DuoAI: Fast, Automated Inference of Inductive Invariants for Verifying Distributed Protocols

Jianan Yao, Runzhou Tao, Ronghui Gu, and Jason Nieh, Columbia University

https://www.usenix.org/conference/osdi22/presentation/yao
Abstract

Distributed systems are complex and difficult to build correctly. Formal verification can provably rule out bugs in such systems, but finding an inductive invariant that implies the safety property of the system is often the hardest part of the proof. We present DuoAI, an automated system that quickly finds inductive invariants for verifying distributed protocols by reducing SMT query costs in checking invariants with existential quantifiers. DuoAI enumerates the strongest candidate invariants that hold on validate states from protocol simulations, then applies two methods in parallel, returning the result from the method that succeeds first. One checks all candidate invariants and weakens them as needed until it finds an inductive invariant that implies the safety property. Another checks invariants without existential quantifiers to find an inductive invariant without the safety property, then adds candidate invariants with existential quantifiers to strengthen it until the safety property holds. Both methods are guaranteed to find an inductive invariant that proves desired safety properties, if one exists, but the first reduces SMT query costs when more candidate invariants with existential quantifiers are needed, while the second reduces SMT query costs when few candidate invariants with existential quantifiers suffice. We show that DuoAI verifies more than two dozen common distributed protocols automatically, including various versions of Paxos, and outperforms alternative methods both in the number of protocols it verifies and the speed at which it does so, including solving Paxos more than two orders of magnitude faster than previous methods.

1 Introduction

The world relies on distributed systems, but these systems are increasingly complex and hard to design and implement correctly. To address this problem, developers are starting to turn to formal verification techniques to prove the correctness of distributed systems [11, 20, 35]. This involves formally verifying that desired safety properties hold for the distributed protocol. A safety property is an invariant that should hold true at any point in a system’s execution. It ensures the protocol does not reach invalid or dangerous states. For example, the safety property for a distributed lock protocol [11] is that no two nodes in the system hold a lock at the same time. The proof requires finding an invariant that implies the safety property, then proving that it is inductive. An invariant is inductive if it holds for all initial states of the system, and is preserved on all valid transitions so that it holds for any reachable state of the system.

Unfortunately, finding an inductive invariant is often the hardest part of the proof [21]. Invariants can be expressed as logical formulas consisting of universal (∀) and existential (∃) quantifiers with a certain number of variables, and a set of logical relations among the variables. Recent work has focused on automating the process of finding an inductive invariant, but has various limitations. I4 [21] was the first to automate the process, but provides no guarantee that it can find the inductive invariant and does not work for invariants with existential quantifiers. Our previous work DistAI [38] provides speed advantages over I4 and a guarantee of finding an ∃-free inductive invariant if one exists, but also does not work for invariants with existential quantifiers. FOL-IC3 [13] was the first to handle existential quantifiers, but is inefficient due to its heavy use of expensive SMT queries. It often fails to find invariants for protocols that can be solved by other approaches such as I4 and DistAI. SWISS [10] can successfully find an inductive invariant for Paxos, but does not work for more complex protocols such as stoppable Paxos [27]. It fails or is much slower than I4 and DistAI for many protocols without existential quantifiers.

We present DuoAI, an automated system to quickly find inductive invariants for verifying distributed protocols, with and without existential quantifiers, including complex versions of Paxos. Even though a distributed protocol may be used in very large systems, its invariants are likely to be concise, as protocols need to be designed and understood by humans to be correct. As a result, DuoAI operates in formula space and considers smaller formulas first to enumerate candidate invariants, which are then checked by an SMT solver. Formula size is defined by a maximum number of quantified variables (a variable and its quantifier ∀ or ∃) and relations. If DuoAI does
Based on this observation, DuoAI introduces and combines new techniques that avoid the limitations of SMT solvers in checking invariants with existential quantifiers.

First, DuoAI runs protocol simulations at various instance sizes and logs the reached protocol states, which we call samples. Instance size refers to the size of distributed system (number of nodes, packets, etc.) running the protocol. These simulations are fast to execute. DuoAI directly checks candidate invariants against the samples, pruning those that do not hold to reduce the number of invariants checked by an SMT solver. To do this systematically, DuoAI introduces the minimum implication graph, which for a given invariant, shows all its implied weaker invariants. It then selects the strongest candidate invariants in the graph that hold for the samples.

Second, DuoAI combines the strongest candidate invariants with the safety property and feeds them to an SMT solver to check if the conjunction is inductive. If the check fails, it monotonically weakens the invariants using the graph and repeats the process until an inductive invariant is found. If the number of candidate invariants is not too large and most are required in the final solution, this method will be effective at reducing the number of SMT queries by feeding all of the candidate invariants to the SMT solver at once.

Third, DuoAI feeds the strongest candidate universal invariants, those without existential quantifiers, from the graph to an SMT solver to check if the conjunction, without the safety property, is inductive. If the check fails, it monotonically weakens the invariants using the graph, only considering candidate universal invariants, and repeats the process until an inductive invariant is found. If the number of candidate invariants with existential quantifiers is large and most are not in the final solution, this method will be effective at avoiding too complex SMT queries, because it only feeds a few invariants to the SMT solver each time.

DuoAI runs these two methods for refining candidate invariants in parallel, a top-down refinement that weakens the candidates and a bottom-up refinement that strengthens the candidates, returning the result from the method that succeeds first. We prove that both methods are guaranteed to find the inductive invariant that proves the desired safety property, but they may have very different running times and resource requirements depending on the distributed protocol being verified. Using both methods together provides the best of both worlds in addressing the inefficiencies of SMT solvers.

We evaluated DuoAI using 27 widely-used distributed protocols in a head-to-head comparison against other approaches, including I4, DistAI, FOL-IC3, and SWISS. DuoAI outperforms all of the other approaches in terms of both the number of protocols for which it finds an inductive invariant and the speed at which it does so. DuoAI solves Paxos more than two orders of magnitude faster than any other approach, and is the only system that can solve more complex versions of Paxos including multi-Paxos, stoppable Paxos, and fast Paxos.

2 Overview

We use a simplified consensus protocol as an example to show how DuoAI works. Figure 1 shows the protocol written in Ivy [28], a language and tool for specifying, modeling, and verifying distributed protocols built on top of the Z3 SMT solver. Each node can vote for another node to be the leader, and when a node receives votes from a quorum of nodes, it can become the leader and decide on a value. The protocol state at any moment is represented by five relations (Lines 5-9).

```
type value
   type quorum
   type node
relation vote(N1:node, N2:node)
relation voted(N:node)
relation leader(N:node)
relation decided(N:node, V:value)
relation member(N:node, Q:quorum)
axiom forall Q1, Q2. exists N. member(N, Q1) & member(N, Q2)

after init {
   voted(N) := false;
   vote(N1, N2) := false;
   leader(N) := false;
   decided(N, V) := false;
}

action cast.vote(n1: node, n2: node) = {
   require -voted(n1);
   vote(n1, n2) := true;
   voted(n1) := true;
}

action become_leader(n: node, q: quorum) = {
   require forall N. member(N, q) -> vote(N, n);
   leader(n) := true;
}

action decide(n:node, v: value) = {
   require leader(n);
   require forall V. ~decided(n, V);
   decided(n, v) := true;
}

invariant decided(N1,V1) & decided(N2,V2) -> V1=V2
```

Figure 1: The simplified consensus protocol written in Ivy. Capitalized variables are implicitly quantified. For example, Line 16 means \(\forall N. node. V: value. decided(N, V) := false\). ‘~’ stands for negation.
indicates whether node $n_1$ has voted for node $n_2$. $\text{voted}(n)$ indicates whether node $n$ has ever cast a vote. $\text{leader}(n)$ indicates if $n$ is the leader among nodes. $\text{decided}(n,v)$ indicates whether node $n$ has decided on value $v$. $\text{member}(n,q)$ indicates if node $n$ belongs to quorum $q$, where each quorum is a set of nodes. The axiom (Line 10) dictates a property of the member relation: any two quorums of nodes must have at least one node in common. After initialization (Lines 13-16), the protocol can non-deterministically transition from one state to another as described by the three actions $\text{cast\_vote}$, $\text{become\_leader}$, and $\text{decide}$ (Lines 19-34). For example, $\text{cast\_vote}(n_1,n_2)$ lets a node $n_1$ vote for another node $n_2$, under the precondition that $n_1$ has not voted before (Line 20). Then the protocol will transition to a new state where $\text{vote}(n_1,n_2) = \text{true}$ and $\text{voted}(n_1) = \text{true}$. Finally, the safety property (Line 36) encodes the desired property of correctness of the protocol that the system cannot decide on two different values.

The safety property is an invariant of the protocol, but is not inductive as taking an action from a state satisfying the safety property may result in a new state that breaks the safety property. To verify the protocol, we need four additional invariants:

\begin{align}
\forall n_1,n_2: \text{node}. \text{vote}(n_1,n_2) \rightarrow \text{voted}(n_1) \quad (1) \\
\forall n_1,n_2,n_3: \text{node}. \text{vote}(n_1,n_2) \land \text{vote}(n_1,n_3) \rightarrow n_2 = n_3 \quad (2) \\
\exists Q: \text{quorum}. \forall n_1,n_2: \text{node}. \\
\text{leader}(n_1) \land \text{member}(n_2,Q) \rightarrow \text{vote}(n_2,n_1) \quad (3) \\
\forall N: \text{node}. V: \text{value}. \text{decided}(N,V) \rightarrow \text{leader}(N). \quad (4)
\end{align}

The first invariant says that if a node has voted for another node, then it must be recorded as $\text{voted}$ in the protocol. The second says that one node cannot vote for two different nodes. The third says that a leader must be endorsed by a quorum of nodes. More specifically, we can find a quorum $Q$ that every node $n_2$ in the quorum must have voted for the leader $n_1$. The fourth says that only a leader can decide on a value. The conjunction of the four invariants and the safety property is inductive.

To find this inductive invariant, DuoAI simulates the protocol using different instance sizes and logs the samples. It then builds a minimum implication graph, a small fragment of which is shown in Figure 2. The full graph for simplified consensus has over 35K nodes and 170K edges. Nodes represent formulas and edges represent implication between formulas. A stronger formula will have a directed edge to an implied weaker formula. DuoAI enumerates possible candidate invariants following the graph and adds it to the candidate invariant set if it holds on the samples. For example, DuoAI checks the root node in Figure 2 and it does not hold on the samples. DuoAI then checks its implied weaker formulas, the two nodes in the second layer, iteratively going down the graph. For the simplified consensus protocol, enumeration ends with 19 candidate invariants, including equivalent forms of Eq. (1), (2), (3), and (4).

After enumeration, DuoAI runs top-down and bottom-up refinement in parallel. Top-down refinement feeds all candidate invariants and the safety property to Ivy to see if their conjunction is inductive. For simplified consensus, the conjunction is inductive, so no further weakening is required. Bottom-up refinement feeds all $\forall$-only invariants from the initial candidate set to Ivy then weakens them until the set of invariants is itself inductive, but may not imply the safety property. For simplified consensus, this universal core includes three invariants Eqs. (1), (2), and (4). DuoAI then tries to search for additional invariants and eventually identifies invariant (3) for the simplified consensus protocol, forming an inductive invariant set. For simplified consensus, top-down refinement succeeds more quickly than bottom-up refinement.

### 3 Minimum Implication Graph

The backbone of DuoAI is the minimum implication graph, which encodes implication relations among formulas. The graph is used to determine the order of formulas to be enumerated, and how invariants are weakened. We present formulas in prenex normal form, where the quantified variables, called the prefix, appear at the beginning of the formula followed by quantifier-free relations, called the matrix. The matrix is required to be in disjunctive normal form (DNF). For simplicity, here we only consider predicate symbols with equality. The methods can be extended to uninterpreted functions in the same manner as DistAI [38].

A formula $P$ is strictly stronger than $Q$ if $P \Rightarrow Q$ and $Q \not\Rightarrow P$. For two formulas $P,Q \in S$, where $S$ is a finite formula search space, there is a directed edge from $P$ to $Q$ in the minimum implication graph if and only if $P$ is strictly stronger than $Q$ and there is no formula $R$ which is strictly weaker than $P$ while strictly stronger than $Q$. For example, the fragment of the minimum implication graph in Figure 2 includes three formulas:

\begin{align}
\forall N. \text{vote}(N,N) \quad (5) \\
\exists N. \text{vote}(N,N) \quad (6) \\
\exists N_1,N_2. \text{vote}(N_1,N_2) \quad (7)
\end{align}

![Figure 2: Fragment of the minimum implication graph for the simplified consensus protocol.](image-url)
Eq. (5) ⇒ (6) since if vote(N,N) is true for all N, there must exist some N for which it is true. Eq. (6) ⇒ (7) since if vote(N,N) is true for some N, there must exist some N₁ = N₂ for which vote(N₁,N₂) is true. Because Eq. (5) ⇒ (6) ⇒ (7), there is an edge from Eq. (5) to (6), an edge from Eq. (6) to (7), but no edge from Eq. (5) to (7), because Eq. (6) is between them.

DuoAI defines the search space S as all formulas in conjunctive normal form for a given set of quantified variables and formula size. The formula size is defined by four parameters: max_exists sets the maximum number of existentially quantified variables, maxliteral sets the upper bound of the total number of literals in the formula, max_and sets the maximum number of literals connected by AND, and max_or sets the maximum number of conjunctions connected by OR.

The minimum implication graph has two important properties as stated in Lemmas 1 and 2:

**Lemma 1.** The minimum implication graph is a directed acyclic graph (DAG).

**Proof.** Suppose there is a cycle P₁ → P₂ → ... → Pₖ → P₁. The edges P₁ → P₂, ..., Pₖ₋₁ → Pₖ imply that P₁ ⇒ P₂, ..., Pₖ₋₁ ⇒ Pₖ. From the transitivity of ⇒ we know P₁ ⇒ Pₖ. Since there is an edge from Pₖ to P₁, we know P₁ ∉ Pₖ, a contradiction. □

**Lemma 2.** For any P,Q ∈ S, there is a path from P to Q in the minimum implication graph if and only if P ⇒ Q ∧ Q ∉ P.

**Proof.** We first prove the “if” direction by induction on the number of formulas in S that are strictly weaker than P while strictly stronger than Q. For the base case, if there are zero such formulas, then by definition there is an edge from P to Q. Next we prove the induction step. Suppose for any P,Q ∈ S, if P ⇒ Q ∧ Q ∉ P, and there is no more than n formulas that are strictly weaker than P while strictly stronger than Q, then there is a path from P to Q. Now consider the case that there are n + 1 formulas that are strictly weaker than P while strictly stronger than Q. By the induction hypothesis, there is a path from P to R. In the same manner, we can show there is a path from R to Q. Then we concatenate the two paths and get a path from P to Q.

Next we prove the “only if” direction. If there is a path from P to Q. Let P,F₁,F₂,...,Fₖ,Q be the path. We know P ⇒ F₁, ..., Fₖ ⇒ Q, so P ⇒ Q. We prove Q ∉ P by contradiction. Suppose Q ∈ P, then P ⇔ Q, so there must be an edge from Fₖ to P. This forms a cycle P,F₁,...,Fₖ,P, a contradiction to Lemma 1. □

To build the minimum implication graph, we need to determine the “root” nodes in the graph, that is, formulas with no predecessors since they cannot be implied by any other formula, and how to find their successors. In DuoAI, a formula P ∈ S is added to the set of root nodes if it falls into one of two cases:

1. P has no ∃-quantified variable and no logical OR. For example:

   P = ∀N : node. vote(N,N) ∧ leader(N).

2. P has unique ∃-quantified variables and no logical OR. For example:

   P = ∃N₁,N₂ : node. N₁ ≠ N₂ ∧ vote(N₁,N₂).

Intuitively, if a formula has an ∃, then by changing it to a ∀, we can get a stronger formula. If a formula has a logical OR, then by removing the OR and any literals followed by it, we can get a stronger formula. So in general, a root formula should have no ∃ and no OR, such as Eq. (8). There is one exception, represented by Eq. (9). At first sight Eq. (9) has a predecessor ∀N₁,N₂ : node. N₁ ≠ N₂ ∧ vote(N₁,N₂). However, this formula is a contradiction because ∀N₁,N₂ : node. N₁ ≠ N₂ cannot be true. The minimum implication graph does not include tautologies and contradictions, so Eq. (9) itself is a root formula.

Starting from the root nodes, DuoAI incrementally builds the minimum implication graph. For formulas P,Q ∈ S, DuoAI adds an edge from P to Q if the shapes of P and Q fall into one of five cases:

1. P and Q share the same matrix. Q replaces the ∀-quantified variables of one type with ∃-quantified variables. For example:

   P = ∀N : node. V : value. ¬decided(N,V)
   Q = ∃N : node. ∀V : value. ¬decided(N,V).

2. P and Q share the same prefix. Q has one less ANDed literal than P. For example:

   P = Eq.(8)  Q = Eq.(5).

3. P and Q share the same prefix. Q has one more ORed conjunction than P. For example:

   P = ∀N : node. vote(N,N)
   Q = ∀N : node. vote(N,N) ∨ (voted(N) ∧ leader(N)).

DuoAI requires that the ORed conjunction be maximal, which means it contains the maximum number of literals for the search space. The conjunction voted(N) ∧ leader(N) in Q is maximal if max_and = 2 or max_literal = 3. For example, Q = ∀N : node. voted(N) ∨ voted(N) also adds one more ORed conjunction from P, but DuoAI does not add an edge from P to Q, because Q is strictly stronger than Q'.

4. Starting from P, Q projects two ∀-quantified variables of the same type into one variable. For example:

   P = ∀N₁,N₂ : node. vote(N₁,N₂)
   Q = ∀N : node. vote(N,N) ∧ leader(N).

5. Starting from Q, P projects two ∃-quantified variables of the same type into one variable. For example:

   P = Eq.(6)  Q = Eq.(7).
The graph constructed in this way may differ slightly from the exact minimum implication graph due to equivalent formulas. For example, formulas $\forall X. p(X) \lor (\neg p(X) \land q(X))$ and $\forall X. p(X) \lor q(X)$ fall into the second case, so there is an edge in the constructed graph. However, the two formulas are equivalent so there is no edge in the exact graph. We call the graph constructed by DuoAI an approximate minimum implication graph, whose properties are formalized in Lemmas 3, 4, and 5:

**Lemma 3.** The approximate minimum implication graph is a directed acyclic graph (DAG).

**Proof.** For all of the five cases, we can show that for formulas along any path in the approximate minimum implication graph, there exists one function that is strictly increasing, so there can be no cycle. For example, this is true for the function $(\# \exists$-variables$) - (\# \forall$-variables$) + (\max$-and$ + (\# \lor) - (\# \land)$, where # denotes “the number of” (e.g., (\# \lor) is the number of logical OR in a formula).

**Lemma 4.** For any $P, Q \in S$, there is a path from $P$ to $Q$ in the approximate minimum implication graph only if $P \Rightarrow Q$.

**Proof.** From the transitivity of $\Rightarrow$, we only need to show that if there is an edge from $P$ to $Q$ in the approximate minimum implication graph, then $P \Rightarrow Q$. This can be proved by showing $P \Rightarrow Q$ holds in each of the five cases. The first three cases are trivial. For the fourth case, in general $P = \ldots \forall X_1 X_2 \ldots$ matrix$(X_1, X_2)$ and $Q = \ldots \forall X_1 \ldots$ matrix$(X_1, X_1)$. Let $P' = \ldots \forall X_1 X_2 \ldots X_3 = X_3 \rightarrow$ matrix$(X_1, X_2)$, then $P \Rightarrow P' \Leftrightarrow Q$. Similarly, for the fifth case, $P = \ldots \exists X_1 \ldots$ matrix$(X_1, X_1) \land (\exists X_1 X_1 X_2 \ldots X_2$ matrix$(X_1, X_2)$. Let $Q' = \ldots \exists X_1 X_2 \ldots X_1 = X_2 \land$ matrix$(X_1, X_2)$, then $P \Rightarrow Q' \Rightarrow Q$.

**Lemma 5.** For any formula $P \in S$ that is not a tautology or a contradiction, there exists a directed path from a root node $Q \in S$ to $P$ in the approximate minimum implication graph.

**Proof.** We prove this by construction. For a $\exists$-free formula $P$, if it includes no logical OR, then it is a root formula itself. Otherwise, we find the root formula $Q$ by removing all but one ORed conjunctions. Starting from $Q$, we can iteratively apply the second and third cases to add conjunctions and remove literals until we reach $P$. For a $\exists$-included formula $P$, if it includes unique $\exists$-quantified variables then it is a root formula itself. Otherwise, we iteratively find a predecessor by replacing $\exists$ with $\forall$ for quantified variables of each type, until the formula becomes the $\exists$-free $P'$. The first case guarantees that there is a path from $P'$ to $P$, and we have already shown for the $\exists$-free $P'$, there exists a path from a root node $Q$. Putting it together, we have a path from $Q$ to $P$ in the approximate minimum implication graph.

In other words, the approximate minimum implication graph is as useful and complete as the exact graph. DuoAI uses the approximate minimum implication graph, which, for simplicity, we will continue to refer to as the minimum implication graph unless otherwise specified.

DuoAI requires that formulas in $S$ must be in a decidable fragment of first-order logic. In general, satisfiability in first-order logic is undecidable [23], so an SMT solver can get stuck in infinite instantiations and never give the sat/unsat answer. DuoAI ensures that the formulas are decidable by enforcing a fixed order of types if there is quantifier alternation (i.e., alternating $\forall$ and $\exists$) [1]. If type $A$ is ordered before type $B$, then for any formula, if there exists a quantified variable $V$ of type $A$, any quantified variable of type $B$ can only occur after $V$ if there is quantifier alternation. For example, if type $node$ is ordered before type $packet$, then $\forall N : node. \exists P : packet \land \exists N : node. \forall P : packet$ are allowed while $\forall P : packet. \exists N : node \land \exists P : packet. \forall N : node$ are not. DuoAI tries to infer the order of types from the protocol specification and obtains input from the user when necessary. For example, for the simplified consensus protocol, DuoAI can infer from Line 10 that type $quorum$ must be ordered before type $node$, then ask the user to place type $value$ in the order. Absent user input, DuoAI will try different possible orders in parallel.

### 4 Candidate Invariant Enumeration

Similar to DistAI [38], DuoAI first repeatedly simulates the distributed protocol using various instance sizes, and records the reached states as samples. For example, DuoAI simulates the simplified consensus protocol on concrete instances of different numbers of values, quorums, and nodes. The simulations of different instance sizes are done in parallel and yield samples of different lengths. DuoAI follows the minimum implication graph to enumerate candidate invariants, but rather than feeding all of them to an inefficient SMT solver, it checks them directly on the samples first. A correct invariant must hold on every reachable protocol state and thus on every sample. A key difference between DuoAI and DistAI is that DuoAI keeps the original variable-length samples and uses them in invariant enumeration, while DistAI projects all samples to fixed-length vectors that it calls subsamples. The problem is that DistAI is not exhaustive in its subsampling, so that a formula with existential quantifiers that holds for DistAI’s subsamples may not actually hold for the original samples. DuoAI avoids this problem by effectively considering all possible subsamples that can be derived from the original samples.

Algorithm 1 shows the enumeration algorithm, in which $pending$ is a queue whose elements are formulas that will be checked on the samples, $candidates$ is the set of formulas that hold on all the samples and $invalidated$ is the set of formulas that do not hold on at least one of the samples. Both $candidates$ and $invalidated$ are initially empty (Lines 2-3), and $pending$ initially consists of the root nodes of the minimum implication graph, that is, formulas that cannot be implied by any other formula. In each iteration, a formula $f$ is popped from the $pending$ queue (Line 5). If one of $f$’s ancestors in the graph has already been added to $candidates$, DuoAI will not check $f$ on the samples or add $f$ to the $candidates$ invariants (Lines 6-7). Oth-
with checking the inductiveness of redundant invariants. More importantly, this procedure guarantees that the resulting invariants, formulas B and F in this example, are the strongest candidate invariants that hold on the samples, which is formally stated in the following theorem:

**Theorem 1.** For any correct invariant \( I \in S \) held by the protocol \( \mathcal{P} \), at the end of invariant enumeration, either 1) \( I \in \text{candidates} \), or 2) one of \( I \)’s ancestors \( I_{\text{anc}} \in \text{candidates} \).

**Proof.** Consider three cases: 1) \( I \) has been checked on the samples, 2) \( I \) has been added to the \( \text{pending} \) queue but was not checked on samples, and 3) \( I \) has been never added to the \( \text{pending} \) queue. In the first case, since \( I \) is a correct invariant held by the protocol, it must hold on all the samples and will be added to \( \text{candidates} \) (Lines 8-9), so \( I \in \text{candidates} \). In the second case, after \( I \) is popped from the \( \text{pending} \) queue, there must be an ancestor \( I_{\text{anc}} \) of \( I \) already in \( \text{candidates} \) (Line 6), otherwise \( I \) will be checked on the samples, so \( I_{\text{anc}} \in \text{candidates} \). In the third case, we show that an ancestor \( I_{\text{anc}} \in \text{candidates} \) exists. From Lemma 5, there must be a path from a root node \( I_0 \) to \( I \), namely \( I_0, I_1, \ldots, I \). On Line 3 the root node \( I_0 \) is added to the \( \text{pending} \) queue. Since \( I_0 \) is added to the \( \text{pending} \) queue and \( I \) is not, let \( I_k \) be the last formula on the path \( I_0, I_1, \ldots, I \) that is ever added to the \( \text{pending} \) queue. After \( I_k \) is dequeued, there are three possible branches to take: Lines 6-7, Lines 8-9, or Lines 10-14. If it takes Lines 6-7, then there is an ancestor \( I_{\text{anc}} \) of \( I_k \) such that \( I_{\text{anc}} \in \text{candidates} \). If it takes Lines 8-9, then \( I_k \) will be added to \( \text{candidates} \) so \( I_k \) is the ancestor \( I_{\text{anc}} \) of \( I \) such that \( I_{\text{anc}} \in \text{candidates} \). If it takes Lines 10-14, its successors will be added to the \( \text{pending} \) queue unless the branch condition at Line 13 evaluates to false. From our hypothesis, \( I_k \) is last formula on path \( I_0, I_1, \ldots, I \) that is ever added to the \( \text{pending} \) queue. Thus, the branch condition for \( I_{k+1} \) must evaluate to false, so either \( I_{k+1} \in \text{candidates} \) or \( I_{k+1} \in \text{invalidated} \). However, \( I_{k+1} \) must be added to the \( \text{pending} \) queue before it can be added to either \( \text{candidates} \) or \( \text{invalidated} \), a contradiction.

Theorem 1 says that any correct invariant has either itself or
we refer to as top-down invariant refinement. Algorithm 2 (left). Correct invariant C is in the candidate invariants itself. For correct invariant E, its ancestor D is in the candidate invariants. Theorem 1 guarantees that \(\{B, F\}\) is not a possibility after enumeration, because for correct invariant C, neither itself nor its lone ancestor A is in the candidate invariants.

Figure 4 gives an illustration. A direct corollary is that, the set of candidate invariants after the enumeration is at least as strong as the correct invariant in \(S\).

5 Top-down Invariant Refinement

Based on Theorem 1, the candidate invariants can only be too strong, so DuoAI can monotonically weaken the candidate invariants until a correct inductive invariant is reached, which we refer to as top-down invariant refinement. Algorithm 2 shows the top-down refinement algorithm. In each iteration, DuoAI feeds the current candidate invariants to Ivy. Ivy invokes the Z3 SMT solver to check the inductiveness of each candidate invariant and the safety property. Ivy will return which invariants fail the check: if there are none, the correct inductive invariant has been found (Lines 4-5). If the safety property fails, there is no point to weaken it, and the system returns NotProvable (Lines 6-7). If one of the candidate invariants fails, DuoAI moves it from candidates to invalidated (Lines 9-10), then adds its successors (i.e., formulas that can be implied by the failed invariant) to candidates so long as the successor does not have a reachable ancestor in candidates and has not already been invalidated (Lines 12-13). An ancestor of a node is reachable if there is a path from the ancestor to the node along which no node is invalidated.

Figure 5 shows an example of top-down refinement. Suppose the current candidate invariants include formulas B and F, and by invoking the Z3 SMT solver, Ivy indicates that B is not inductive. Formulas D and E are not in candidates, because they can be implied by formula B which is already in candidates. After B is invalidated, both D and E will be added to candidates to let Ivy decide their inductiveness in future iterations. Alternatively, if formula F is invalidated by Ivy, no formula will be added to candidates because F has no successor in the minimum implication graph of search space \(S\).

By weakening failed invariants based on the minimum implication graph rather than discarding them, DuoAI can guarantee that it never overweakens invariants to bypass the correct invariants in between. In other words, top-down refinement has a theoretical guarantee to eventually find an inductive invariant if one exists in the search space, as stated in the following theorem:

Theorem 2. For any protocol \(\mathcal{P}\) and finite search space \(S\), if there exists an inductive invariant \(\mathcal{I}^*\) that can prove the safety property, then Algorithm 1 followed by Algorithm 2 will output such an inductive invariant \(\mathcal{I}^*\) in finite time.

Proof. The key is to prove that the while loop (Lines 2-13) maintains the following loop invariant: For any invariant \(I \in \mathcal{I}^*\), either 1) \(I \in \text{candidates}\), or 2) there exists a reachable ancestor \(I_{\text{anc}}\) of \(I\) such that \(I_{\text{anc}} \in \text{candidates}\). The loop invariant says that after any rounds of invariant weakening, the candidate invariants must be at least as strong as the correct invariants. If Algorithm 2 terminates, it is impossible to have the safety property fail (Line 7). The only possibility is that a correct inductive invariant is returned (Line 5).

Figure 4: Possible (left) and impossible (right) candidate invariants after enumeration. Formulas C and E are correct invariants held by the protocol. It is possible that after enumeration, candidates = \(\{C, D\}\) (left). Correct invariant C is in the candidate invariants itself. For correct invariant E, its ancestor D is in the candidate invariants. Figure 4 gives an illustration. A direct corollary is that, the set of candidate invariants after the enumeration is at least as strong as the correct invariant in \(S\).

Algorithm 2 Top-down Invariant Refinement Algorithm

Input: Distributed protocol \(\mathcal{P}\), minimum implication graph \(\mathcal{G}\), candidate invariants from enumeration \(\mathcal{CI}\)
Output: Either an inductive invariant \(\mathcal{II}\), or NotProvable

1: candidates, invalidated := \(\mathcal{CI}\), \(\emptyset\)
2: while candidatesnotEmpty() do
3: failed_inv := Ivy_check(\(\mathcal{P}\), candidates)
4: if failed_inv is None then
5: return candidates
6: else if failed_inv = safety_property then
7: return NotProvable
8: else
9: candidates := candidates \ \{failed_inv\}
10: invalidated := invalidated \ \{failed_inv\}
11: for next_inv in graph.successors(failed_inv) do
12: if graph.reachable_ancestors(next_inv) \ \{failed_inv\} candidates = \emptyset and next_inv \ \{next_inv\} invalidated then
13: candidates := candidates \ \{next_inv\}
14: return NotProvable
not on the path from \(I_{\text{anc}}\) to \(I\). If it is not on the path, \(I_{\text{anc}}\) remains a reachable ancestor of \(I\) and \(I_{\text{anc}} \in \text{candidates}\) still holds at the beginning of iteration \(k+1\). If it is on the path, let \(I_0\) be the successor of the invalidated invariant on the path. From Lines 11-13, either \(I_0\) is added to \(\text{candidates}\), in which case \(I_0\) can be the new \(I_{\text{anc}}\) for iteration \(k+1\), or \(I_0\) has a reachable ancestor \(I_0 \in \text{candidates}\), in which case we choose \(I_0\) as the new \(I_{\text{anc}}\) for iteration \(k+1\). In all cases, we can find either \(I\) or a reachable ancestor \(I_{\text{anc}}\) in the candidate set, therefore the loop invariant holds.

Now we only need to prove that Algorithm 2 terminates, which follows from three observations: 1) In each loop iteration a formula is removed from \(\text{candidates}\) (Line 9); 2) each formula can only be added to \(\text{candidates}\) once (Lines 10 & 12); and 3) the formula search space \(\mathcal{S}\) is finite.

6 Bottom-up Invariant Refinement

Although top-down refinement provides a strong theoretical guarantee of finding an inductive invariant, it may take too long or run out of memory given limited computing resources if there are too many unnecessary invariants to consider. For the simplified consensus protocol in Figure 1, besides the four invariants (1)(2)(3)(4), many other invariants hold for the protocol but are unnecessary to prove the inductiveness of the safety property, for example,

\[
\forall V : \text{value}, Q : \text{quorum}. \exists N : \text{node}.
\]

\[
\text{member}(N, Q) \land (\text{leader}(N) \lor \neg \text{decided}(N, V)). \quad (10)
\]

Invariants such as Eq. (10) do not affect the soundness of DuoAI, but they will significantly slow down the validation of candidate invariants by the SMT solver. If there are \(m\) candidate invariants, validating each invariant takes \(O(m)\) time in the worst case, since the inductiveness of one invariant can depend on any other invariant, so checking all candidate invariants can take \(O(m^2)\) time. Adding unnecessary invariants can increase validation time quadratically.

The key issue though is not just how many unnecessary invariants there are, but whether they have quantifier alternation (i.e., alternating \(\forall\) and \(\exists\)), which we observe causes

---

**Algorithm 3: Bottom-up Invariant Refinement Algorithm**

**Input:** Distributed protocol \(\mathcal{P}\), minimum implication graph \(\mathcal{G}\), candidate invariants from enumeration \(\mathcal{I}\)

**Output:** Either an inductive invariant \(\mathcal{I}\), or NotProvable

**Procedure 1**
1: \(\mathcal{I}_\ell := \{I \mid I \in \mathcal{I} \land I \text{ is } \exists\text{-free}\}\)
2: \(\text{core} := \text{Algorithm2}(\mathcal{P}, \mathcal{G}, \mathcal{I}_\ell)\)
3: \(\text{noncore} := \mathcal{I} \setminus \text{core}\)

**Procedure 2**
4: \(CE := \emptyset\)
5: for sub in powerset(noncore) do
6: \(\text{if } \exists x \in CE \text{. invs\_hold\_on\_state}(\text{sub}, x) \text{ then}
7: \(\text{continue}\)
8: \(\text{result} := \text{Algorithm2}(\mathcal{P}, \mathcal{G}, \text{core})\)
9: \(\text{if result} = \text{NotProvable} \text{ then}
10: \(s \vdash s':= \text{get\_counterexample}()\)
11: \(CE := CE \cup \{s\}\)
12: \(\text{else}\)
13: \(\text{return result}\)
14: \(\text{return NotProvable}\)

SMT solvers to struggle. For the Paxos protocol, a correct inductive invariant set of size 14 can be validated in less than a second. If we add 10 correct but unnecessary invariants with quantifier alternation, the validation will take 5 minutes. If we add 20 such invariants, the validation will take over 3 hours. In contrast, the chord ring maintenance protocol [21] with 149 \(\forall\)-only invariants only takes 8 seconds to validate.

However, a correct distributed protocol typically has a clear and human-understandable intuition, which leads to concise invariants [10]. This motivates our bottom-up invariant refinement algorithm shown in Algorithm 3. In essence, the algorithm tries to identify a small set of correct and helpful invariants that can eventually prove the safety property. §8 shows that the combination of bottom-up with top-down refinement provides fast performance for finding inductive invariants across a wide-range of protocols.

Algorithm 3 consists of two procedures. In Procedure 1, DuoAI first extracts all the \(\forall\)-only invariants from the candidate invariants (Line 1), which are guaranteed to be the strongest \(\forall\)-only invariants that hold on the samples. Then, DuoAI runs the top-down refinement algorithm (Line 2) using only the universal invariants and the universal portion of the minimum implication graph by removing all nodes representing existentially quantified formulas. The safety property is neglected in this top-down refinement. In this way, the \(\forall\)-only invariants are monotonically weakened until they become inductive, regardless of whether the safety property can be proved (it probably cannot).

Recall that we call the now inductive \(\forall\)-only invariants the universal inductive core. DuoAI then puts every enumerated candidate invariant that is not in the universal inductive core
into noncore (Line 3). noncore mainly consists of formulas with existential quantifiers, but also includes ∀-only formulas that are not in the core, whose inductiveness may depend on ∃-included invariants. For example, for the simplified consensus protocol, the universal inductive core includes five candidate invariants, which are exactly the equivalent forms of Eq. (1), (2), and (4). There are 14 non-core candidate invariants, 13 of which have quantifier alternation, including Eq. (3) and (10).

Based on our observation that SMT solvers struggle with quantifier alternation, we expect noncore formulas will have a much higher cost of checking. Procedure 2 aims to identify a small subset of noncore to strengthen the candidate invariants, such that the conjunction of the universal inductive core and the subset (denoted as \( \text{core} \cup \text{sub} \)), or their weaker forms, can prove the safety property. Procedure 2 enumerates each subset \( \text{sub} \) of noncore (Line 5), and runs the monotonic weakening algorithm (Algorithm 2) on \( \text{core} \cup \text{sub} \) (Line 8). If Algorithm 2 returns NotProvable (Line 9), DuoAI moves on to consider the next subset. Otherwise, Algorithm 2 outputs a correct inductive invariant (Line 13). The enumeration of subsets is conducted in increasing order of size, starting from the \( \emptyset \), followed by all single formulas from noncore, then pairs, triples, and so on. Whenever Algorithm 2 finds the safety property failed and reports NotProvable, Ivy returns a counterexample of inductiveness \( s \not\rightarrow s' \) (Line 10), which means starting from a protocol state \( s \) satisfying the safety property and the candidate invariants, and taking an action \( a \), the system reaches a new state \( s' \) where the safety property is violated.¹

If we view the samples from protocol simulation as positive samples on which the invariants must hold, then we can view these counterexample states \( s \) as negative samples which the invariants must exclude. DuoAI needs to identify and include another invariant \( I \) that does not hold on \( s \), so that the counterexample \( s \not\rightarrow s' \) can be excluded. When enumerating a subset of noncore, Procedure 2 first checks if the subset can exclude all counterexamples seen so far (Line 6). If there exists one counterexample state \( s \) on which all invariants in the subset hold, or in other words, the counterexample cannot be excluded, the monotonic weakening algorithm is bound to fail, because if a stronger invariant cannot exclude the counterexample, then its weaker forms cannot either. So Procedure 2 simply moves on to enumerate the next subset (Line 7).

For the simplified consensus protocol, when \( sub = \emptyset \), the safety property fails and Ivy gives the counterexample \( s = \{ \text{vote}(n_1,n_1) = \text{vote}(n_1,n_2) = \text{vote}(n_2,n_1) = \text{vote}(n_2,n_2) = \text{false}, \text{voted}(n_1) = \text{voted}(n_2) = \text{false}, \text{leader}(n_1) = \text{true}, \text{member}(n_1,q) = \text{member}(n_2,q) = \text{true}, \text{decided}(n_2,v_1) = \text{true}, \text{decided}(n_1,v_1) = \text{decided}(n_1,v_2) = \text{decided}(n_2,v_2) = \text{false} \} \). Eq. (3) does not hold on \( s \), so it can exclude this counterexample. In contrast, Eq. (10) holds on \( s \), so the counterexample will persist even if Eq. (10) is added to the candidate set. Therefore, DuoAI will skip Eq. (10) and try Eq. (3), and run Algorithm 2 on its conjunction with the universal core, which gives a correct inductive invariant set consisting of Eq. (1)(2)(3)(4).

Although counterexamples can be used for top-down refinement, DuoAI currently does not because Ivy cannot return counterexamples in batch. When Ivy is configured to return a counterexample, it terminates once it identifies the first broken invariant. This is inefficient for top-down refinement, but for bottom-up refinement, counterexamples are only needed for the safety property, so DuoAI puts the safety property on top of other invariants and Ivy will give the desired counterexample.

Like top-down refinement, bottom-up refinement has a theoretical guarantee to eventually find an inductive invariant if one exists in the search space, as stated in the following theorem:

**Theorem 3.** For any protocol \( \mathcal{P} \) and finite search space \( S \), if there exists an inductive invariant \( I^* \subset S \) that can prove the safety property, then Algorithm 1 followed by Algorithm 3 will output such an inductive invariant \( I^* \) in finite time.

**Proof.** We first prove that Algorithm 3 terminates in finite time. This directly follows from three facts: 1) \( \text{powerset}(\text{noncore}) \) is a finite set so the for loop (Line 5) has a finite number of iterations; 2) In each loop iteration, there is at most one invocation of Algorithm 2 (Line 8); and 3) From Theorem 2, Algorithm 2 terminates in finite time.

To prove the soundness of Algorithm 3, we first observe that if Algorithm 3 outputs an invariant, it must be a correct inductive invariant, because the output must come from Algorithm 2, in which the output can only occur when the safety property is proved.

Now we prove that there will be an output invariant eventually. Observe that \( \text{noncore} \in \text{powerset}(\text{noncore}) \) (Line 5), When \( sub = \text{noncore} \), we have \( C \subset \text{core} \cup \text{sub} \), then Line 8 degenerates to Algorithm 2 in §5. From Theorem 2, we know a correct inductive invariant will be outputted.

For both the top-down and bottom-up refinement, if NotProvable is returned, we know the protocol cannot be verified using invariants in the search space \( S \). DuoAI will try a larger search space by increasing either max_{\text{literal}}, max_{\text{or}}, max_{\text{and}}, or max_{\text{exists}}, or the per-domain number of quantified variables. By default, DuoAI alternates among the five in a round-robin manner. DuoAI sets the initial max_{\text{literal}} = 4, max_{\text{or}} = max_{\text{and}} = 3, and max_{\text{exists}} = 1 unless the safety property already involves \( k \geq 2 \) existentially quantified variables, in which case DuoAI sets max_{\text{exists}} = \( k \). DuoAI sets the initial number of quantified variables for domain \( T \) as the maximum number of variables of type \( T \) in any relation. For example, the relation \( \text{vote}(N_1:n_{\text{node}}, N_2:n_{\text{node}}) \) guarantees type \( n_{\text{node}} \) has at least two variables.

Because SMT solvers are much less efficient at checking invariants with existential quantifiers, and many distributed protocols are provable by \( \forall \)-only invariants [21], DuoAI runs
7 Optimizations Based on Mutual Implication

In using the minimum implication graph, DuoAI introduces several optimizations based on mutual implication relations among formulas. These relations further prune the search space and avoid redundant candidate invariants. DuoAI considers two kinds of mutual implication relations, 1) \( P_1 \land P_2 \land \ldots \land P_k \Rightarrow Q \), and 2) \( P_1 \land P_2 \land \ldots \land P_k \Leftrightarrow Q \). Although the latter is a special case of the former, DuoAI treats them differently. We refer to \( Q \) as a conjunction implied formula in the former and an equivalently decomposable formula in the latter. Since checking inductiveness has a quadratic complexity with the number of invariants, these optimizations have a significant improvement on efficiency.

Conjunction implied formulas. DuoAI identifies conjunction implied formulas to avoid redundant candidate invariants. Given a mutual implication relation \( P_1 \land P_2 \land \ldots \land P_k \Rightarrow Q \), if all \( P_1, P_2, \ldots, P_k \) are already in the candidate invariants, DuoAI will mark \( Q \) as a conjunction implied formula and not add \( Q \) to the candidate invariants. Later during refinement, if one of \( P_1, P_2, \ldots, P_k \) is invalidated by Ivy, then the conjunction implied invariant \( Q \) is no longer redundant and will be added to the candidate invariants.

One can check that among Eq. (11)(12)(13), no formula can imply another. But the conjunction of Eq. (11) and (12) can imply Eq. (13). This is because Eq. (12) says that for every epoch \( E \), there must be a readable replica \( R \). Then from Eq. (11), the readable replica \( R \) cannot be crashed. Therefore, for every epoch \( E \), there must be a replica \( R \) that does not crash, which is expressed by Eq. (13). If Eq. (11) and (12) are already candidate invariants, DuoAI will mark Eq. (13) as a conjunction implied formula and not add it to the candidate invariants.

There are many classes of mutual implication relations in first-order logic. DuoAI identifies three classes of conjunction implied formulas to prune candidate invariants; in each class, the first two formulas mutually imply the third:

1. Replace a literal with a weaker literal, as discussed in the example Eq. (11)(12)(13):
   \[
   \begin{align*}
   P_1 &= \forall X. r(X) \rightarrow s(X) \\
   P_2 &= \text{prefix.} \ (r(X) \land \ldots) \lor \ldots \\
   Q &= \text{prefix.} \ (s(X) \land \ldots) \lor \ldots
   \end{align*}
   \]

2. Conjure a literal with a weaker literal:
   \[
   \begin{align*}
   P_1 &= \forall X. r(X) \rightarrow s(X) \\
   P_2 &= \text{prefix.} \ (r(X) \land \ldots) \lor \ldots \\
   Q &= \text{prefix.} \ (s(X) \land \ldots) \lor \ldots
   \end{align*}
   \]

3. “Merge” a \( \forall \) formula and an \( \exists \) formula:
   \[
   \begin{align*}
   P_1 &= \exists X. r(X) \\
   P_2 &= \forall X. s(X) \lor \ldots \\
   Q &= \exists X. (r(X) \land s(X)) \lor \ldots
   \end{align*}
   \]

In all three classes, \( r \) and \( s \) can be generalized to conjunctions (e.g., \( r_1(X) \land \neg r_2(X), \neg s_1(X) \land s_2(X) \land s_3(X) \)). A key advantage of this optimization is that given a finite search space, DuoAI can identify conjunction implied formulas based on invariants within that search space, even though the conjunction of invariants is not in that search space.

Equivalently decomposable formulas. DuoAI also identifies equivalently decomposable formulas to avoid redundant candidate invariants. Given a mutual implication relation \( P_1 \land P_2 \land \ldots \land P_k \Leftrightarrow Q \), DuoAI will mark \( Q \) as an equivalently decomposable formula and never add \( Q \) to the candidate invariants. Later during refinement, if one of \( P_1, P_2, \ldots, P_k \) is invalidated by Ivy, \( Q \) will also be invalidated and therefore there is never any reason to consider \( Q \) further as a candidate invariant.

For example, suppose the disk replication protocol has invariant:

\[
\forall E: \text{epoch.} \ \exists R_1, R_2: \text{replica.}
\]

\[
\text{readable}(E, R_1) \land \neg \text{writable}(E, R_2).
\]

There is no need to ever include such an invariant in the candidate set, because it is equivalently decomposable to invariants (15) and (16).

\[
\forall E: \text{epoch.} \ \exists R: \text{replica. readable}(E, R).
\]

\[
\forall E: \text{epoch.} \ \exists R: \text{replica. writable}(E, R).
\]

However, suppose we slightly modify invariant (14) to one of the following two formulas:

\[
\forall E: \text{epoch.} \ \exists R_1: \text{replica.}
\]

\[
\text{readable}(E, R_1) \land \neg \text{writable}(E, R_1).
\]

\[
\forall E: \text{epoch.} \ \exists R_1, R_2: \text{replica.}
\]

\[
R_1 \neq R_2 \land \text{readable}(E, R_1) \land \neg \text{writable}(E, R_2).
\]

These invariants are not equivalently decomposable to invariants (15) and (16). Take Eq. (17) as an example. One can verify that (17) \( \Rightarrow (15) \land (16) \), but (15) \( \land (16) \neq (17) \), because Eq. (17) requires the same replica to be both readable and writable, while for Eq. (15) and (16), it is possible to have one readable replica and a different writable replica.

DuoAI identifies if a formula is equivalently decomposable based on the structure of the formula itself by considering two classes of equivalently decomposable formulas. One class is embodied by the following lemma:
Lemma 6. For a formula $F$ in prenex and disjunctive normal form, we build a graph $G_C$ for each conjunction $C$ in $F$. $G_C$ has one node for each literal, and an edge between two literals if and only if they share an existentially quantified variable. If for some $C$ in $F$, the graph $G_C$ has $k \geq 2$ connected components, then $F$ is equivalently decomposable into $k$ formulas.

Proof. For simplicity, here we show the proof for $k = 2$ (i.e., the literals in $C$ form two connected components). If there are $k > 2$ connected components, then the same analysis below will show that formula $F$ is equivalently decomposable into $k$ formulas.

Literals that share $3$-variables must be in the same connected component. So we can divide the $3$-variables into two sets $\{Y_1, ..., Y_m\}$ and $\{Z_1, ..., Z_n\}$. The first connected component can only include $3$-variables $Y_1, ..., Y_m$, while the second can only include $Z_1, ..., Z_n$. Assume the quantifier prefix has shape $\forall X_1 ... X_r \exists Y_1 ... Y_m \exists Z_1 ... Z_n$. We use $X, Y, Z$ to denote $X_1 ... X_r$, $Y_1 ... Y_m$, and $Z_1 ... Z_n$. The proof can be generalized to any alternating $\forall \exists$ using skolemization.

Let $f(X, Y)$ be the disjunction of literals in the first connected component, and $g(X, Z)$ be the disjunction of literals in the second connected component. Let $h(X, Y, Z)$ be the disjunction of all conjunctions other than $C$ in formula $F$.

Then formula $F$ can be rewritten as:

$$\forall X \exists Y \exists Z. (f(X, Y) \lor g(X, Z)) \lor h(X, Y, Z).$$

We now show that, Eq. (19) is equivalently decomposable into:

$$\forall X \exists Y \exists Z. f(X, Y) \lor h(X, Y, Z)$$

and

$$\forall X \exists Y \exists Z. g(X, Z) \lor h(X, Y, Z).$$

It is trivial that Eq. (19) implies both Eq. (20) and (21). We now show the interesting direction — the conjunction of Eq. (20) and (21) implies Eq. (19). Suppose both Eq. (20) and (21) hold. For any $X$, consider two cases: 1) $\exists Y \exists Z. h(X, Y, Z)$. In this case Eq. (19) directly holds. 2) $\forall Y \exists Z. \neg h(X, Y, Z)$. Then according to Eq. (20), $\forall Y \exists Z. f(X, Y)$. Similarly, from Eq. (21), $\exists Y \exists Z. g(X, Z)$. If we select $Y_1$ and $Z_2$, then we have $f(X, Y_1) \land g(X, Z_2)$, so Eq. (19) still holds. Putting the two cases together, when both Eq. (20) and (21) are true, Eq. (19) must be true.

The proof also gives an algorithm to find the $k$ decomposed formulas. Figure 6 shows how to apply Lemma 6 on the aforementioned formulas. For Eq. (14), the two literals $\text{readable}(E, R_1)$ and $\text{writeable}(E, R_2)$ share no $3$-quantified variable ($E$ is $\forall$-quantified), so there is no edge between the two literals. The graph has two connected components, so Eq. (14) is equivalently decomposable into two formulas (Eq. (15)(16)).

For Eq. (17), the two literals share an $3$-quantified variable $R_1$, so there is an edge between the two literals and the graph is connected, which means Eq. (17) cannot be decomposed in this way. The same analysis can be applied to Eq. (18).

We note a corollary of Lemma 6. For an $3$-free formula, it is equivalently decomposable if it has any conjunction.
the instance size upon failure (e.g., node = 2, node = 3, \ldots). FOL-IC3 provides a $\forall$-only mode and a default mode. We ran both and report the runtime of whichever succeeded first.

Results summary. Table 1 shows the running time in seconds for each tool on each protocol. For each protocol, we also report the number of relations and lines of code in its Ivy specification; for example, Figure 1 is a simplified version of consensus epr. The top portion of the table shows protocols provable with a $\forall$-only inductive invariant, while the bottom portion shows protocols that can only be proved with a $\exists$-included inductive invariant. We allowed each tool to spend up to an entire week trying to solve each protocol. For protocols that a tool fails to solve, we report “fail” if the tool terminated without an inductive invariant, “error” if the tool itself returned an error, “Z3 error” if the underlying SMT solver used returned an error, “memout” if the tool ran out of memory and terminated, and “timeout” if the tool did not complete within a week.

DuoAI dominates all other tools in the number of protocols it solves, solving all but 1 of the 27 protocols. SWISS cannot solve 8 protocols, FOL-IC3 and IC3PO cannot solve 9 protocols, DistAI and UPDR cannot solve 13 protocols, while I4 cannot solve 15 protocols. DuoAI is the only tool that solves all $\forall$-only protocols, is the only tool that solves Paxos as well as all other non-Paxos protocols with $\exists$ quantifiers, and is the only tool that solves 3 of the more complex Paxos variants, including multi-Paxos, stoppable Paxos, and fast Paxos. There were no protocols solvable by another tool that were not solved by DuoAI.

DuoAI also dominates all other tools in how fast it solves the protocols, solving 15 of the protocols faster than any other tool. DuoAI is faster than SWISS on all but 3 of the protocols solved by SWISS, is faster than IC3PO on all but 3 of the protocols solved by IC3PO, is faster than FOL-IC3 on all but 2 of the protocols solved by FOL-IC3, and is faster than UPDR on all of the protocols solved by UPDR. DuoAI is up to 3 orders of magnitude faster than each of these protocols. DuoAI is faster than DistAI on all but 5 of the protocols solved by DistAI, and is faster than I4 on all but 2 of the protocols solved by I4. DuoAI is up to an order of magnitude faster than either DistAI or I4. The speed differences versus DistAI and I4 appear less in part because neither could solve any of the protocols with existential quantifiers. In most cases in which DuoAI is slower than other protocols, it is by at most a few seconds.

Detailed comparison and discussion. For the protocols provable with $\forall$-only invariants, DuoAI is the only tool that solves all 15 protocols. On $\forall$-only protocols, DuoAI’s $\forall$-only instance is similar to DistAI, without subsampling and with mutual implication optimization and parallelism in simulation. DuoAI beats DistAI on 10 protocols. Unlike DuoAI, DistAI times out on ticket lock, which we discovered is due to a bug in the implementation of its protocol simulation. Chord ring maintenance is the only protocol on which DuoAI is much slower than DistAI. DistAI only allows invariants as disjunction of literals, and implements an invariant as a set<vector<int>>. In contrast, DuoAI considers invariants in disjunctive normal form, so an invariant is a disjunction of conjunction of literals, implemented as a set<vector<int>>. This makes invariant operation slower in DuoAI. Chord ring maintenance is the only $\forall$-provable protocol that takes significant time on candidate invariant enumeration so the overhead is exacerbated.

For the protocols that require invariants with $\exists$-quantifiers to prove, DuoAI solves 11 out of 12 protocols, more than any other tool. DuoAI only fails on vertical paxos, which other tools also fail on. DistAI, I4, and UPDR fail on all of these protocols because they can only generate $\forall$-only invariants. IC3PO solves 4 protocols and fails on 3 protocols, but runs out of memory on 6 protocols, because it requires model checking to infer invariants on a finite instance. For more complex protocols like fast Paxos, the model checker requires too large of an instance size. In contrast, DuoAI searches in formula space and its performance does not depend (exponentially) on instance size.

For the complex Paxos-family protocols, only SWISS also verified Paxos and flexible Paxos, though it required several hours to do so. All other tools failed on all Paxos-family protocols. In contrast, DuoAI verified Paxos and flexible Paxos in less than 2 minutes. Only DuoAI verified multi-Paxos, stoppable Paxos, and fast Paxos.

As the only other tool that solves Paxos, it is instructive to compare SWISS with DuoAI. Similar to DuoAI, SWISS also enumerates candidate invariants given a bounded search space and checks their inductiveness using the SMT solver. However, it has two fundamental differences compared with DuoAI. First, SWISS relies exclusively on the SMT solver to tell the correctness of invariants, while DuoAI also uses the samples from protocol simulation to filter out invalid invariants. As we demonstrated in §6, SMT calls can be expensive with quantifier alternation and will negatively affect performance. Second, SWISS struggles to find mutually inductive invariants, i.e., a bundle of invariants that are inductive together but none are inductive individually. This is because SWISS can only build the invariant set by adding one and only one invariant each time and keep the set inductive. In the lock server async and the sharded key-value store protocols, where mutually inductive invariants are required to prove the safety property, SWISS has to manually increase the maximum number of literals from 6 to 9. This allows the mutually inductive invariants to be conjuncted into one big invariant, but results in a much larger search space and long runtimes of 44 and 128 minutes, respectively. DuoAI enumerates candidate invariants following the minimum implication graph and generates the strongest candidate invariants. The mutually inductive invariants (or their stronger forms) are guaranteed to be in the candidate invariants together. DuoAI solved both protocols within 2 seconds.

For the vertical paxos protocol, the human-expert inductive invariants include an invariant with 8 literals. Even after the optimization based on mutual implication, it still has 7
<table>
<thead>
<tr>
<th>Distributed protocol</th>
<th>Relations</th>
<th>LoC</th>
<th>DuoAI</th>
<th>SWISS</th>
<th>IC3PO</th>
<th>FOL-IC3</th>
<th>DistAI</th>
<th>UPDR</th>
<th>I4</th>
</tr>
</thead>
<tbody>
<tr>
<td>chord ring maintenance</td>
<td>8</td>
<td>123</td>
<td>200.9</td>
<td>timeout</td>
<td>17.1</td>
<td>timeout</td>
<td>58.0</td>
<td>Z3</td>
<td>673</td>
</tr>
<tr>
<td>consensus forall</td>
<td>7</td>
<td>55</td>
<td>11.9</td>
<td>40.3</td>
<td>457</td>
<td>1500</td>
<td>15.6</td>
<td>59.0</td>
<td>122</td>
</tr>
<tr>
<td>consensus wo decide</td>
<td>6</td>
<td>46</td>
<td>3.9</td>
<td>26.1</td>
<td>160</td>
<td>24.8</td>
<td>8.5</td>
<td>24.8</td>
<td>27.5</td>
</tr>
<tr>
<td>database chain replication</td>
<td>13</td>
<td>96</td>
<td>9.5</td>
<td>108951</td>
<td>4.5</td>
<td>559</td>
<td>90.3</td>
<td>57.6</td>
<td>66.6</td>
</tr>
<tr>
<td>decentralized lock</td>
<td>2</td>
<td>21</td>
<td>9.9</td>
<td>5.8</td>
<td>24.3</td>
<td>69.0</td>
<td>10.2</td>
<td>51.0</td>
<td>20.7</td>
</tr>
<tr>
<td>distributed lock</td>
<td>4</td>
<td>43</td>
<td>6.1</td>
<td>timeout</td>
<td>12856</td>
<td>1660</td>
<td>15.3</td>
<td>63568</td>
<td>195</td>
</tr>
<tr>
<td>ring leader election</td>
<td>3</td>
<td>45</td>
<td>3.5</td>
<td>14.3</td>
<td>memout</td>
<td>10.8</td>
<td>2.9</td>
<td>103</td>
<td>5.3</td>
</tr>
<tr>
<td>learning switch ternary</td>
<td>4</td>
<td>45</td>
<td>14.2</td>
<td>308</td>
<td>23.8</td>
<td>timeout</td>
<td>24.7</td>
<td>1334</td>
<td>12.9</td>
</tr>
<tr>
<td>learning switch quad</td>
<td>2</td>
<td>21</td>
<td>52.4</td>
<td>1322</td>
<td>63.6</td>
<td>timeout</td>
<td>372</td>
<td>273</td>
<td>memout</td>
</tr>
<tr>
<td>lock server async</td>
<td>5</td>
<td>45</td>
<td>1.9</td>
<td>2625</td>
<td>5.6</td>
<td>4.8</td>
<td>1.1</td>
<td>4.4</td>
<td>8.7</td>
</tr>
<tr>
<td>lock server sync</td>
<td>2</td>
<td>21</td>
<td>1.3</td>
<td>1.0</td>
<td>3.2</td>
<td>1.0</td>
<td>0.9</td>
<td>3.3</td>
<td>0.6</td>
</tr>
<tr>
<td>sharded key-value store</td>
<td>3</td>
<td>31</td>
<td>1.9</td>
<td>7662</td>
<td>5.4</td>
<td>9.7</td>
<td>1.2</td>
<td>3.5</td>
<td>error</td>
</tr>
<tr>
<td>ticket lock</td>
<td>5</td>
<td>49</td>
<td>23.9</td>
<td>fail</td>
<td>56.2</td>
<td>58.1</td>
<td>timeout</td>
<td>143</td>
<td>fail</td>
</tr>
<tr>
<td>toy consensus forall</td>
<td>4</td>
<td>27</td>
<td>1.9</td>
<td>5.9</td>
<td>3.0</td>
<td>5.4</td>
<td>3.1</td>
<td>3.4</td>
<td>9.4</td>
</tr>
<tr>
<td>two-phase commit</td>
<td>7</td>
<td>70</td>
<td>1.5</td>
<td>9.1</td>
<td>4.7</td>
<td>4.8</td>
<td>2.0</td>
<td>9.4</td>
<td>10.2</td>
</tr>
<tr>
<td>client server ae</td>
<td>4</td>
<td>28</td>
<td>1.5</td>
<td>5.2</td>
<td>2.3</td>
<td>355</td>
<td>timeout</td>
<td>fail</td>
<td>fail</td>
</tr>
<tr>
<td>client server db ae</td>
<td>7</td>
<td>48</td>
<td>3.1</td>
<td>33.7</td>
<td>memout</td>
<td>4822</td>
<td>timeout</td>
<td>fail</td>
<td>fail</td>
</tr>
<tr>
<td>consensus epr</td>
<td>7</td>
<td>52</td>
<td>4.8</td>
<td>28.8</td>
<td>1118</td>
<td>471</td>
<td>timeout</td>
<td>fail</td>
<td>memout</td>
</tr>
<tr>
<td>hybrid reliable broadcast</td>
<td>12</td>
<td>120</td>
<td>1211.2</td>
<td>fail</td>
<td>memout</td>
<td>931</td>
<td>error</td>
<td>fail</td>
<td>error</td>
</tr>
<tr>
<td>sharded kv no lost keys</td>
<td>3</td>
<td>32</td>
<td>2.1</td>
<td>1.8</td>
<td>4.8</td>
<td>3.7</td>
<td>timeout</td>
<td>fail</td>
<td>error</td>
</tr>
<tr>
<td>toy consensus epr</td>
<td>4</td>
<td>25</td>
<td>2.6</td>
<td>4.3</td>
<td>2.4</td>
<td>32.9</td>
<td>timeout</td>
<td>fail</td>
<td>fail</td>
</tr>
<tr>
<td>Paxos</td>
<td>9</td>
<td>75</td>
<td>60.4</td>
<td>16665</td>
<td>fail</td>
<td>timeout</td>
<td>timeout</td>
<td>timeout</td>
<td>memout</td>
</tr>
<tr>
<td>flexible Paxos</td>
<td>10</td>
<td>77</td>
<td>78.7</td>
<td>28337</td>
<td>memout</td>
<td>timeout</td>
<td>fail</td>
<td>memout</td>
<td></td>
</tr>
<tr>
<td>multi-Paxos</td>
<td>10</td>
<td>91</td>
<td>1549</td>
<td>timeout</td>
<td>fail</td>
<td>timeout</td>
<td>timeout</td>
<td>timeout</td>
<td>memout</td>
</tr>
<tr>
<td>stoppable Paxos</td>
<td>11</td>
<td>118</td>
<td>4051</td>
<td>error</td>
<td>fail</td>
<td>error</td>
<td>timeout</td>
<td>error</td>
<td>error</td>
</tr>
<tr>
<td>fast Paxos</td>
<td>12</td>
<td>102</td>
<td>26979</td>
<td>timeout</td>
<td>memout</td>
<td>memout</td>
<td>timeout</td>
<td>fail</td>
<td>error</td>
</tr>
<tr>
<td>vertical Paxos</td>
<td>12</td>
<td>120</td>
<td>memout</td>
<td>memout</td>
<td>memout</td>
<td>memout</td>
<td>error</td>
<td>fail</td>
<td>error</td>
</tr>
</tbody>
</table>

| Notes: c The SWISS authors reported that FOL-IC3 solved chord ring maintenance [10], but we found that the chord.pyv file they used has 3 bugs. i The IC3PO authors [8, 9] reported that IC3PO succeeded on client server db ae (17 s), hybrid reliable broadcast (587 s), Paxos (568 s), and flexible Paxos (561 s). However, they retrofitted the protocols and manually provided clauses with quantifier alternation that could appear in the invariants, which is difficult to do without first knowing the ground-truth invariants. The 4 protocols have much simpler inductive invariants when expressed on top of these clauses, with all except the simplest, client server db ae, becoming quantifier-free. Ivy fails when checking the invariants generated by IC3PO for Paxos and flexible Paxos. The IC3PO authors [9] imply that the invariants had to be manually checked against the human-expert invariants. |

Table 1: Comparison of different tools for finding inductive invariants for 27 distributed protocols (running time in seconds).
small subset of noncore invariants conjuncted with the $\forall$-only core are fed to Ivy, so the Z3 SMT solver could handle the candidate invariants. For Paxos, flexible Paxos, multi-Paxos, and stoppable Paxos, a subset of size 2 were sufficient, while a subset of size 6 was needed for fast Paxos. This also validates our assumption that real-world distributed protocols should have concise invariants, and should not require too many invariants with quantifier alternation to verify.

**Limitations** By requiring quantifier alternation to conform to a fixed order of types, DuoAI ensures that the verification condition is in a decidable fragment of first-order logic. However, without decidability, an SMT solver may still succeed. For client server db ae and hybrid reliable broadcast, the invariants written by human experts are not in a decidable fragment, yet they can be efficiently verified by the SMT solver. For both protocols, DuoAI found alternative inductive invariants within the decidable fragment. If a protocol cannot be verified in decidable logic, DuoAI will fail to prove it.

9 Related Work

Many studies [11, 17, 20, 31, 34–36] verify the correctness of distributed protocols with manually given inductive invariants. Early systems [12, 21, 29, 38] for automatically inferring inductive invariants do not work for invariants with $\exists$-quantifiers which are required for protocols such as Paxos, though pdH [29] can find inductive invariants for retrofitted Paxos-family protocols without $\exists$-quantifiers.

Recent systems consider invariants with $\exists$-quantifiers. FOL-IC3 [13] generates an invariant candidate that can separate a positive and negative example set, and iteratively adds more examples until the invariant is correct. It has no theoretical guarantee of success. Its heavy use of SMT queries to validate as well as synthesize invariants makes it slow in practice, timing out on even protocols with $\forall$-only inductive invariants.

SWISS [10] iteratively strengthens an invariant by adding small inductive formulas until the invariant is strong enough to prove the safety property. It was the first tool to automatically verify Paxos. Its inefficiency in exploring the search space and inability to infer mutually inductive invariants make it fail on several protocols solved by alternative tools.

IC3PO [8, 9] applies model checking on a finite instance similar to I4, while adding support to generalize existentially quantified invariants. The model checker functions well on small instances, but frequently exhausts memory on complex protocols that require larger instances, as shown in Table 1.

P-FOL-IC3 [14] is concurrent work that extends FOL-IC3 by exploiting parallelism in formula search, introducing the invariant-friendly k-Term Pseudo-DNF to bound the search space, and randomly guessing some not-yet-inductive formulas to be eventually inductive, forcing their counterexamples to be excluded. P-FOL-IC3 has no theoretical guarantee and is less robust in practice due to its randomized nature; it failed in three out of five trials on stoppable Paxos, and two out of five trials on fast Paxos.

The tools discussed above, along with DuoAI, only verify safety properties of distributed protocols. Complementary work has explored connecting verification of protocols to their practical implementations [11, 31], and verifying liveness properties of distributed protocols [26].

AutoML [5, 18, 33] searches for machine learning models and hyperparameters, which may appear similar to finding inductive invariants. However, the inductiveness of invariants has strong correlation, which is difficult to capture for AutoML.

Many automated invariant inference tools have been built for other domains, mostly on learning loop invariants to verify sequential programs [3, 4, 6, 7, 15, 24, 25, 30, 32, 37, 39]. Invariant inference has been used to prove properties on inductive algebraic data types [16, 22], integer linear dynamical systems [19], and deep neural networks [2]. None of these methods consider nondeterminism in concurrent or distributed settings, thus they cannot be directly applied to distributed protocols.

10 Conclusions

DuoAI automatically and efficiently infers inductive invariants for verifying distributed protocols by reducing SMT costs. It introduces the minimum implication graph to define the structure of the invariant search space. This enables efficient enumeration of possible invariants, which are checked on samples from protocol simulation to reduce SMT queries. DuoAI guarantees that the enumerated candidate invariants are at least as strong as any correct invariants. DuoAI then runs top-down and bottom-up refinement in parallel. The former monotonically weakens the candidate invariants following the minimum implication graph. The latter divides the candidate invariants into an SMT-friendly universal inductive core and other noncore invariants, and searches for a small subset of noncore invariants that can be added to the core to prove the safety property of the protocol. Both top-down and bottom-up refinement have strong theoretical guarantees for finding inductive invariants, and their combination is effective at reducing SMT query costs for invariants with existential quantifiers. DuoAI dominates alternative tools in both the number of protocols it verifies and the speed at which it does so, including giving automated proofs for several Paxos variants.

11 Acknowledgments

Ji-Yong Shin provided helpful comments on earlier drafts. This work was supported in part by three Amazon Research Awards, a Guggenheim Fellowship, DARPA contract N66001-21-C-4018, and NSF grants CCF-1918400, CNS-2052947, and CCF-2124080. Ronghui Gu is the Founder of and has an equity interest in CertiK.
References


