the algorithms above based on communication graphs, described in Section 5, did not have a significant impact on their performance. The histories we generated contained few biconnected components (many histories contained just a single biconnected component) which we believe is due to our proof of concept deployment of these databases on a single machine that did not allow to experiment with very large number of sessions and variables.

### 7 RELATED WORK

Cerone et al. \cite{14} give the first formalization of the criteria we consider in this paper, using the specification methodology of Burckhardt et al. \cite{12}. This formalization uses two auxiliary relations, a \textit{visibility} relation which represents the fact that a transaction “observes” the effects of another transaction and a \textit{commit order}, also called arbitration order, like in our case. Executions are abstracted using a notion of history that includes only a session order and the adherence to some consistency criterion is defined as the existence of a \textit{visibility} relation and a \textit{commit order} satisfying certain axioms. Motivated by practical goals, our histories include a write-read relation, which

\textsuperscript{14}In order to increase the frequency of valid histories, all sessions are executed on a single node.
enables more uniform and in our opinion, more intuitive, axioms to characterize consistency criteria. Moreover, Cerone et al. [14] do not investigate algorithmic issues as in our paper.

Papadimitriou [23] showed that checking serializability of an execution is NP-complete. Moreover, it identifies a stronger criterion called conflict serializability which is polynomial time checkable. Conflict serializability assumes that histories are given as sequences of operations and requires that the commit order be consistent with a conflict-order between transactions defined based on this sequence (roughly, a transaction $t_1$ is before a transaction $t_2$ in the conflict order if it accesses some variable $x$ before $t_2$ does). This result is not applicable to distributed databases where deriving such a sequence between operations submitted to different nodes in a network is impossible.

Bouajjani et al. [11] showed that checking several variations of causal consistency on executions of a non-transactional distributed database is polynomial time (they also assume that every value is written at most once). Assuming singleton transactions, our notion of CC corresponds to the causal convergence criterion in Bouajjani et al. [11]. Therefore, our result concerning CC can be seen as an extension of this result concerning causal convergence to transactions.

There are some works that investigated the problem of checking consistency criteria like sequential consistency and linearizability in the case of shared-memory systems. Gibbons and Korach [19] showed that checking linearizability of the single-value register type is NP-complete in general, but polynomial time for executions where every value is written at most once. Using a reduction from serializability, they showed that checking sequential consistency is NP-complete even when every value is written at most once. Emmi and Enea [17] extended the result concerning linearizability to a series of abstract data types called collections, that includes stacks, queues, key-value maps, etc.

The notion of communication graph is inspired by the work of Chalupa et al. [15] which investigates partial-order reduction (POR) techniques for multi-threaded programs. In general, the goal of partial-order reduction [18] is to avoid exploring executions which are equivalent w.r.t. some suitable notion of equivalence, e.g., Mazurkiewicz trace equivalence [21]. They use the acyclicity of communication graphs to define a class of programs for which their POR technique is optimal. The algorithmic issues they explore are different than ours and they don’t investigate biconnected components of this graph as in our results.

8 CONCLUSIONS

Our results provide an effective means of checking the correctness of transactional databases with respect to a wide range of consistency criteria, in an efficient way. We devise a new specification framework for these criteria, which besides enabling efficient verification algorithms, provide a novel understanding of the differences between them in terms of set of transactions that must be committed before a transaction which is read during the execution. These algorithms are shown to be scalable and orders of magnitude more efficient than standard SAT encodings of these criteria (as defined in our framework). While the algorithms are quite simple to understand and implement, the proof of their correctness is non-trivial and benefits heavily from the new specification framework.

One important venue for future work is identifying root causes for a given violation. The fact that we are able to deal with a wide range of criteria is already helpful in identifying the weakest criterion that is violated in a given execution. Then, in the case of RC, RA, and CC, where inconsistencies correspond to cycles in the commit order, the root cause could be attributed to a minimal cycle in this relation. We did this in our communication with the Antidote developers to simplify the violation we found which contained 42 transactions. In the case of PC, SI, and SER, it could be possible to implement a search procedure similar to CDCL in SAT solvers, in order to compute the root-cause as a SAT solver would compute an unsatisfiability core.
[24] Douglas B. Terry, Alan J. Demers, Karin Petersen, Mike Spreitzer, Marvin Theimer, and Brent B. Welch. 1994. Session Guarantees for Weakly Consistent Replicated Data. In Proceedings of the Third International Conference on Parallel and Distributed Information Systems (PDIS 94), Austin, Texas, USA, September 28-30, 1994. IEEE Computer Society, 140–149. https://doi.org/10.1109/PDIS.1994.331722

[25] Pierre Wolper. 1986. 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. ACM Press, 184–193. https://doi.org/10.1145/512644.512661
A PROOFS OF SECTION 2

Lemma A.1. Let \( h = \langle T, so, wr \rangle \) be a history. If \( \langle h, co \rangle \) satisfies Read Atomic, then for every transaction \( t \) and two reads \( read_t(x, v_1), read_t(x, v_2) \in \text{reads}(t) \), \( \text{wr}^{-1}(read_t(x, v_1)) = \text{wr}^{-1}(read_t(x, v_2)) \) and \( v_1 = v_2 \).

Proof. Let \( \langle t_1, read_t(x, v_1) \rangle, \langle t_2, read_t(x, v_2) \rangle \in \text{wr}_x \). Then \( t_1, t_2 \) write to \( x \). Let us assume by contradiction, that \( t_1 \neq t_2 \). By Read Atomic, \( \langle t_2, t_1 \rangle \in \text{co} \) because \( \langle t_1, read_t(x, v_1) \rangle \in \text{wr}_x \) and \( t_2 \) writes to \( x \). Similarly, we can also show that \( \langle t_1, t_2 \rangle \in \text{co} \), which contradicts the fact that \( \text{co} \) is a strict total order. Therefore, \( t_1 = t_2 \). We also have that \( v_1 = v_2 \) because each transaction contains a single write to \( x \).

Lemma A.2. The following entailments hold:

\[
\text{Causal} \Rightarrow \text{Read Atomic} \Rightarrow \text{Read Committed} \\
\text{Prefix} \Rightarrow \text{Causal} \\
\text{Serializability} \Rightarrow \text{Prefix} \lor \text{Conflict}
\]

Proof. We will show the contrapositive of each implication:

- If \( \langle h, co \rangle \) does not satisfy Read Committed, then
  \[\exists x, \exists t_1, t_2, \exists \alpha, \beta. \langle t_1, \alpha \rangle \in \text{wr}_x \land t_2 \text{ writes } x \land \langle t_2, \beta \rangle \in \text{wr} \land \langle \beta, \alpha \rangle \in \text{po} \land \langle t_1, t_2 \rangle \in \text{co}.\]

  Let \( t_3 \) the transaction containing \( \alpha \) and \( \beta \). We have that \( \langle t_2, t_3 \rangle \in \text{wr} \). But then we have \( t_1, t_2, t_3 \) such that \( \langle t_1, t_3 \rangle \in \text{wr}_x \) and \( \langle t_2, t_3 \rangle \in \text{wr} \) and \( t_2 \) writes \( x \). So by Read Atomic, \( \langle t_2, t_1 \rangle \in \text{co} \). This contradicts the fact that \( \text{co} \) is a strict total order. Therefore, \( \langle h, co \rangle \) does not satisfy Read Atomic.

- If \( \langle h, co \rangle \) does not satisfy Read Atomic, then
  \[\exists x, \exists t_1, t_2, t_3. \langle t_1, t_3 \rangle \in \text{wr}_x \land t_2 \text{ writes } x \land \langle t_2, t_3 \rangle \in \text{wr} \cup \text{so} \land \langle t_1, t_2 \rangle \in \text{co}.\]

  Then \( \langle t_2, t_3 \rangle \in (\text{wr} \cup \text{so})^+ \). Then, by Causal, we have \( \langle t_2, t_1 \rangle \in \text{co} \), which contradicts the fact that \( \text{co} \) is a strict total order. Therefore, \( \langle h, co \rangle \) does not satisfy Causal.

- If \( \langle h, co \rangle \) does not satisfy Causal, then
  \[\exists x, \exists t_1, t_2, t_3. \langle t_1, t_3 \rangle \in \text{wr}_x \land t_2 \text{ writes } x \land \langle t_2, t_3 \rangle \in (\text{wr} \cup \text{so})^+ \land \langle t_1, t_2 \rangle \in \text{co}.\]

  But, \((\text{wr} \cup \text{so})^+ = (\text{wr} \cup \text{so})^* : (\text{wr} \cup \text{so})^* : (\text{wr} \cup \text{so})^*\). Therefore, \( \langle t_2, t_3 \rangle \in \text{co}^* : (\text{wr} \cup \text{so})^* \). Then, by Prefix, we have \( \langle t_2, t_1 \rangle \in \text{co} \), which contradicts the fact that \( \text{co} \) is a strict total order. Therefore, \( \langle h, co \rangle \) does not satisfy Prefix.

- If \( \langle h, co \rangle \) does not satisfy Prefix or Conflict, then
  \[\exists x, \exists t_1, t_2, t_3, t_4. \langle t_1, t_3 \rangle \in \text{wr}_x \land t_2 \text{ writes } x \land \langle t_2, t_4 \rangle \in \text{co}^* \land \langle t_1, t_2 \rangle \in \text{co}\]

  and
  \[- \langle t_4, t_3 \rangle \in \text{co} \land t_3 \text{ writes } y \land t_5 \text{ writes } y \text{ if it violates Conflict.}\]
  \[- \langle t_4, t_3 \rangle \in (\text{wr} \cup \text{so}) \text{ if it violates Prefix.}\]

  In both cases, we have that \( \langle t_4, t_3 \rangle \in \text{co} \). Because \( \text{co} \) is transitive, \( \langle t_2, t_4 \rangle \in \text{co}^* \) and \( \langle t_4, t_3 \rangle \in \text{co} \) imply that \( \langle t_2, t_3 \rangle \in \text{co} \). Then by Serializability, we have \( \langle t_2, t_1 \rangle \in \text{co} \), which contradicts the fact that \( \text{co} \) is a strict total order. Therefore, \( \langle h, co \rangle \) does not satisfy Serializability.

\[\square\]
On the Complexity of Checking Transactional Consistency 29

Algorithm 3: Checking Read Committed

Input: A history $h = \langle T, so, wr \rangle$
Output: true iff $h$ satisfies causal consistency

1. if $so \cup wr$ is cyclic then
2. return false;
3. $co \leftarrow so \cup wr$;
4. foreach $x \in \text{vars}(h)$ do
5. foreach $t_1 \neq t_2 \in T$ s.t. $t_1$ and $t_2$ write on $x$ do
6. if $\exists \alpha, \beta. \langle t_1, \alpha \rangle \in wr_x \land \langle t_2, \beta \rangle \in (so \cup wr) \land \langle \alpha, \beta \rangle \in po$ then
7. $co \leftarrow co \cup \{\langle t_2, t_1 \rangle\}$;
8. if $co$ is cyclic then
9. return false;
else
10. return true;

Algorithm 4: Checking Read Atomic

Input: A history $h = \langle T, so, wr \rangle$
Output: true iff $h$ satisfies causal consistency

1. if $so \cup wr$ is cyclic then
2. return false;
3. $co \leftarrow so \cup wr$;
4. foreach $x \in \text{vars}(h)$ do
5. foreach $t_1 \neq t_2 \in T$ s.t. $t_1$ and $t_2$ write on $x$ do
6. if $\exists t_3. \langle t_1, t_3 \rangle \in wr_x \land \langle t_2, t_3 \rangle \in (so \cup wr)$ then
7. $co \leftarrow co \cup \{\langle t_2, t_1 \rangle\}$;
8. if $co$ is cyclic then
9. return false;
else
10. return true;

B PROOFS OF SECTION 3

Theorem B.1. The problem of checking whether a history satisfies Read Committed, Read Atomic, or Causal consistency is polynomial time.

Proof. We first consider the case of Read Committed. Algorithm 3 finds all the $co$ relations that are implied by the ReadCommitted axiom (fig. 2a) i.e., for all $t_1$, $t_2$ and for all $\alpha$, $\beta$ if we have, $\langle t_1, \alpha \rangle \in wr_x$ and $\langle t_2, \beta \rangle \in wr$ and $\langle \beta, \alpha \rangle \in po$ and $t_2$ writes $x$ (from figure 2a), then we add $\langle t_2, t_1 \rangle \in co$. Quantification can be done in cubic iteration over the transactions for each variable. Now, we claim $h$ is Read Committed if and only if $co$, the union of these found relations is acyclic.

First we prove that if $co$ is acyclic, then $h$ satisfies Read Committed. $co$ is acyclic, hence consider a topological order $co'$ of $co$. If $\langle h, co' \rangle$ does not satisfies Read Committed, there exists $t_1$, $t_2$ and $\alpha$, $\beta$ such that, $\langle t_1, \alpha \rangle \in wr_x$ and $\langle t_2, \beta \rangle \in wr$ and $\langle \alpha, \beta \rangle \in po$ and $t_2$ writes $x$ and $\langle t_1, t_2 \rangle \in co'$. But with the same $t_1$, $t_2$, $\alpha$, $\beta$ and variable $x$, we must have added $\langle t_2, t_1 \rangle$ in $co$ which implies any topological order of $co$ can not have $\langle t_1, t_2 \rangle$ which contradicts that $co'$ contains $\langle t_1, t_2 \rangle$.

, Vol. 1, No. 1, Article . Publication date: August 2018.
Now we prove, if \( \text{co} \) is not acyclic, then \( h \) does not satisfy Read Committed. If the history is Read Committed, there must be a commit order \( \text{co}' \) for \( h \) for which \( \langle h, \text{co}' \rangle \) satisfies Read Committed. \( \text{co}' \) must be acyclic. Now, take any cycle in \( \text{co}, t_1 \xrightarrow{\text{co}} t_2 \xrightarrow{\text{co}} \cdots \xrightarrow{\text{co}} t_k \xrightarrow{\text{co}} t_1 \). Now along these, if for all \( i, j \) \( t_i \xrightarrow{\text{co}} t_j \) then, it becomes a cycle in \( \text{co}' \). Therefore, there must be at least one pair, where \( \langle t_i, t_j \rangle \in \text{co} \), but \( \langle t_i, t_j \rangle \notin \text{co}' \) or \( \langle t_j, t_i \rangle \in \text{co}' \) since \( \text{co}' \) is total.

But \( \langle t_i, t_j \rangle \in \text{co} \) must have been added because there exist \( \alpha, \beta \) such that \( \langle t_i, \beta \rangle \in \text{wr}, \langle \beta, \alpha \rangle \in \text{po} \) and \( \langle t_j, \alpha \rangle \in \text{wr} \) and \( t_i \) writes \( x \). But \( \langle t_i, t_j \rangle \in \text{co}' \), so \( \text{co}' \) violates Read Committed for \( t_i, t_j, \alpha, \beta \). Therefore, if \( \text{co} \) has a cyclic, \( h \) does not satisfy Read Committed.

The case of Read Atomic and Causal Consistency is similar. If the \( \text{co} \) at the end of the algorithm is acyclic, then if a topological order extending it does not satisfy resp. consistency model, then it contains \( \langle t_1, t_2 \rangle \) with the quantified transactions, variables, and operations for resp. consistency model. But, then for some quantified transactions, variables and operations, we must have added \( \langle t_2, t_1 \rangle \in \text{co} \) in the algorithm. It contradicts the topological order contains \( \langle t_1, t_2 \rangle \). For the other direction, if the \( \text{co} \) at the end of the algorithm has cycle, we show there exists \( \langle t_i, t_j \rangle \in \text{co} \), like the case of Read Committed, yet it is not in a commit order satisfying the resp. consistency models. Then the commit order must have \( \langle t_j, t_i \rangle \) which violates the resp. consistency models for the exact same quantified transactions, variables and operations for which \( \langle t_i, t_j \rangle \) was added in \( \text{co} \) at first. \( \square \)

C PROOFS OF SECTION 4.2

**Lemma C.1.** The histories \( h \) and \( h_{R\mid W} \) have the same width.

**Proof.** We show that if \( h \) is of width \( k \), then the session order \( \text{so}' \) of \( h_{R\mid W} \) cannot contain an antichain of size \( k + 1 \). Let \( \{X_i^1, X_i^2, \ldots, X_i^k, X_i^{k+1}\} \) with \( X_i^l \in \{R, W\} \), for all \( 1 \leq i \leq k + 1 \), be a set of \( k + 1 \) transactions in \( h_{R\mid W} \). Then,

- if \( t_i = t_j = t \) for some \( i \neq j \), then \( X_i^j = R_t \) and \( X_j^i = W_t \) or vice-versa. Since \( \langle R_t, W_t \rangle \in \text{so}' \), this set cannot be an antichain of \( \text{so}' \).
- otherwise, by hypothesis, the set \( \{t_1, t_2, \ldots, t_k, t_{k+1}\} \) is not an antichain of \( \text{so} \). Thus, there exists \( i, j \) such that \( \langle t_i, t_j \rangle \in \text{so} \). By the definition of \( \text{so}' \), \( \langle X_i^j, X_j^i \rangle \in \text{so}' \), which implies that this set is not an antichain of \( \text{so}' \).

\( \square \)

D PROOFS OF SECTION 4.3

**Theorem D.1.** A history \( h \) satisfies snapshot isolation iff \( h_{R\mid W}^c \) is serializable.
Proof. For the “only-if” direction, we define partial commit orders $co'_t$ and $RW(co'_t)$ as in the case of prefix consistency. Along with them, we define a partial commit order $WR(co'_t)$

$$WR(co'_t) = \{ (W_{t_1}, R_{t_2}) | \exists x_{2,1} \in \text{vars}(h^c_{R|W}),$$

$$(R_{t_1}, W_{t_2}) \in \text{wr}_{x_{2,1}}',$$

$$(W_{t_1}, W_{t_2}) \in co'_t, W_{t_1} \text{ writes } x_{2,1} \}$$

which intuitively, enforces that the read part $R_{t_2}$ of a transaction $t_2$ observes the effects of the write part $W_{t_1}$ of a transaction $t_1$ when $t_1$ and $t_2$ write on a common variable and the commit order in $h$ orders $t_1$ before $t_2$ (which implies that the corresponding write transactions are ordered in the same way in $co'_t$). We define $co'_t = co'_t \cup RW(co'_t) \cup WR(co'_t)$.

The characterization of minimal cycles of $co'_t$ and ultimately, the fact that it is acyclic can be proved as in Lemma 4.5. The proof that $co'_t$ is acyclic goes as follows. As for PC, since $co'_t$ is acyclic, a cycle in $co'_t$, and in particular a minimal one, must necessarily contain a dependency from $RW(co'_t)$ or $WR(co'_t)$. Note that a minimal cycle cannot contain two dependencies in either $RW(co'_t)$ or $WR(co'_t)$ since this would imply that it contains two non-consecutive write transactions. Differently from the previous case, the cycle in $co'_t$ here can also contains the dependencies in $WR(co'_t)$ which are from write transactions to read transactions. The case of minimal cycles in $co'_t$ that contain only a dependency from $RW(co'_t)$, and no dependencies from $WR(co'_t)$, can be dealt with as in the case of PC.

Consider a minimal cycle of $co'_t$ that contains a dependency $(W_{t_1}, R_{t_2})$ in $WR(co'_t)$, which implies that $W_{t_1}, W_{t_2}$ must write on some common variable $y$. Because the minimal cycle contains at most two write transactions and one read transaction, it must also contain a dependency from read transactions to write transactions. Note that such a dependency can come only from $WR(co'_t)$. The red edges in Figure 16a show such a cycle. By the definition of $h^c_{R|W}$, we have that $W_{t_1}$ and $R_{t_2}$ write on a variable $x_{3,4}$ and $(R_{t_1}, W_{t_2}) \in \text{wr}_{x_{3,4}}'$. Since $(R_{t_1}, W_{t_2}) \in RW(co'_t)$, we have that there exists a write transaction $W_{t_1}$ s.t. $(W_{t_1}, R_{t_2}) \in \text{wr}[x]$, for some $x$, and $(W_{t_1}, W_{t_2}) \in co'_t$. The relations between these transactions of $h^c_{R|W}$ imply that the corresponding transactions of $h$ are related as shown in Figure 16b, which implies a violation of Conflict, a contradiction of the hypothesis.

For the “if” direction, let $co$ be a commit (total) order on transactions of $h^c_{R|W}$ which satisfies the serializability axiom. Let $co$ be a commit order on transactions of $h$ defined by $co = \{ (t_1, t_2) \in (W_{t_1}, W_{t_2}) \in co' \} \text{ (co is clearly a total order).}$ Showing that $co$ is an extension of $\text{wr} \cup \text{so}$ and that it doesn’t expose a Prefix violation can be done as for prefix consistency. Now, assume by contradiction that there exists a Conflict violation between $t_1, t_2, t_3, t_4$ (shown in Figure 17a). Then, the corresponding transactions $W_{t_1}, W_{t_2}, W_{t_4}, R_{t_3}, W_{t_4}$ in $h^c_{R|W}$, shown in Figure 17b, would be related as follows: (1) since $(t_1, t_2) \in \text{wr}[x]$ and $(t_1, t_2) \in co$, we have that $(W_{t_1}, R_{t_2}) \in \text{wr}'$, and $(W_{t_1}, W_{t_2}) \in co'$, (2) since $co'$ satisfies Serializability, then $(R_{t_1}, W_{t_2}) \in co'$, (3) $(t_2, t_4) \in co'$ implies $(W_{t_2}, W_{t_4}) \in co''$, (4) $(t_4, t_3) \in co$ and $t_4, t_3$ write on a common variable $y$ implies that $(W_{t_4}, W_{t_4}) \in co'$, $(R_{t_3}, W_{t_4}) \in \text{wr}[x_{3,4}]$, and $W_{t_4}$ writes the variable $x_{3,4}$, which by the serializability axiom, implies $(W_{t_4}, R_{t_3}) \in co'$. Therefore, $co'$ contains a cycle, a contradiction to the hypothesis. □

E \ SPACE BETWEEN OUR DEFINITIONS AND THE FORMALIZATION IN \cite{14}

Cerone et al. \cite{14} define the criteria RA, CC, PC, SI, and SER using a notion of history that contains only the session order so. Such a history satisfies one of these criteria in their formalization if there exists a visibility relation vis between transactions, and a commit order co extending the visibility relation that satisfy certain axioms.
The axioms used by Cerone et al. [14] are given in Table 3.

Int is an axiom which enforces that if there is a read operation $O$ on variable $x$ in a transaction and there is a read or write operation on $x$ before $O$ i.e., $\{o' \in p^{-1}(o) \mid o' = \langle x, \_ \rangle\} \neq \emptyset$, then the latest operation on $x$ before $O$ must read or write the value read by $O$ i.e., $\text{max}_p\{\{o' \in p^{-1}(o) \mid o' = \langle x, \_ \rangle\}\} = \langle x, n \rangle$.

Ext is an axiom which enforces that if a transaction $t$ has a operation $O$ which reads a variable $x$ and which is not preceded by a write on $x$, denoted by $t \models \text{read}(x, n)$, then either:

- it read the initial value 0, and there is no transaction writing on $x$ visible to $t$, i.e., $\text{vis}^{-1}(t) \cap \text{Write}_x = \emptyset$, or
- it read from a write of another transaction $t'$ which writes to variable $x$ and $t'$ is the last one in the commit order in the visibility set of $t$, i.e., $\text{vis}^{-1}(t') \cap \text{Write}_x \neq \emptyset$.

Since, the writes in our history have unique values, this is equivalent to, for all $t_1, t_2$ if $t_1 \models \text{write}(x, n)$ and $t_3 \models \text{read}(x, n)$, then for any $t_2 \in \text{vis}^{-1}(t_3)$ where $t_2 \neq t_1$ and $t_2 \models \text{write}(x, \_)$, $t_2$ cannot be after $t_1$ in co order (i.e., $t_2, t_1 \in \text{co}$ since co is total), because $t_1$ must be the maximal among the transactions that wrote $x$. We illustrated the axiom in Figure 18a, which is very similar to our definition in Figure 2.

The definitions for Session, TransVis, Prefix, TotalVis are straightforward. NoConflict enforces vis to totally order the transactions those write on same variable.

We will show in our axioms definition figures, the path between $t_2$ and $t_3$ is essentially a vis relation in $h_{\text{so}}$.

The definitions of RA, CC, PC, SI, and SER in Cerone et al. [14] are given in Table 4. Next, we show the equivalence between these definitions and our definitions in Figure 2 on histories where every value is written at most once. For a history $h = \langle T, \text{wr}, \text{so} \rangle$ as in our framework, $h_{\text{so}} = \langle T, \text{so} \rangle$.

- We show that Int $\land$ Ext $\land$ Session $\equiv$ Read Atomic

- For a history $h = \langle T, \text{wr}, \text{so} \rangle$, if $h_{\text{so}}$ satisfies Int $\land$ Ext $\land$ Session for some vis and co, we show that $h$ satisfies Read Atomic for the same co. If it does not, then, there exists $t_1, t_2, t_3$
On the Complexity of Checking Transactional Consistency

For the other direction, we have a commit order \( \text{co} \) for \( h \) which satisfies Read Atomic. We show that there exists a visibility relation \( \text{vis} \) which together with the same \( \text{co} \) and \( h_{so} \) satisfies \( \text{INT} \land \text{EXT} \land \text{SESSION} \). Let \( \text{vis} = \{ \langle t_1, t_2 \rangle | \langle t_1, t_2 \rangle \in \text{wr} \cup \text{so} \} \).

* First of all, by definition, the internal reads in our transactions are consistent to the last read or write before them. Only thing is left, to show that the first reads of a variable \( x \) before a write to \( x \) inside a variable is also reading from a unique transaction.

* If \( o_1, o_2 \) are two reads on \( x \) and \( \langle t_1, o_1 \rangle, \langle t_2, o_2 \rangle \in \text{wr} \), then by Read Atomic axiom, we have \( \langle t_1, t_2 \rangle, \langle t_2, t_1 \rangle \in \text{co} \). Therefore, the reads to \( x \) in a transaction before the first write to \( x \) are from same transaction.

* We can not have a violation of \( \text{INT} \) and \( \text{EXT} \) because we defined \( \text{vis} \) as \( \{ \langle t_1, t_2 \rangle | \langle t_1, t_2 \rangle \in \text{wr} \cup \text{so} \} \). So any violation of \( \text{EXT} \) will be a violation of Read Atomic

* \( \text{vis} \) satisfy Session, since \( \text{so} \subseteq \text{vis} \)

We show that \( \text{INT} \land \text{EXT} \land \text{SESSION} \land \text{TRANSVIS} \equiv \text{CAUSAL CONSISTENCY} \).

* If \( h \) satisfies Causal Consistency, there exists a \( \text{co} \) for \( h \). We define \( \text{vis} = (\text{wr} \cup \text{so})^+ \). \( \text{vis} \supseteq \text{wr} \cup \text{so} \), therefore as previous case, \( \text{vis} \) satisfies \( \text{INT} \land \text{EXT} \land \text{SESSION} \) and by construction of \( \text{vis} \) it is a transitive closure therefore it also satisfies \( \text{TRANSVIS} \). If there is any \( \text{INT} \) and \( \text{EXT} \) violation then there exist \( t_1, t_2, t_3 \) such that \( \langle t_1, t_3 \rangle \in \text{wr}_x \), \( t_2 \) writes on \( x \), \( \langle t_1, t_2 \rangle \in \text{co} \) and \( \langle t_2, t_3 \rangle \in \text{vis} = (\text{wr} \cup \text{so})^+ \) which is a violation of Causal Consistency. This is a contradiction.

* If there exists a \( \text{co} \) for \( h_{so} \) which satisfies \( \text{INT} \land \text{EXT} \land \text{SESSION} \land \text{TRANSVIS} \), we show, the same \( \text{co} \) satisfies Causal Consistency. If it does not, we have \( t_1, t_2, t_3 \) such that \( \langle t_1, t_3 \rangle \in \text{wr}_x \) \( t_2 \) writes on \( x \) and \( \langle t_2, t_3 \rangle \in (\text{wr} \cup \text{so})^+ \) and \( \langle t_1, t_2 \rangle \in \text{co} \). But, by \( \text{INT} \land \text{Ext} \),

\[ \forall x, \forall t_1, t_2, \forall t_3. \quad \langle t_1, t_3 \rangle \in \text{wr}_x \land t_2 \text{ writes } x \land \langle t_2, t_3 \rangle \in \text{vis} \implies \langle t_2, t_1 \rangle \in \text{co} \]

(a) Int \& Ext

\[ \begin{array}{|c|c|}
\hline
\text{Consistency model} & \text{Axioms} \\
\hline
\text{Read atomic} & \text{INT} \land \text{EXT} \land \text{SESSION} \\
\hline
\text{Causal consistency} & \text{INT} \land \text{EXT} \land \text{SESSION} \land \text{TRANSVIS} \\
\hline
\text{Prefix consistency} & \text{INT} \land \text{EXT} \land \text{SESSION} \land \text{PREFIX} \\
\hline
\text{Snapshot isolation} & \text{INT} \land \text{EXT} \land \text{SESSION} \land \text{PREFIX} \land \text{NOCONFLICT} \\
\hline
\text{Serializability} & \text{INT} \land \text{EXT} \land \text{TOTALVIS} \\
\hline
\end{array} \]

Table 4. Consistency model definitions in Cerone et al. [14].
wr ⊆ vis and by Session so ⊆ vis and by TransVis we have vis⁺ ⊆ vis which implies (wr ∪ so)⁺ ⊆ vis. There fore ⟨t₂, tr₃⟩ ∈ vis. So t₁, t₂, t₃ violates INT and EXT axiom for co, which is a contradiction.

• We show that INT ∧ EXT ∧ Session ∧ Prefix ≡ Prefix consistency.

  – If h satisfies Prefix consistency, there exists a co for h. We define vis = co⁺(wr ∪ so). vis ⊆ wr ∪ so therefore as previous case, vis satisfies INT ∧ EXT ∧ Session. Assume ⟨t₁, t₂⟩ ∈ co ∩ vis. Then there exists t₃ such that ⟨t₁, t₃⟩ ∈ co and ⟨t₃, t₂⟩ ∈ vis = co⁺(wr ∪ so). Therefore, there exists t₄ such that either t₃ = t₄ or ⟨t₃, t₄⟩ ∈ co and ⟨t₄, t₂⟩ ∈ (wr ∪ so). Since, co is a total order, then ⟨t₁, t₃⟩ ∈ co and either t₃ = t₄ or ⟨t₃, t₄⟩ imply ⟨t₁, t₄⟩ ∈ co. We have ⟨t₄, t₂⟩ ∈ (wr ∪ so). Therefore, ⟨t₁, t₂⟩ ∈ co ∩ (wr ∪ so) ⊆ vis. Therefore, co ∩ vis ⊆ vis which is Prefix axiom.

  – If hₘ satisfies INT ∧ EXT ∧ Session ∧ Prefix, then there exists a co for which the axioms satisfy. The same co will satisfy Read Atomic axiom for h. So if we have a violation in Prefix consistency, then there exist t₁, t₂, t₃ such that ⟨t₁, t₂⟩ ∈ wrₓ, t₂ writes on x and ⟨t₃, t₄⟩ ∈ co⁺(wr ∪ so) and ⟨t₃, t₂⟩ ∈ co. If ⟨t₃, t₂⟩ ∈ (wr ∪ so), then it is violation in Read Atomic, therefore, ⟨t₃, t₂⟩ ∈ co⁺(wr ∪ so) = co⁺(wr ∪ so) because co is transitive. But by INT ∧ EXT ∧ Session, (wr ∪ so) ⊆ vis, therefore co⁺(wr ∪ so) ⊆ co ∩ vis ⊆ vis. Then t₁, t₂, t₃ violates Ext.

• We have to show, INT ∧ EXT ∧ Session ∧ Prefix ∧ NoConflict ≡ Snapshot isolation.

  – If h satisfies Snapshot isolation, it also satisfies Prefix consistency. We define vis = (co⁺(wr ∪ so)) ∪ (co⁺{(t₁, t₂)|⟨t₁, t₂⟩ ∈ co, ∃x. t₁, t₂ write on x}). Clearly, vis contains the three relations for INT ∧ EXT ∧ Session ∧ Prefix proof, therefore, vis satisfies them. Also, vis satisfies NoConflict by definition since co is a total order. Any violation in INT and EXT will imply there is a t₁, t₂, t₃ such that ⟨t₁, t₃⟩ ∈ wrₓ, t₂ writes on x and ⟨t₂, t₃⟩ ∈ vis and ⟨t₁, t₂⟩ ∈ co. But by definition of vis we will have violations in either Prefix or Conflict axioms of Snapshot isolation model.

  – If hₘ satisfies INT ∧ EXT ∧ Session ∧ Prefix ∧ NoConflict, then there exists a co for which the axioms satisfy. The same co will satisfy Prefix consistency axiom for h. So if we have a violation in Snapshot isolation, it is a violation of Conflict axiom, i.e., there exist t₁, t₂, t₃ such that ⟨t₁, t₃⟩ ∈ wrₓ t₂ writes on x and ⟨t₂, t₃⟩ ∈ co⁺{(t₁, t₂)|∃x. t₁, t₂ write on x} and ⟨t₁, t₂⟩ ∈ co. But ⟨t₁, t₂⟩ ∈ co⁺{(t₁, t₂)|∃x. t₁, t₂ write on x} ⊆ vis by NoConflict and co ∩ vis ⊆ vis by Prefix. Hence, ⟨t₂, t₃⟩ ∈ vis. Then t₁, t₂, t₃ violates EXT.

• We show that INT ∧ EXT ∧ TotalVis = Serialization.

  – If h satisfies Serialization, there exists co for h that satisfy Serialization. We define vis = co. Clearly it satisfies TotalVis because co is total. We have any violation in INT and EXT, that will imply we have t₁, t₂, t₃ such that t₁, t₂, t₃ such that ⟨t₁, t₃⟩ ∈ vis t₂ writes on x and ⟨t₁, t₂⟩ ∈ co. But since vis = co, t₁, t₂, t₃ will violate Serialization axiom, which is a contradiction.

  – If hₘ satisfies INT ∧ EXT ∧ TotalVis, then there exists a co for which the axioms satisfy. If for same co, we have a violation of Serialization, then there exist t₁, t₂, t₃ such that ⟨t₁, t₃⟩ ∈ wrₓ t₂ writes on x and ⟨t₂, t₃⟩ ∈ co and ⟨t₁, t₂⟩ ∈ co. But co = vis, so then we have a INT and EXT violation in hₘ for t₁, t₂, t₃.