From Sequential Specifications to Eventual Consistency

Radha Jagadeesan and James Riely(✉)

DePaul University, Chicago, USA
jriely@gmail.com

Abstract. We address a fundamental issue of *interfaces* that arises in the context of cloud computing. We define what it means for a replicated and distributed implementation satisfy the standard sequential specification of the data structure. Several extant implementations of replicated data structures already satisfy the constraints of our definition. We describe how the algorithms discussed in a recent survey of convergent or commutative replicated datatypes [17] satisfy our definition. We show that our definition simplifies the programmer task significantly for a class of clients who conform to the CALM principle [10].

1 Introduction

An example serves to motivate the problem addressed in this paper. Consider an integer set interface with mutator methods add and remove and a single, boolean-valued accessor method get. We will assume that mutators do not return values (have return type Unit or void) and that accessors do not alter the state of the object. The sequential behavior of such a set can be defined as a set of strings such as ✗0 +0 ✓0 ✗1 and +0 +1 ✓0 ✓1 −1 ✓0 ✗1, where $+k$ represents a call to add with argument k, $-k$ represents remove(k), ✓k represents get(k) returning true and ✗k represents get(k) returning false. Since accessor methods do not alter the state of the object, the interface is closed under commutation of accessors: if $(s$ ✓0 ✗1$)$ is a valid traces in the interface, for some s, then so is $(s$ ✗1 ✓0$)$.

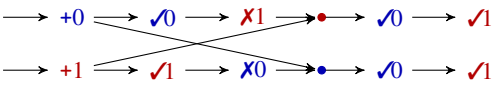
Consider the implementation of such a set as a cloud service that is implemented by replication of the data structure (eg. see [17]). In this distributed setting, we assume intra-node atomicity and sequencing of state transitions, whereas temporal relations between two computers that are distributed is only induced by the receipt of messages over the network. In this distributed context, there are two impediments to requiring the replicas to achieve consensus on a global total order [13] on the operations on the data structure. Firstly, the associated serialization bottleneck negatively affects performance and scalability (eg, see [6]). Secondly, the CAP theorem [8] imposes a tradeoff between consistency and partition-tolerance.

This has led to the emergence of alternative approaches based on *eventual consistency* and *optimistic replication* [16,19]. In such approaches, a replica may execute an operation without synchronizing with other replicas. The other replicas are updated asynchronously with the update operation. However, due to the vagaries of the network, even if every replica eventually receives and applies all updates, it could happen in possibly different orders. So, there has to be some mechanism to reconcile conflicting

M.M. Halldórsson et al. (Eds.): ICALP 2015, Part II, LNCS 9135, pp. 247–259, 2015.
DOI: 10.1007/978-3-662-47666-6_20

updates (for illustrative examples, see [17,18]). Thus, such approaches address the issue of efficiency (since any query to the state of the data structure at a replica is answered locally at the replica without any consensus overhead) and data remains available even in the presence of network partitions.

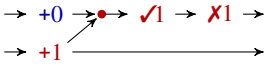
The literature on convergent or commutative replicated datatypes (CRDTs) (see [17] for a survey) provides a systematic attempt to design such datastructures. Consider the following diagram, in the style of [17].



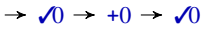
(1)

In this sample execution, the mutators +0 and +1 are executed at distinct replicas. The actions in each replica are temporally ordered from left to right, as indicated by the horizontal arrows. We assume the local updates are atomic. After a local update, the replica forwards messages to the other replicas; in the diagram, the diagonal arrows between replicas indicate messages that propagate such local updates, with the interpretation that the operation is guaranteed to be finished at the recipient at the point the arrow appears on the recipients timeline. The accessors are executed locally and atomically at each replica. Of course, there is a consistent global state, testified by ✓0 and ✓1 at both replicas, after both messages have been delivered. Thus, the literature (eg. see [17] for a precise formalization) deems this implementation to be eventually consistent, since the states of all the replicas eventually converge at quiescent points, when all the messages have been delivered. This view is adequate for examples where we are interested only in the final state of the data structure.

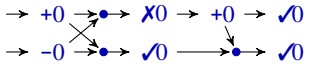
Since eventual consistency only speaks about the quiescent points of the system, it does not address correctness of intermediate states in the evolution of the system. For example, all of the following implementation traces of a putative replicated set are deemed to be eventually consistent, even though we see very problematic behavior.



(2)



(3)



(4)

In figure (2), the accessor results regresses from ✓1 to ✗1 even though there is no remove invocation in the system; in figure (3), the initial accessor ✓0 is not justified; in figure (4), the replicas conflict in their ordering of concurrent add/remove updates.

This problem is addressed by the seminal papers of [2,3]. [3] defines a notion of eventual consistency for transactions intuitively as compatibility with a serialization of them. In contrast, [2] views the interface of a replicated data structure as a *concurrent* specification that determines the valid result of an accessor from the context of a prior concurrent history. [1] extends this approach to allow for bounded rollbacks. In this style, the above examples are *declared* invalid; for example in figure (2), the result ✗1 is deemed invalid in the context of its prior history.

In addition to capturing the properties of replicated implementations much more precisely than the traditional definitions of eventual consistency, this line of work has also lead to useful tools and techniques to aid the programmer: [3] provides general

control flows sturctures that are guaranteed to yield eventually consistent implementations of transactions; [9] proves abstraction and composition theorems, applying it in particular to the replicated implementation of a graph data structure; [1] develops model checking techniques to reason about implementations relative to these specifications.

In these approaches, replicated data structures are specified directly, without any formal comparison to the sequential data structures that they are meant to approximate. This approach is (intentionally) agnostic to the design of the specifications themselves. For example, whereas the result ✗1 in figure (2) is not valid, the result ✗1 in figure (1) is valid. The justification for the different decisions about ✗1 in figures (1) and (2) is the traditional *sequential* specification of Set; namely, if there are no remove operations, ✓1 is acceptable iff there is a preceding +1.

In this paper, building on [3], we provide a definition of eventual consistency that develops precisely such a connection with the sequential specification. (As can be seen from figure (1), traditional criteria, such as linearizability [11] and quiescent consistency [5,12], do not apply here.) We show the utility of our definition by showing that clients satisfying the CALM principle (see [10] for a survey) can in fact abstract away completely from the distributed and replicated implementation and program against the sequential specification realized by the implementation.

Our work complements the research program of [1–3,9]. Our methods aim to provide a way to justify the interfaces described in this approach. In future work, we hope to use our methods to show that CALM clients of their interfaces can also be protected from details of distribution and replication. We also hope to adopt their methods to support a more general class of clients and to develop reasoning methods to show that implementations satisfy their specification.

An Informal Outline of our Approach. In a replicated data structure, a mutator m is *visible* to an event a if m executes at a's replica before a executes. We say that an implementation trace (such as those in the figures above) satisfies a sequential specification if for each event a, we can associate a string of events $\mathtt{t}(a)$ that satisfies the following.

Mutator closed: $\mathtt{t}(a)$ includes a as well as the mutator events that are visible to a
Validity: $\mathtt{t}(a)$ is a valid sequential trace that ends in a
History consistency: For any events d and e, $\mathtt{t}(d)$ and $\mathtt{t}(e)$ agree on the ordering of mutator events that are visible to both d and e.

Figure (2) does not satisfy validity at the event ✗1 in the top replica since neither +0 +1 ✗1 nor +1 +0 ✗1 is a valid trace of a set. Figure (3) does not satisfy validity at the initial event ✓0 since the trace ✓0 is not a valid trace of a set. In Figure (4), to satisfy validity, we have to associate the trace −0 +0 at the ✓0 event in the top replica and the trace +0 −0 at the ✗0 event in the bottom replica, thus violating history-consistency.

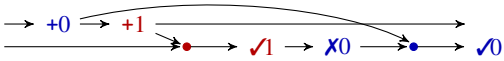
For a positive example, in figure (1), the traces associated to the event ✗1 in the top replica is +0 and the trace associated to the event ✗0 in the bottom replica is +1. There is a choice for the trace associated with the events ✓1 in the top replica and ✓0 in the bottom replica. By consistency, they need to be the same, but they can both be chosen to be either +0 +1 or +0 +1.

Our definition is flexible enough to accommodate the data structures discussed in [17], a recent survey of the literature on CRDTs. For several of these data structures, the implementations unambiguously and categorically satisfy our definitions. There are particular subtleties that arise when we match some SET implementations (the OR-set and the 2P-set) against the sequential set specification that we discuss in the technical sections that follow.

Such data structures provide a particularly simple programming view for clients located at a replica. In a logically monotone execution, the arrival time of a concurrent mutator does not alter the evolution of the system (Our formalization of logically monotone executions is inspired by ideas in [14,15].) We formalize a weaker monotonicity property: that there is *some* ordering of concurrent mutators that does not alter the evolution of a system. Under this weak monotonicity assumption (that is satisfied by all CALM executions), we prove abstraction [7] and composition [11] theorems. This is particularly relevant because it simplifies the programmer perspective for a large class of programs that includes those written in languages that realize the CALM principle, such as Bloom [4].

2 Bracketed Partial Orders and Labeled Visibility Relations

In this section, we define bracketed partial orders (BPOs). BPOs provide a formalization of diagrams such as those given in the introduction. BPOs are labelled partial orders, enriched with *replicas* and *bracketing*. Bracketing relates the remote execution of a mutator to the initial call of the mutator. Consider the following example.



(5)

This is formalized as a BPO with seven events. There are two replicas: one for each horizontal line. The partial order is given by the arrows. Two events are labelled as mutators: +0 and +1. Three events are labelled as accessors: ✓1, ✗0 and ✓0. The remaining two events (shown without labels in the diagram) are bracketing events. In the formalism, bracketing events are labelled with the name of the preceding mutator event. Generally one is interested in the isomorphism class of labelled partial orders (the pomset), and therefore the event names themselves are uninteresting.

A BPO is *causal* if the order of mutator and bracketing events at each replica respects the partial order of the mutator events themselves. All of the figures in the introduction are causal. Figure (5) is not causal, however, since the mutator order is +0 +1 but the order at the bottom replica is +1 +0.

BPOs directly capture the notion of an *operation-based* CRDT (see [17]). *State-based* CRDTs can be considered a special case of causal BPOs that communicate multiple brackets with a single communication (modelled as an uninterrupted sequence of bracketed events at the receiving replica).

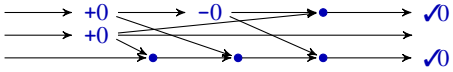
Let $\mathscr{A}$ and $\mathscr{M}$ be disjoint sets of *accessor labels* and *mutator labels*, respectively, and let $\mathscr{L} = \mathscr{A} \cup \mathscr{M}$ be a set of *labels*. We use metavariables *s*–*v* to range over various types of relations with labels in $\mathscr{L}$, which we generically refer to as "traces".

Example 2.1. In this paper we consider four implementations of an integer set datatype: the *G-set*, *U-set*, *OR-set*, and *2P-set*. See [17] for implementation details.

A G-set has mutator labels of the form $+k$, where k is an integer, and accessor labels of the form ✓k and ✗k. A G-set is *grow only*; thus, once ✓k has been observed for a particular k, it is impossible to subsequently observe ✗k. It is straightforward to specify the replicated implementation and, therefore, the corresponding BPO.

A U-set adds mutators of the form $-k$ to the labels of a G-set, denoting removal. A U-set requires that for every k, $+k$ may appear at most once in each execution—each $+k$ is *unique*. In addition, a $-k$ may only occur when $+k$ is visible. These requirements are imposed on the *client* of the U-set; it is not ensured by the U-set itself. The implementation is again straightforward. The client can guarantee uniqueness using various techniques; for example, take $k = 2^c \cdot 3^n$ where c is a globally unique client thread identifier and n is a monotone thread-local counter.

An OR-set (observed-remove set) has the same labels as a U-set, but does not require that $+k$ actions are unique. The implementation uses an underlying U-set and a map from the elements of the U-set to the elements of the OR-set. Consider the following BPO, from [17].



(6)

This BPO is not a valid execution of a G-set (because of the −0) or a U-set (because of the two +0's). However, this is a valid execution of an OR-set. The +0 in the middle replica is concurrent with the −0 of the top replica. Since they are working on top of an underlying U-set, the −0 only removes the +0 added by the top replica; the middle +0 is not affected and eventually prevails.

A 2P-set is implemented using two grow sets; one representing additions and one representing tombstones for removed elements, in the obvious way. Like a U-set, a 2P-set also constrains the behaviour of clients. A client must ensure that no element that is removed is subsequently re-added. The BPO in figure (6) is a valid 2P-set BPO if the events labeled ✓0 are re-labeled to ✗0. In a OR-set, an add "wins" over a concurrent remove, whereas in a 2P-set, the remove wins. Thus these two examples represent different specializations of the set API. The OR-set resolves figure (6) to the sequential specification +0 −0 +0 ✓0 ✓0, whereas the 2P-set resolves it to +0 +0 −0 ✗0 ✗0.

The constraints on the clients of U-set and 2P-set are required for correct functioning *as a set*. The definition of *correctness* is given informally in [17]. The main contribution of this paper is to provide a formalization, which we do in Section 3. Under our definition, all executions of the G-set will be considered correct, and all causal executions of U-set will be considered correct, but only a subset of executions of the OR-set and 2P-set will be considered correct. □

Definition 2.2. A *(replicated) bracketed partial order (BPO)* is a octuple $\langle E_\mathsf{A}, E_\mathsf{M}, E_\mathsf{B}, L, R, \lambda, \rho, \Rightarrow \rangle$ where R is a set of replicas, and the following hold.

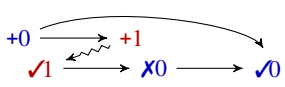
(a) sets E_A, E_M and E_B are disjoint, $L \subseteq \mathscr{L}$, and $\langle E_\mathsf{A} \cup E_\mathsf{M} \cup E_\mathsf{B}, \Rightarrow \rangle$ is a partial order,
(b) $\rho \in (E_\mathsf{A} \cup E_\mathsf{M} \cup E_\mathsf{B}) \mapsto R$ and $\lambda \in (E_\mathsf{A} \mapsto L \cap \mathscr{A}) \cup (E_\mathsf{M} \mapsto L \cap \mathscr{M}) \cup (E_\mathsf{B} \mapsto E_\mathsf{M})$,
(c) $\forall e \in E_\mathsf{B}.\ \lambda(e) \Rightarrow e$ and $\rho(\lambda(e)) \neq \rho(e)$
(d) $\forall d, e \in E_\mathsf{B}.$ if $\lambda(d) = \lambda(e)$ then either $d = e$ or $\rho(d) \neq \rho(e)$
(e) $\forall d, e \in E.$ if $\rho(d) = \rho(e)$ then either $d \Rightarrow e$ or $e \Rightarrow d$.

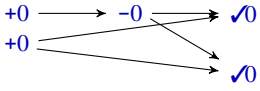
For a BPO s, we write $\mathsf{E_A}(s)$ for the accessor events of s, $\mathsf{E_M}(s)$ for the mutator events and $\mathsf{E_B}(s)$ for the bracketing events. We also define $\mathsf{E_{AM}}(s) \triangleq \mathsf{E_A}(s) \cup \mathsf{E_M}(s)$. □

Condition (b) establishes the interpretation of the labelling function: The elements of E_{A} denote local events (accessors), the elements of E_{M} denote the origination of a global event (mutators), and the elements of E_{B} denote the remote reception of a global event (brackets). Events $m \in E_{\mathsf{M}}$ and $b \in E_{\mathsf{B}}$ are a *bracketed pair* when $\lambda(b) = m$. Condition (c) establishes that in a bracketed pair, the beginning must precede the end and occur at a separate replica. Condition (d) establishes that each mutator is bracketed at most once per replica. Thus, each mutator event has one "beginning" and as many as $|R| - 1$ "endings". Condition (e) establishes that events are totally ordered at each replica; concurrency within a replica can be handled via standard means.

Definition 2.3 (Causal). Let s be an BPO. Define $\mathsf{remote}_s(e) \triangleq \{b \in \mathsf{E_B}(s) \mid \lambda_s(b) = e\}$. The BPO s is *causal* when $\forall d, e \in \mathsf{E_M}(s).\ \forall d' \in \mathsf{remote}_s(d).\ \forall e' \in \mathsf{remote}_s(e).$ if $d \Rightarrow_s e$ and $\rho_s(d') = \rho_s(e')$ then $d' \Rightarrow_s e'$. □

BPOs have a clear operational intuition. We now provide an abstract view of BPOs which is sufficient to define correctness. The relations we need are weaker than labeled partial orders. In particular, we do not require transitivity. We refer to these potentially intransitive relations as *labeled visibility relations* (LVRs). For example, starting with the BPO given in figures (5) and (6), we derive the following LVRs.



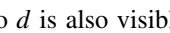
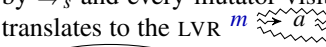
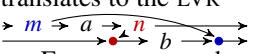


In these diagrams, we use $\rightsquigarrow$ to represent an intransitive edge and $\rightarrow$ to represent a "transitive" edge. Thus, in the left diagram, the event ✗0 sees +1 and ✓1, but not +0, whereas ✓0 sees all four prior events. Recall from figure (5) that the replica that generates ✗0 sees +1 before +0, even though these are initiated in the reverse order. A causal BPO generates a transitive LVR, as in the right diagram above. Formally, LVRs are defined with a single visibility relation, which may or may not be transitive. We include replica identifiers to define liveness properties; we ignore them except when important.

Definition 2.4. Let $s = \langle E, L, R, \lambda, \rho, \rightsquigarrow \rangle$ be a sextuple such that E is a finite set of events, L is a set of labels, R is a set of replicas, $\lambda \in (E \mapsto L)$, $\rho \in (E \mapsto R)$ and $\rightsquigarrow \subseteq (E \times E)$. We say that s is a *labeled visibility relation (LVR)* if $\rightsquigarrow$ is reflexive and acyclic. We say that s is a *labeled partial order (LPO)* if $\rightsquigarrow$ is a partial order. We say that s is a *labeled total order (LTO)* if $\rightsquigarrow$ is a total order.

Given an LVR s, we write $\mathsf{E}(s)$ for the event set of s, $\mathsf{L}(s)$ for the label set, λ_s for the labeling function and $\rightsquigarrow_s$ for the visibility relation. Define $\mathsf{E_A}(s) \triangleq \{e \in \mathsf{E}(s) \mid \lambda(e) \in \mathscr{A}\}$ and $\mathsf{E_M}(s) \triangleq \{e \in \mathsf{E}(s) \mid \lambda(e) \in \mathscr{M}\}$. □

Below, we define the translation from BPOs to LVRs. For a BPO s, the relation $\xRightarrow{\mathsf{local}}_s$ is the union of the local orders at each replica. Whenever $d \xRightarrow{\mathsf{local}}_s e$, we have that $d \rightsquigarrow_s e$. For mutators m and accessors a, we have that $m \rightsquigarrow a$ if m has been received at a's replica. Otherwise, events d and e at different replicas are ordered when they are ordered

by $\Rightarrow_s$ and every mutator visible to d is also visible to e. The BPO  translates to the LVR  , which we draw as $m \to a \to n \to b$. The BPO  translates to the LVR $m \to a \to n \rightsquigarrow b$.

For a BPO s, we have that $\forall m \in \mathsf{E_M}(s).\ \forall a, b \in \mathsf{E_A}(s).$ if $m \rightsquigarrow_s a \rightsquigarrow_s b$ then $m \rightsquigarrow_s b$.

Definition 2.5. For any sets $C \subseteq A$ and relation $\mathbf{R} \subseteq A \times A$, define $\mathbf{R} \setminus C \triangleq \mathbf{R} \cap (C \times C)$. Similarly, for $\mathbf{R} \subseteq A \times B$ and $C \subseteq A$, define $\mathbf{R} \setminus C \triangleq \mathbf{R} \cap (C \times B)$.

Let s be a BPO. Define $(d \xRightarrow{\text{local}}_s e) \triangleq (d \Rightarrow_s e)$ and $(\rho_s(d) = \rho_s(e))$. Recall Definition 2.3 of remote. Define $\mathsf{visM}_s(e) \triangleq \{m \in \mathsf{E_M}(s) \mid m \xRightarrow{\text{local}}_s e \text{ or } \exists b \in \mathsf{remote}_s(m).\ b \xRightarrow{\text{local}}_s e\}$. Then we define the LVR derived from s as follows: $\mathsf{lvr}(s) \triangleq \langle \mathsf{E_{AM}}(s), \mathsf{L}(s), \mathsf{R}(s), \rho_s, \lambda_s \setminus \mathsf{E_{AM}}(s), \rightsquigarrow \rangle$ where $\forall d, e \in \mathsf{E_{AM}}(s).\ d \rightsquigarrow e$ iff $d \in \mathsf{visM}_s(e)$ or $d \Rightarrow_s e$ and $\mathsf{visM}_s(d) \subseteq \mathsf{visM}_s(e)$. We write $\rightsquigarrow_s$ for the visibility relation of $\mathsf{lvr}(s)$. □

In a strongly distributed BPO, events at different replicas are only ordered via bracketed pairs; this disallows synchronization between replicas outside of the data structure formalized by the BPO.

Definition 2.6. A BPO is *strongly distributed* if $\forall d, e \in E_\mathsf{A} \cup E_\mathsf{M} \cup E_\mathsf{B}.$ if $\rho(d) \neq \rho(e)$ and $d \Rightarrow e$ then $\exists d' \in E_\mathsf{M}, e' \in E_\mathsf{B}.\ \lambda(e') = d'$ and $d \Rightarrow d' \Rightarrow e' \Rightarrow e$ □

Lemma 2.7. Let s be a strongly distributed BPO. Then the following three statements are equivalent: (a) s is causal, (b) $(\rightsquigarrow_s)$ is transitive, and (c) $(\rightsquigarrow_s) = (\Rightarrow_s \setminus \mathsf{E_{AM}}(s))$. □

3 Eventual Consistency

Definitions of eventual consistency (EC) traditionally include both safety and liveness properties. Liveness is purely a property of implementations. It can be expressed as a simple closure property over sets of LVRs, which we call *eventual delivery*[1].

To define safety, we must first define specifications (Definition 3.1) and give some basic vocabulary for permutations, order extensions and the like (Definition 3.2).

Specifications of sequential structures are typically given as sets of strings of labels. To simplify the definitions, we use isomorphism closed sets of LTOs: the event set identifies a bijection between an implementation LVR and its specification as an LTO. Specification sets are closed with respect to renaming of events and arbitrary replacement of the replica function (replicas don't matter in specifications). In addition, we ask that specification sets be prefix closed, accessor enabled (an specification string can always be extended by some accessor) and closed under reordering of adjacent accessors (if there is no intervening mutator, then accessors commute).

Definition 3.1. Strings may be regarded as labeled total orders (LTOs) up to replica-insensitive isomorphism. LTOs s and t are *replica-insensitive isomorphic* if $\mathsf{L}(s) = \mathsf{L}(t)$ and there exists a bijection $\alpha : \mathsf{E}(s) \to \mathsf{E}(t)$ such that $\forall e \in \mathsf{E}(s).\ \lambda_s(e) = \lambda_t(\alpha(e))$ and $\forall d, e \in \mathsf{E}(s).\ (d \rightsquigarrow_s e)$ iff $(\alpha(d) \rightsquigarrow_t \alpha(e))$.

[1] See Definition 3.2 of the *extension* of a partial order (notation $\subseteq$). A set S of LVRs satisfies *eventual delivery* if each mutator is eventually seen at every replica: $\forall s \in S.\ \forall m \in \mathsf{E_M}(s).\ \forall p \in \mathsf{R}(s).\ \exists t \in S.\ s \subseteq t$ and $\exists a \in \mathsf{E_A}(t).\ m \rightsquigarrow_t a$.

The following closure properties, defined on sets of strings, lift to isomorphism closed sets of LTOs. For strings $s, t \in \mathscr{L}^*$, let "st" denote concatenation. Let $T \subseteq \mathscr{L}^*$ be a set of strings. We say that T is *prefix closed* when $st \in T$ implies $s \in T$. We say that T is *accessor enabled* when $s \in T$ implies $\exists a \in \mathscr{A}.\ sa \in T$. We say that T is *accessor closed* when $\forall a, b \in \mathscr{A}.\ \{ta, tb\} \subseteq T$ implies $\{tab, tba\} \subseteq T$.

A *specification* is a set of total orders (LTOs) that is replica-insensitive isomorphism closed, prefix closed, accessor enabled and accessor closed. □

A specification, as given by Definition 3.1, is "sequential" because the orders are total.

Definition 3.2. We write $=_\pi$ for permutation equivalence; if $s \leq_\pi t$ then t may contain additional events that are not matched in s. If $s \subseteqq t$, then t is an *visibility-extension* of s, with the same events and greater visibility. (For an LPO this is an *order-extension*.) If $s \subseteq t$, then t is an *extension* of s, with both more events and greater visibility. $(s \setminus D)$ denotes the restriction of s to the events in D. Define $\lfloor s \rfloor^{\mathsf{M}}_s e \triangleq s \setminus \big(\{e\} \cup \{d \in \mathsf{E}_{\mathsf{M}}(s) \mid d \rightsquigarrow e\}\big)$ and $\lceil s \rceil^{\mathsf{M}}_s e \triangleq s \setminus \big(\{e\} \cup \{d \in \mathsf{E}_{\mathsf{M}}(s) \mid e \not\rightsquigarrow d\}\big)$. □

For trace s and $e \in \mathsf{E}(s)$, $\lfloor s \rfloor^{\mathsf{M}}_s e$ denotes the restriction of s to the mutator events visible to e, and $\lceil s \rceil^{\mathsf{M}}_s e$ denotes the restriction to the mutator events that are either visible to or "concurrent with" e. Both $\lfloor s \rfloor^{\mathsf{M}}_s e$ and $\lceil s \rceil^{\mathsf{M}}_s e$ include at most one accessor: e itself.

To establish eventual consistency of s with respect to T, we must exhibit a function t that maps each event in $\mathsf{E}(s)$ to a specification trace in T. The choice of t is constrained by two conditions.

Fix an event e and let $\mathsf{t}(e) = t$. The first condition requires that t include only events visible to or concurrent with e, and that t respect the order of those events in s. The requirement $\mathsf{E}(\lfloor s \rfloor^{\mathsf{M}}_s e) \subseteq \mathsf{E}(t)$ establishes that t includes e, as well as all of the mutators visible to e. The requirement $\mathsf{E}(t) \subseteq \mathsf{E}(\lceil s \rceil^{\mathsf{M}}_s e)$ establishes that t only includes mutators that are either visible to or concurrent with e. Finally, the requirement that $(s \setminus \mathsf{E}(t)) \subseteqq t$ establishes that t must respect the order of events in s.

Fix events d and e. The second condition requires that $\mathsf{t}(d)$ and $\mathsf{t}(e)$ agree on the order of mutator events in their intersection.

Definition 3.3. We say that t *refines* s at e if $\mathsf{E}(\lfloor s \rfloor^{\mathsf{M}}_s e) \subseteq \mathsf{E}(t) \subseteq \mathsf{E}(\lceil s \rceil^{\mathsf{M}}_s e)$ and $(s \setminus \mathsf{E}(t)) \subseteqq t$. We write $s \approx_{\mathsf{M}} t$ when $\forall m, n \in \mathsf{E}_{\mathsf{M}}(s) \cap \mathsf{E}_{\mathsf{M}}(t).\ m \rightsquigarrow_s n$ iff $m \rightsquigarrow_t n$.

An LVR s is *eventually consistent* (EC) with a specification T (notation $s \vDash_{\mathsf{ec}} T$) when there exists a map $\mathsf{t} : \mathsf{E}(s) \to T$ such that (a) $\forall e \in \mathsf{E}(s).\ \mathsf{t}(e)$ refines s at e, and (b) $\forall d, e \in \mathsf{E}(s).\ \mathsf{t}(d) \approx_{\mathsf{M}} \mathsf{t}(e)$.

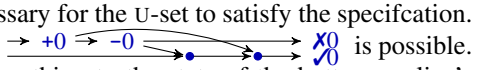
Write $S \vDash_{\mathsf{ec}} T$ when $\forall s \in S.\ s \vDash_{\mathsf{ec}} T$. □

We call this "eventual consistency" because the definition ensures that at quiescent points the same accessors at all the replicas are mapped to the same sequential trace of visible mutator events. Given eventual delivery, then all replicas must eventually agree on the order of all mutators. In the case that specifications are mutator enabled, eventual consistency can be defined in terms of a global order on mutators (u in the proposition below) that all replicas must agree to.

Definition 3.4. A specification T is *mutator enabled* if $\forall s \in T.\ \forall m \in \mathscr{M}.\ sm \in T$. □

Proposition 3.5. Suppose T is mutator enabled specification. Then $s \vDash_{\mathsf{ec}} T$ iff there exists a total order $u =_\pi s \setminus \mathscr{M}$ such that $\forall e \in \mathsf{E}(s).\ \exists t_e \in T.\ t_e$ refines s at e and $t_e \approx_{\mathsf{M}} u$. □

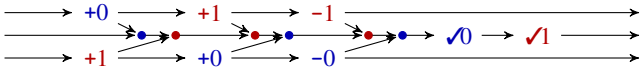
Example 3.6. Any G-set execution s satisfies our definition. To see this, we follow the characterization from Proposition 3.5. Choose u to be any linearization of the mutators in s consistent with the execution. For any accessor (✓k or ✗k), choose t to be the subsequence of the prefix of u that contains *only* the adds that precede the accessor in s.

Any causal execution s of a U-set satisfies our definition. Again, we follow the characterization from Proposition 3.5. For any query, choose t to be the subsequence of the prefix of u that contains *only* the mutators (adds and removes) that precede the accessor in s. Causality, as assumed in [17], is necessary for the U-set to satisfy the specifcation. Without causality, the following execution 

is possible. In this execution, the initial remove does nothing to the state of the bottom replica's local copy of the set, leaving the two replicas out of sync.

We now turn to the OR-set and 2P-set. First a positive example. Consider figure (6) from Example 2.1. What are acceptable return values for the get actions? The top replica sees the actions +0 −0 +0 whereas the bottom replica sees +0 +0 −0. They see the same actions, but in different orders. In the 2P-set implementation, both gets return false (remove has priority over add). In the OR-set implementation, both gets return true (add has priority over remove). Both executions are EC. For the 2P-set, let u be +0 +0 −0. For the OR-set, let u be +0 −0 +0. An implementation which returns different values for the gets is not EC because there is no t that satisfies the requirements. Since the gets see the same mutators, the traces chosen by t must agree on their order.

As a negative example, consider the following OR-set execution.



In an OR-set, removes only affect the adds that are visible. In this execution, the top −1 does not affect the bottom +1, and symmetrically, the bottom −0 does not affect the top +0; thus, the execution is possible. However, this execution is not EC with respect to any set trace: since the final mutators are both removes, at least one of ?0 and ?1 must return false in any sequential trace.

To guarantee EC executions of an OR-set, it is sufficient to require that every −k action be ordered before any concurrent +k of the same value. If the resulting enriched BPO is acyclic, then the OR-set execution is EC. The example above fails this test since we would have a cycle involving all of the mutators: +0 +1 −1 +1 +0 −0 +0.

The analysis of the 2P-set is symmetric. □

We end this section with the following simple fact about eventual consistency. The proof uses the fact that we allow events that are concurrent with e to be included in $\mathtt{t}(e)$.

Lemma 3.7. If $v \vDash_{\mathsf{ec}} T$ and $s \subseteq v$ then $s \vDash_{\mathsf{ec}} T$. □

4 Results

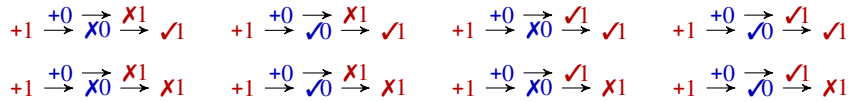
We define a language of clients and define interaction between a client and data structure. We then define monotonicity and state the abstraction and composition results.

Clients. We consider a simple language for clients: parallel composition of sequential processes, which include method call, sequencing and conditional. Let tt and ff represent the boolean constants. Let k range over *values*, which include tt and ff. Let o range over *objects*, m over *mutator methods*, and a over *accessor methods*. Then *programs* (P), *configurations* (C) and *labels* (ℓ) are defined as follows.

$$\begin{array}{rl} P & ::= \mathsf{stop} \mid o.m(k);P \mid \mathsf{if}\, o.a(k)\, \mathsf{then}\, P \mid \mathsf{if}\, o.a(k)\, \mathsf{then}\, P_1\, \mathsf{else}\, P_2 \\ C & ::= P_1 \parallel \cdots \parallel P_n \\ \ell & ::= o.m(k) \mid o.a(k){:}\mathsf{tt} \mid o.a(k){:}\mathsf{ff} \end{array}$$

For the most part, we elide occurrences of stop and explicit object references, writing $o.a(k);\mathsf{stop}$ as "$a(k)$". We also write $\mathsf{if}\, a(k)\, \mathsf{then}\, P\, \mathsf{else}\, P$ as "$a(k);P$". In our running example, we have been writing the label $\mathsf{add}(k)$ as "+k", $\mathsf{remove}(k)$ as "–k", $\mathsf{get}(k){:}\mathsf{tt}$ as "✓k" and $\mathsf{get}(k){:}\mathsf{ff}$ as "✗k".

Let $[\![\cdot]\!]$ be a semantic function mapping configurations to sets of LVRs. The definition is the obvious one. For example, let C be the configuration $\mathsf{add}(0);\mathsf{get}(1) \parallel \mathsf{add}(1);\mathsf{get}(0);\mathsf{get}(1)$. Then $[\![C]\!]$ is a set of the following eight LVRs (up to isomorphism).



(7)

Under what circumstances can such a client interact with a 2P-set or OR-set and expect that the observed behaviour if compatible with a sequential set? This question is addressed in our first result, known as *abstraction* : when is the actual implementation of a data structure a safe substitute for its "abstract" specification?

We must first define what it means for a client and a data structure to interact.

Interaction. From figure (7) it is clear that the data structure must be able to filter out executions of the client. The set datatype does not include any traces that are compatible with the four LPOs on the second line of figure (7).

From figure (7) it is equally clear that the data structure must be able to introduce visibility that is not found in the client. For example, to achieve the results on the first line, one must introduce visibility between the client programs, as follows.

It is safe for the data structure to add visibility (and therefore order) to the client; however, the reverse is not true. A client can only introduce order that is compatible with the data structure specification. Consider the sequential client $\mathsf{add}(0);\mathsf{get}(0);\mathsf{get}(0)$. If this client communicates to separate replicas in a G-set, the execution +0 ✓0 ✗0 is possible, via the BPO $\xrightarrow{\quad} +0 \rightarrow \underset{\quad}{\overset{\quad}{\checkmark 0 \rightarrow}}$. To avoid such anomalies, it is sufficient to require that sequential clients alway move forward in the visibility relation. This can be achieved by restricting each client program to communicate with a single replica, or by other means. We include this requirement in our definition of composition, without specifying how it is fulfilled.

Definition 4.1. Let S be a set of LVRs. $[\![C]\!](S) \triangleq \{s \in S \mid \exists s' \in [\![C]\!].\ s' \subseteq s\}$ □

One reading of the asymmetry in this definition is that a data structure may introduce order, but not its clients. A more generous reading is that clients may require order that is compatible with the data structure (that the data structure *could* have), but may not introduce incompatible order.

Monotonicity and Abstraction. Even with this definition of the semantics, abstraction fails in general. Consider the client $\mathsf{add}(0);\mathsf{get}(1) \parallel \mathsf{add}(1);\mathsf{get}(0)$. The BPO $\xrightarrow{} +0 \rightarrow \xrightarrow[+1]{} \rightarrow \xrightarrow{} \rightarrow \xrightarrow[\times 0]{} \rightarrow$ has order agreeing with the client and is an EC execution of a set, but this behaviour is not observable by a client interacting with a sequential set. Abstraction holds for clients that ensure *monotone* access to the data structure.

A set V is monotone if whenever V contains a trace u with a mutator m that is concurrent with another event e, then V also contains a visibility extension v that orders m and e. Since v is an visibility extension of u, it must contain the same labels.

Definition 4.2. A set V of LVRs is *monotone* when $\forall u \in V.\ \forall m \in \mathsf{E}_{\mathsf{M}}(u).\ \forall e \in \mathsf{E}(u).$ if $(m \not\rightsquigarrow_u e$ and $e \not\rightsquigarrow_u m)$ then $\exists v \in V.\ u \subsetneqq v$ and $(m \rightsquigarrow_u e$ or $e \rightsquigarrow_u m)$ □

Theorem 4.3. Let S be a set of LVRs and let T be a specification such that $S \vDash_{\mathsf{ec}} T$. Let C be a client such that $[\![C]\!](S)$ is monotone. Then $\forall s \in [\![C]\!](S).\ \exists t \in [\![C]\!](T).\ s \subsetneqq t$. □

The theorem states that if there is an execution s in $[\![C]\!](S)$, then is a corresponding execution t in $[\![C]\!](T)$ that has exactly the same labels, and potentially more order. This says that any client behaviour possible with the implementation S is also possible using the sequential specification T.

Example 4.4. The G-set trace $\xrightarrow{} +0 \rightarrow \xrightarrow[+1]{} \times 1 \rightarrow$ can be allowed in a monotone subset of G-set executions, since we can order ✗1 before +1 and still have a set execution; the events +1 and +0 can be ordered arbitrarily. The G-set trace $\xrightarrow{} +0 \rightarrow \xrightarrow[+1]{} \times 1 \rightarrow \xrightarrow[\times 0]{} \rightarrow$, however, cannot be allowed in a monotone subset of G-set executions. In this case, if we order +1 before ✗1, then the result is clearly not a set execution: 1 has been added, but is not reported present. If we choose the reverse order, we have +0 before ✗0, and again the result fails to be a valid set execution. Example 4.7 below gives an example of a specific G-set client that satisfies monotonicity, under given assumptions. To design a general class of context-independent monotone clients for a given data structure, it is necessary to limit client programs, as done in languages in the CALM framework [10].

For example, in order to create a monotone subset of G-set traces, it is sound to restrict clients to disallow the two-armed if-then-else. The semantics of the one-armed if-then is blocking—the client must wait until the condition is true. The theorem establishes that such clients can safely us a G-set as though it were a sequential set.

The theorem provides guidance about how to design safe clients. In order to allow a two-armed conditional with the G-set, we must ensure that events occurring concurrently with a negative response cannot invalidate that response. One way to achieve this, following [10], is for the G-set to insert a barrier before returning a negative response. □

Composition of Data Structures. We now turn our attention to reasoning about compound data structures.

Definition 4.5. Given disjoint LTOs t_1 and t_2 (that is, $\mathsf{E}(t_1) \cap \mathsf{E}(t_2) = \emptyset$), let $t_1 ||| t_2$ denote the set of their interleavings. This notion lifts to sets as follows: $(T_1 ||| T_2) \triangleq \{t \in (t_1 ||| t_2) \mid t_1 \in T_1 \text{ and } t_2 \in T_2 \text{ and } (\mathsf{E}(t_1) \cap \mathsf{E}(t_2) = \emptyset)\}$.

Given an LVR s and $L \subseteq \mathsf{L}(s)$, write $s \setminus L$ for the LVR that results by restricting s to events with labels in L. This notation lifts to sets in the obvious way: $S \setminus L \triangleq \bigcup_{s \in S} s \setminus L$. □

Theorem 4.6. Let $[\![C]\!](S)$ be a monotone set of LVRs. Let L_1 and L_2 be disjoint subsets of $\mathscr{L}$. For $i \in \{1,2\}$, let T_i be a specification with labels chosen from L_i. If $([\![C]\!](S) \setminus L_1) \vDash_{\mathsf{ec}} T_1$ and $([\![C]\!](S) \setminus L_2) \vDash_{\mathsf{ec}} T_2$ then $[\![C]\!](S) \vDash_{\mathsf{ec}} (T_1 ||| T_2)$. □

Example 4.7. The following definitions implement a 2P-set p, using two G-sets, a for "added" and t for "tombstone": $p.\mathsf{add}(k) \triangleq a.\mathsf{add}(k)$, $p.\mathsf{remove}(k) \triangleq t.\mathsf{add}(k)$, and $p.\mathsf{get}(k) \triangleq a.\mathsf{get}(k) \wedge \neg t.\mathsf{get}(k)$. If we can establish the necessary monotonicity properties, then we can reason with the sequential specifications of a and t in proving p correct. An execution of a grow set g is monotone so long as for any $g.\text{✗}k$, there is no concurrent $g.{+}k$. We must show that both a and t are accessed monotonically, so long as p is accessed monotonically. An execution of a 2P-set p is monotone so long as (1) for any $p.\text{✓}k$, there is no concurrent $p.{-}k$, and (2) for any $p.\text{✗}k$, there is no concurrent $p.{+}k$.

The conditions for monotonicity of p are sufficient to establish monotonicity of a and t. There are two cases: (1) Suppose $p.\text{✓}k$. By monotonicity, we know there is no concurrent $p.{-}k$, therefore no concurrent $t.{+}k$. By definition of $p.\mathsf{get}$, we must have $a.\text{✓}k$ and $t.\text{✗}k$. Monotonicity imposes no constraints on $a.\text{✓}k$; to satisfy $t.\text{✗}k$, we must have no concurrent $t.{+}k$, but this is exactly guaranteed by monotonicity of p. (2) Suppose $p.\text{✗}k$. Then we know there is no concurrent $p.{+}k$, therefore no concurrent $a.{+}k$. By definition of $p.\mathsf{get}$, we must have either $a.\text{✗}k$ or $t.\text{✓}k$. The argument is as before. □

References

1. Bouajjani, A., Enea, C., Hamza, J.: Verifying eventual consistency of optimistic replication systems. In POPL 2014, pp. 285–296 (2014)
2. Burckhardt, S., Gotsman, A., Yang, H., Zawirski, M.: Replicated data types: specification, verification, optimality. In: POPL 2014, pp. 271–284 (2014)
3. Burckhardt, S., Leijen, D., Fähndrich, M., Sagiv, M.: Eventually consistent transactions. In: Seidl, H. (ed.) Programming Languages and Systems. LNCS, vol. 7211, pp. 67–86. Springer, Heidelberg (2012)
4. Conway, N., Marczak, W.R. et al.: Logic and lattices for distributed programming. In: ACM Symposium on Cloud Computing, pp. 1:1–1:14 (2012)
5. Derrick, J., Dongol, B., et al.: Quiescent consistency: defining and verifying relaxed linearizability. In: Formal, Methods, pp. 200–214 (2014)
6. Ellis, C.A., Gibbs, S.J.: Concurrency control in groupware systems. ACM SIGMOD Record **18**(2), 399–407 (1989)
7. Filipovic, I., O'Hearn, P.W., Rinetzky, N., Yang, H.: Abstraction for concurrent objects. Theoretical Comp. Sci. **411**, 4379–4398 (2010)

8. Gilbert, S., Lynch, N.: Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services. SIGACT News, pp. 51–59 (2002)
9. Gotsman, A., Yang, H.: Composite replicated data types. In: Vitek, J. (ed.) ESOP 2015. LNCS, vol. 9032, pp. 585–609. Springer, Heidelberg (2015)
10. Hellerstein, J.M.: The declarative imperative: Experiences and conjectures in distributed logic. SIGMOD Rec. **39**(1), 5–19 (2010)
11. Herlihy, M., Wing, J.M.: Linearizability: A correctness condition for concurrent objects. ACM TOPLAS **12**(3), 463–492 (1990)
12. Jagadeesan, R., Riely, J.: Between linearizability and quiescent consistency. In: Esparza, J., Fraigniaud, P., Husfeldt, T., Koutsoupias, E. (eds.) ICALP 2014, Part II. LNCS, vol. 8573, pp. 220–231. Springer, Heidelberg (2014)
13. Lamport, L.: Time, clocks, and the ordering of events in a distributed system. Commun. ACM **21**(7), 558–565 (1978)
14. Panangaden, P., Shanbhogue, V., Stark, E.W.: Stability and sequentiality in dataflow networks. In: ICALP 1990, pp. 308–321 (1990)
15. Panangaden, P., Stark, E.W.: Computations, residuals, and the power of indeterminacy. In: ICALP 1988, pp. 439–454 (1988)
16. Saito, Y., Shapiro, M.: Optimistic replication. Comput. Surv. **37**(1), 42–81 (2005)
17. Shapiro, M., Preguiça, N., Baquero, C., Zawirski, M.: A comprehensive study of Convergent and Commutative Replicated Data Types. TR 7506, Inria (2011)
18. Terry, D.B., Theimer, M.M. et al.: Managing update conflicts in bayou, a weakly connected replicated storage system. In: SOSP (1995)
19. Vogels, W.: Eventually consistent. Communications of the ACM **52**(1), 40–44 (2009)