Synthesis of Distributed Protocols by Enumeration Modulo Isomorphisms

Derek Egolf and Stavros Tripakis
Northeastern University, Boston, MA, USA
{egolf.d,stavros}@northeastern.edu

Abstract. Synthesis of distributed protocols is a hard, often undecidable, problem. Completion techniques provide partial remedy by turning the problem into a search problem. However, the space of candidate completions is still massive. In this paper, we propose optimization techniques to reduce the size of the search space by a factorial factor by exploiting symmetries (isomorphisms) in functionally equivalent solutions. We present both a theoretical analysis of this optimization as well as empirical results that demonstrate its effectiveness in synthesizing both the Alternating Bit Protocol and Two Phase Commit. Our experiments show that the optimized tool achieves a speedup of approximately 2 to 10 times compared to its unoptimized counterpart.

1 Introduction

Distributed protocols are at the heart of the internet, data centers, cloud services, and other types of infrastructure considered indispensable in a modern society. Yet distributed protocols are also notoriously difficult to get right, and have therefore been one of the primary application domains of formal verification [15,19,20,22,31]. An even more attractive proposition is distributed protocol synthesis: given a formal correctness specification $\psi$, automatically generate a distributed protocol that satisfies $\psi$, i.e., that is correct-by-construction.

Synthesis is a hard problem in general, suffering, like formal verification, from scalability and similar issues. Moreover, for distributed systems, synthesis is generally undecidable [12,23,29,30]. Techniques such as program sketching [26,27] remedy scalability and undecidability concerns essentially by turning the synthesis problem into a completion problem [2,3]: given an incomplete system $M_0$ and a specification $\psi$, automatically synthesize a completion $M$ of $M_0$, such that $M$ satisfies $\psi$.

For example, the synthesis of the well-known alternating-bit protocol (ABP) is considered in [4] as a completion problem: given an ABP system containing the incomplete Sender$_0$ and Receiver$_0$ processes shown in Fig. 1, complete these two processes (by adding but not removing any transitions, and not adding nor removing any states), so that the system satisfies a given set of requirements.
In cases where the space of all possible completions is finite, completion turns synthesis into a decidable problem. However, even then, the number of possible completions can be prohibitively large, even for relatively simple protocols. For instance, as explained in [4], the number of all possible completions in the ABP example is $512^4 \cdot 36$, i.e., approximately 2.5 trillion candidate completions.

Not only is the number of candidate completions typically huge, but it is often also interesting to generate not just one correct completion, but many. For instance, suppose both $M_1$ and $M_2$ are (functionally) correct solutions. We may want to evaluate $M_1$ and $M_2$ also for efficiency (perhaps using a separate method) [10]. In general, we may want to synthesize (and then evaluate w.r.t. performance or other metrics) not just one, but in principle all correct completions. We call this problem the completion enumeration problem, which is the main focus of this paper.

Enumeration is harder than 1-completion (synthesis of just one correct solution), since the number of correct solutions might be very large. For instance, in the case of the ABP example described above, the number of correct completions is 16384 and it takes 88 min to generate all of them [4].

The key idea in this paper is to exploit the notion of isomorphisms in order to reduce the number of correct completions, as well as the search space of candidate completions in general. To illustrate the idea, consider a different incomplete Sender$_0$ process, shown in Fig. 2. Two possible completions of this Sender$_0$ are shown in Fig. 3. Although these two completions are in principle different, they are identical except that states $s_3$ and $s_7$ are swapped. Our goal is to develop a technique which considers these two completions equivalent up to isomorphism, and only explores (and returns) one of them.

---

1 We emphasize that no generality is lost in the sense that one can augment the search for correct completions with an outer loop that keeps adding extra empty states (with no incoming or outgoing transitions), which the inner completion procedure then tries to complete. Thus, we can keep searching for progressively larger systems (in terms of number of states) until a solution is found, if one exists.
Fig. 2. An incomplete ABP Sender with permutable states $s_3, s_7$

Fig. 3. Two synthesized completions of the incomplete process of Fig. 2. Observe that the two completions are identical except that states $s_3$ and $s_7$ are flipped.

To achieve this goal, we adopt the guess-check-generalize paradigm (GCG) [1, 2, 13, 26, 27]. In a nutshell, GCG works as follows: (1) pick a candidate completion $M$; (2) check whether $M$ satisfies $\psi$: if it does, $M$ is one possible solution to the synthesis problem; (3) if $M$ violates $\psi$, prune the search space of possible completions by excluding a generalization of $M$, and repeat from step (1). In the most trivial case, the generalization of $M$ contains only $M$ itself. Ideally, however, and in order to achieve a more significant pruning of the search space, the generalization of $M$ should contain many more “bad” completions which are somehow “similar” (for instance, isomorphic) to $M$. 
A naive way to generalize based on isomorphism is to keep a list of completions encountered thus far and perform an isomorphism check against every element of this list whenever a new candidate is picked. Our approach is smarter: in fact, it does not involve any isomorphism checks whatsoever. Instead, our approach guarantees that no isomorphic completions are ever picked to begin with by pruning them from the search space. This is ultimately done using syntactic transformations of completion representations. The details are left for Sect. 4.

Furthermore, our notion of “encountering” a completion is quite wide. Rather than just pruning completions that are isomorphic to candidates, we also prune completions that are isomorphic to any completion in the generalizations of the candidates (with respect to some prior, unextended notion of generalization). Between the trivial approach involving isomorphism checks and our own approach are several other approaches which are good, but not excellent. Indeed, a categorization of the subtle differences between such approaches is a key contribution of this paper (see Sect. 4.3). These subtleties are easy to miss.

In summary, the main contributions of this paper are the following: (1) we define the 1-completion and completion-enumeration problems modulo isomorphisms; (2) we examine new methods to solve these problems based on the GCG paradigm; (3) we identify properties that an efficient GCG modulo isomorphisms algorithm should have; (4) we propose two instances of such an algorithm, using a naive and a sophisticated notion of generalization; (5) we evaluate our methods on the synthesis of two simple distributed protocols: the ABP and Two Phase Commit (2PC) and demonstrate speedups with respect to the unoptimized method of approximately 2 to 10 times.

2 Preliminaries

Labeled Transition Systems. A (finite) labeled transition system (LTS) $M$ is a tuple $\langle \Sigma, Q, Q_0, \Delta \rangle$, where

- $\Sigma$ is a finite set of transition labels
- $Q$ is a finite set of states
- $Q_0 \subseteq Q$ is the set of initial states
- $\Delta \subseteq Q \times \Sigma \times Q$ is the transition relation.

We write the transition $(p, a, q) \in \Delta$ as $p \xrightarrow{a} q$.

A run of $M$ is an infinite sequence $q_0 \xrightarrow{a_0} q_1 \xrightarrow{a_1} q_2 \xrightarrow{a_2} \ldots$, where $q_0 \in Q_0$ and for each $i$ we have $(q_i, a_i, q_{i+1}) \in \Delta$. The trace produced by this run is $a_0 a_1 a_2 \ldots$. Semantically, an LTS $M$ represents a set of infinite traces, denoted $[M] \subseteq \Sigma^\omega$. Specifically, a trace $a_0 a_1 a_2 \ldots$ is in $[M]$ exactly when there exists a run $q_0 \xrightarrow{a_0} q_1 \xrightarrow{a_1} q_2 \xrightarrow{a_2} \ldots$ of $M$. 
Correctness Specification. We will assume that we have some formal notion of specification and some formal notion of satisfaction between an LTS $M$ and a specification $\psi$. We write $M \models \psi$ to denote that $M$ satisfies $\psi$. Our work is agnostic to what exactly $\psi$ might be (e.g., a temporal logic formula, etc.).

Completions and Syntactic Constraints. Suppose that $M$ and $M_0$ are two LTSs with the same set of labels $\Sigma$, the same set of states $Q$, the same set of initial states $Q_0$, and with transition relations $\Delta$ and $\Delta_0$, respectively. We say that $M$ is a completion of $M_0$ exactly when $\Delta_0 \subseteq \Delta$. That is, $M$ completes $M_0$ by adding more transitions to it (and not removing any). For example, each of the two LTSs of Fig. 3 is a completion of the LTS shown in Fig. 2.

Often, we wish to impose some constraints on the kind of synthesized processes that we want to obtain during automated synthesis, other than the global constraints imposed on the system by the correctness specification. For example, in the formal distributed protocol model proposed in [4], synthesized processes such as the ABP Sender and Receiver are constrained to satisfy a number of requirements, including absence of deadlocks, determinism of the transition relation, the constraint that each state is either an input state (i.e., it only receives inputs) or an output state (i.e., it emits a unique output), the constraint that input states are input-enabled (i.e., they do not block any inputs), and so on. Such properties are often syntactic or structural and can be inferred statically by observing the transition relation. The fact that an LTS is a completion of another LTS can also be captured by such constraints.

Constraints like the above are application-specific, and our approach is agnostic to their precise form and meaning. We will therefore abstract them away, and assume that there is a propositional logic formula $\Phi$ which captures the set of all syntactically well-formed candidate completions. The variable space of $\Phi$ and its precise meaning is application-specific. We will give a detailed construction of $\Phi$ for LTS in Sect. 3. We write $M \models \Phi$ when LTS $M$ satisfies the syntactic constraints $\Phi$. Let $[\Phi] = \{M \mid M \models \Phi\}$.

We say that an LTS is correct if it satisfies both the syntactic constraints imposed by $\Phi$ and the semantic constraints imposed by $\psi$.

Computational Problems

Problem 1 (Model-Checking). Given LTS $M$, specification $\psi$, and constraints $\Phi$, check whether $M \models \psi$ and $M \models \Phi$.

A solution to the model-checking problem is an algorithm, $mc$, such that for all $M, \Phi, \psi$, if $M \models \Phi$ and $M \models \psi$ then $mc(M, \Phi, \psi) = 1$; otherwise, $mc(M, \Phi, \psi) = 0$.

Problem 2 (Synthesis). Given specification $\psi$ and constraints $\Phi$, find, if one exists, LTS $M$ such that $M \models \psi$ and $M \models \Phi$.

Problem 3 (Completion). Given LTS $M_0$, specification $\psi$, and constraints $\Phi$, find, if one exists, a completion $M$ of $M_0$ such that $M \models \psi$ and $M \models \Phi$.

Problem 4 (Completion enumeration). Given LTS $M_0$, specification $\psi$, and constraints $\Phi$, find all completions $M$ of $M_0$ such that $M \models \psi$ and $M \models \Phi$. 
3 The Guess-Check-Generalize Paradigm

In this section we first propose a generic GCG algorithm and reason about its correctness (Sect. 3.1). We then show how to instantiate this algorithm to solve Problems 3 and 4 (Sect. 3.2).

3.1 A Generic GCG Algorithm and Its Correctness

Algorithm 1 is a formal description of a generic GCG algorithm. The algorithm takes as input: (1) a set of syntactic constraints in the form of a propositional formula $\Phi$, as described in Sect. 2; (2) a specification $\psi$ as described in Sect. 2; and (3) a generalizer function $\gamma$, described below.

<table>
<thead>
<tr>
<th>Algorithm 1: GCG[$\Phi, \psi, \gamma$]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 while $\Phi$ is satisfiable do</td>
</tr>
<tr>
<td>2 $\sigma := \text{SAT}(\Phi)$;</td>
</tr>
<tr>
<td>3 if $\text{MC}(M_\sigma, \Phi, \psi) = 1$ then</td>
</tr>
<tr>
<td>4 $\text{return } \sigma$;</td>
</tr>
<tr>
<td>5 $\Phi := \Phi \land \neg \sigma$;</td>
</tr>
<tr>
<td>6 else</td>
</tr>
<tr>
<td>7 $\Phi := \Phi \land \neg \gamma(\sigma)$;</td>
</tr>
</tbody>
</table>

$\Phi$ is a propositional logic formula (over a certain set of boolean variables that depends on the application domain at hand) encoding all possible syntactically valid completions. Every satisfying assignment $\sigma$ of $\Phi$ corresponds to one completion, which we denote as $M_\sigma$. Observe that GCG does not explicitly take an initial (incomplete) model $M_0$ as input: this omission is not a problem because $M_0$ can be encoded in $\Phi$, as mentioned in Sect. 2. We explain specifically how to do that in the case of LTS in Sect. 3.2.

The algorithm works as follows: while $\Phi$ is satisfiable: Line 2: pick a candidate completion $\sigma$ allowed by $\Phi$ by calling a SAT solver. Line 3: model-check the corresponding model $M_\sigma$ against $\psi$ (by definition, $M_\sigma$ satisfies $\Phi$ because $\sigma$ satisfies $\Phi$). Line 4: if $M_\sigma$ satisfies $\psi$ then we have found a correct model: we can return it and terminate if we are solving Problem 3, or return it and continue our search for additional correct models if we are solving Problem 4. In the latter case, in line 5 we exclude $\sigma$ from $\Phi$ (slightly abusing notation, we treat $\sigma$ as a formula satisfied exactly and only by $\sigma$; so that $\neg \sigma$ is the formula satisfied by all assignments except $\sigma$). Line 7: if $M_\sigma$ violates $\psi$, then we exclude from $\Phi$ the generalization $\gamma(\sigma)$ of $\sigma$, and continue our search.

**Generalizers.** A generalizer is a function $\gamma$ which takes an assignment $\sigma$ and returns a propositional logic formula $\gamma(\sigma)$ that encodes all “bad” assignments that we wish to exclude from $\Phi$. Ideally, however, $\gamma(\sigma)$ will encode many more assignments (and therefore candidate completions), so as to prune as large a
part of the search space as possible. A concrete implementation of $\gamma$ may require additional information other than just $\sigma$. For example, $\gamma$ may consult the specification $\psi$, counter-examples returned by the model-checker (which are themselves a function of $\psi$ and $\sigma$), and so on. We avoid including all this information in the inputs of $\gamma$ to ease presentation. We note that $\psi$ does not change during a run of Algorithm 1 and therefore $\psi$ can be “hardwired” into $\gamma$ without loss of generality.

A valid generalizer should include the assignment being generalized and it should only include bad assignments (i.e., it should exclude correct completions). Formally, a generalizer $\gamma$ is said to be proper if for all $\sigma$ such that $\sigma \models \Phi$ and $M_\sigma \not\models \psi$, the following conditions hold: (1) Self-inclusion: $\sigma \models \gamma(\sigma)$, and (2) Correct-exclusion: for any $\varrho$, if $\varrho \models \Phi$ and $M_\varrho \models \psi$ then $\varrho \not\models \gamma(\sigma)$.

The Correctness of GCG

Lemma 1. If $\gamma$ is proper then GCG[$\Phi, \psi, \gamma$] terminates.

Proof. If $\gamma$ is proper then $\gamma(\sigma)$ is guaranteed to include at least $\sigma$. $\Phi$ is a propositional logic formula, therefore it only has a finite set of satisfying assignments. Every iteration of the loop removes at least one satisfying assignment from $\Phi$, therefore the algorithm terminates.

During a run, Algorithm 1 returns a (possibly empty) set of assignments $\text{Sol} = \{\sigma_1, \sigma_2, ..., \sigma_n\}$, representing the solution to Problems 3 or 4. Also during a run, the algorithm guesses candidate assignments by calling the subroutine sat (line 2). Let $\text{Cand}$ be the set of all these candidates. Note that $\text{Sol} \subseteq \text{Cand}$, since every solution returned (line 4) has been first guessed in line 2.

Whenever the algorithm reassigns $\Phi := \Phi \land \lnot \varphi$, we say that it prunes $\varphi$, i.e., the satisfying assignments of $\varphi$ are now excluded from the search. We will need to reason about the set of assignments that have been pruned after a certain partial run of the program. In such cases we can imagine running the algorithm for some amount of time and pausing it. Then the set $\text{Pruned}$ denotes the set of assignments that have been pruned up until that point. It is true that after the program terminates $\text{Pruned} = \left[\Phi\right] \setminus \text{Cand}$, but this equality does not necessarily hold for all partial runs.

Theorem 1. (1) GCG[$\Phi, \psi, \gamma$] is sound, i.e., for all $\sigma \in \text{Sol}$, we have $\sigma \models \Phi$ and $M_\sigma \models \psi$. (2) If $\gamma$ is proper then GCG[$\Phi, \psi, \gamma$] is complete, i.e., for all $\sigma \models \Phi$, if $M_\sigma \models \psi$ then $\sigma \in \text{Sol}$.

Proof. Every $\sigma \in \text{Sol}$ satisfies $\Phi$ (line 2) and the corresponding $M_\sigma$ satisfies $\psi$ (line 3), therefore GCG[$\Phi, \psi, \gamma$] is sound. Now, suppose that $\gamma$ is proper, and take $\varrho$ such that $\varrho \models \Phi$ and $M_\varrho \models \psi$. To show completeness, it suffices to show that $\varrho \in \text{Cand}$. Then, we also have $\varrho \in \text{Sol}$ because $M_\varrho$ passes the model-checking test in line 3. Suppose, for a contradiction, that $\varrho \not\in \text{Cand}$, i.e., that $\varrho$ is pruned. Then there must exist some $\sigma$ such that $\varrho \models \gamma(\sigma)$ (line 7). But $\sigma \models \Phi$ (line 2), which means that $\varrho$ violates the correct-exclusion property of $\gamma$. Contradiction. □
3.2 A Concrete Instance of GCG for LTS

Algorithm 1 is generic in the sense that depending on how exactly we instantiate $\Phi$, $\psi$, and $\gamma$, we can encode different completion enumeration (and more generally model enumeration) problems, as well as solutions. We now show how to instantiate Algorithm 1 to solve Problems 3 and 4 concretely for LTS.

Encoding LTSs and Completions in Propositional Logic. Let $M_0 = (\Sigma, Q, Q_0, \Delta_0)$ be an incomplete LTS. Then we can define a set of boolean variables

$$ V := \{ p \xrightarrow{a} q \mid p, q \in Q \land a \in \Sigma \} $$

so that boolean variable $p \xrightarrow{a} q$ encodes whether transition $p \xrightarrow{a} q$ is present or not (if $p \xrightarrow{a} q$ is present, then $p \xrightarrow{a} q$ is true, otherwise it is false). More formally, let $\text{ASGN}_V$ be the set of all assignments over $V$. An assignment $\sigma \in \text{ASGN}_V$ represents LTS $M_\sigma$ with transition relation $\Delta_\sigma = \{(p, a, q) \mid \sigma(p \xrightarrow{a} q) = 1\}$. To enforce $M_\sigma$ to be a completion of $M_0$, we need to enforce that $\Delta_0 \subseteq \Delta_\sigma$. We do so by initializing our syntactic constraints $\Phi$ as $\Phi := \Phi_{\Delta_0}$, where

$$ \Phi_{\Delta_0} := \bigwedge_{p \xrightarrow{a} q \in \Delta_0} p \xrightarrow{a} q. $$

We can then add extra constraints to $\Phi$ such as determinism or absence of deadlocks, as appropriate.

A Concrete Generalizer for LTS. Based on the principles of [4], we can construct a concrete generalizer $\gamma_{LTS}(\sigma)$ for LTS as $\gamma_{LTS}(\sigma) := \gamma_{safe}(\sigma) \lor \gamma_{live}(\sigma)$, which we separate into a disjunction of a safety violation generalizer and a liveness violation generalizer. The safety component $\gamma_{safe}$ works on the principle that if LTS $M_\sigma$ violates a safety property, then adding extra transitions will not solve this violation. Thus:

$$ \gamma_{safe}(\sigma) := \bigwedge_{x \in V} x. $$

The liveness component $\gamma_{live}$ can be defined based on a notion of reachable, “bad” cycles that enable something to happen infinitely often. Thus, $\neg \gamma_{live}$ captures all LTSs that disable these bad cycles by breaking them or making them unreachable.

It can be shown that the concrete generalizer $\gamma_{LTS}$ is proper. Therefore, the concrete instance $\text{GCG}[\Phi, \psi, \gamma_{LTS}]$ is sound, terminating, and complete, i.e., it solves Problems 3 and 4.

Even though the concrete generalizer is correct, it is not very effective. In particular, it does not immediately prune isomorphisms. There may be $O(n!)$ trivially equivalent completions up to state reordering, where $n$ is the number of states in the LTS. In the next section we present two optimizations exploiting isomorphisms.
4 Synthesis Modulo Isomorphisms

4.1 LTS Isomorphisms

Intuitively, two LTS are isomorphic if we can rearrange the states of one to obtain the other. For synthesis purposes, we often wish to provide as a constraint a set of permutable states $A$, so as to exclude rearrangements that move states outside of $A$. If we can still rearrange the states of an LTS $M_1$ to obtain another LTS $M_2$ subject to this constraint, then we say that $M_1$ and $M_2$ are isomorphic up to $A$. For example, the two LTSs of Fig. 3 are isomorphic up to the set of permutable states $A = \{s_3, s_7\}$. Strictly speaking, they are permutable up to any set of their states, but we choose $A$ to reflect the fact that those two states have no incoming or outgoing transitions in Fig. 2. Permuting any other states would yield an LTS that is not a completion of Fig. 2.

We now define isomorphisms formally. Let $M_0$, $M_1$, and $M_2$ be LTSs with the same $\Sigma, Q, Q_0$, and with transition relations $\Delta_0$, $\Delta_1$, and $\Delta_2$, respectively. Suppose that $M_1$ and $M_2$ are both completions of $M_0$. Let $A \subseteq Q \setminus Q_0$. Then we say $M_1$ and $M_2$ are isomorphic up to $A$, denoted $M_1^A \simeq M_2$, if and only if there exists a bijection $f : A \rightarrow A$ (i.e., a permutation) such that

$$p \xrightarrow{a} q \in \Delta_1 \text{ if and only if } f(p) \xrightarrow{a} f(q) \in \Delta_2.$$ 

By default, we will assume that $A$ is the set of non-initial states that have no incoming or outgoing transitions in $M_0$. In that case we will omit $A$ and write $M_1 \simeq M_2$.

Lemma 2. LTS isomorphism is an equivalence relation, i.e., it is reflexive, symmetric, and transitive.

We use $[M]$ to denote the equivalence class of $M$, i.e., $[M] = \{M' \mid M' \simeq M\}$.

Lemma 3. If $M_1^A \simeq M_2$ then $[M_1] = [M_2]$.

Lemma 3 states that LTS isomorphism preserves traces. More generally, we will assume that our notion of specification is preserved by LTS isomorphism, namely, that if $M_1^A \simeq M_2$ then for any specification $\psi$, $M_1 \Vdash \psi$ iff $M_2 \Vdash \psi$.

Isomorphic Assignments. Two assignments $\sigma$ and $\varrho$ are isomorphic if the LTSs that they represent are isomorphic. Hence we write $\sigma \simeq \varrho$ if and only if $M_\sigma \simeq M_\varrho$. We write $[\varrho]$ to denote the equivalence class of $\varrho$, i.e., the set of all assignments that are isomorphic to $\varrho$. These equivalence classes partition $\Phi$ since $\simeq$ is an equivalence relation.

4.2 Completion Enumeration Modulo Isomorphisms

Isomorphisms allow us to focus our attention to Problem 5 instead of Problem 4:
Problem 5 (Completion enumeration modulo isomorphisms). Given LTS $M_0$, specification $\psi$, and constraints $\Phi$, find the set

$$\{[M] \mid M \text{ is a completion of } M_0 \text{ such that } M \models \psi \text{ and } M \models \Phi\}.$$  

Problem 5 asks that only significantly different (i.e., non-isomorphic) completions are returned to the user. Problem 5 can be solved by a simple modification to Algorithm 1, namely, to exclude the entire equivalence class $[\sigma]$ of any discovered solution $\sigma$, as shown in Algorithm 2, line 5.

**Algorithm 2:** $\text{gCG}_\sim[\Phi, \psi, \gamma]$ solving Problem 5

```plaintext
1 while $\Phi$ is satisfiable do
2     $\sigma := \text{SAT}(\Phi)$;
3     if $\text{mc}(M_\sigma, \Phi, \psi) = 1$ then
4         return $\sigma$;
5     $\Phi := \Phi \land \neg[\sigma]$;
6     else
7         $\Phi := \Phi \land \neg \gamma(\sigma)$;
```

### 4.3 Properties of an Efficient GCG Algorithm

We begin by presenting a list of properties that an efficient instance of GCG ought to satisfy. Except for Property 1, satisfaction of these properties generally depends on the generalizer used.

**Property 1.** For all $\sigma$ that satisfy $\Phi$, $[\sigma] \cap \text{Sol}$ has 0 or 1 element(s). In other words, we return at most one solution per equivalence class.

Property 1 asks that only significantly different (i.e., non-isomorphic) completions are returned to the user, thereby solving Problem 5, which is our main goal. In addition, this property implies that the number of completions is kept small, which is important when these are fed as inputs to some other routine (e.g., one that selects a “highly fit” completion among all valid completions).

$\text{gCG}_\sim$ satisfies Property 1, regardless of the parameters. However, we can go further, by ensuring that not only we do not return isomorphic completions, but we do not even consider isomorphic candidate completions in the first place:

**Property 2.** For all $\sigma$ that satisfy $\Phi$, $[\sigma] \cap \text{Cand}$ has 0 or 1 element(s). In other words, we consider at most one candidate per equivalence class.

Maintaining Property 2 now guarantees that we only call the most expensive subroutines at most once for each equivalence class. Note that, since $\text{Sol} \subseteq \text{Cand}$, Property 2 implies Property 1.

Property 2 is still not entirely satisfactory. For instance, suppose the algorithm generates $\sigma$ as a candidate and then prunes $\gamma(\sigma)$. Now suppose that $\varrho \bowtie \sigma$. Property 2 implies that we cannot call/prune $\gamma(\varrho)$. Property 3 rectifies this:
Property 3 (invariant). Suppose that $\text{gCG}_{\sim}$ invokes $\Phi := \Phi \land \neg \gamma(\sigma)$. Then for any $\varrho \simeq \sigma$, we should have $[\gamma(\varrho)] \subseteq \text{Pruned}$. In other words, if we prune $\gamma(\sigma)$, we should also prune $\gamma(\varrho)$ for every $\varrho$ isomorphic to $\sigma$.

We note that, contrary to Properties 1 and 2 which need only hold after termination, Property 3 is an invariant: we want it to hold for all partial executions of the algorithm.

Theorem 2. Suppose $\gamma$ is proper. If $\text{gCG}_{\sim}[\Phi, \psi, \gamma]$ maintains Property 3 as an invariant, then $\text{gCG}_{\sim}[\Phi, \psi, \gamma]$ also maintains Property 2.

Maintaining Property 3 increases the rate at which the search space is pruned, but is still not enough. Suppose that $\tau \models \gamma(\sigma)$ and that $\tau' \simeq \tau$. If we prune the members of $\gamma(\sigma)$, then we will prune $\tau$, but not necessarily $\tau'$. This possibility is unsatisfactory, since $\tau$ and $\tau'$ should both be treated whenever one of them is.

Property 4 (invariant). Suppose $\tau \in \text{Pruned}$ and $\tau' \simeq \tau$. Then $\tau' \in \text{Pruned}$ or $\tau' \in \text{Sol}$. In other words, if we prune $\tau$ we should also prune any isomorphic $\tau'$, unless $\tau'$ happens to be a solution. (Note that Property 1 guarantees that this exception applies to at most one $\tau'$).

Maintaining Property 4 as an invariant further accelerates pruning. Under certain conditions, Property 3 implies Property 4. In particular, Property 3 implies Property 4 if $\gamma$ is invertible, a concept that we define next.

Invertible Generalizers. Let $\gamma$ be a generalizer and let $\tau$ be an assignment. We define the inverse $\gamma^{-1}(\tau)$, to be the propositional logic formula satisfied by all $\sigma$ such that $\tau \models \gamma(\sigma)$. That is, $\sigma \models \gamma^{-1}(\tau)$ iff $\tau \models \gamma(\sigma)$.

Let $\varphi$ and $\varphi'$ be propositional logic formulas. Suppose that for every $\sigma \models \varphi$, there exists a $\sigma' \models \varphi'$ such that $\sigma' \simeq \sigma$. Then we say that $\varphi$ subsumes $\varphi'$ up to isomorphism. If $\varphi$ and $\varphi'$ both subsume each other, then we say that they are equivalent up to isomorphism.

A generalizer $\gamma$ is invertible if for all assignments $\tau, \tau'$ that satisfy $\Phi$, if $\tau \simeq \tau'$ then $\gamma^{-1}(\tau)$ and $\gamma^{-1}(\tau')$ are equivalent up to isomorphism. Now if $\tau \models \gamma(\sigma)$ and $\tau' \simeq \tau$, invertibility guarantees that we can point to a $\sigma' \simeq \sigma$ such that $\tau' \models \gamma(\sigma')$.

Theorem 3. Suppose $\gamma$ is proper and invertible. If $\text{gCG}_{\sim}[\Phi, \psi, \gamma]$ maintains Property 3 as an invariant, then $\text{gCG}_{\sim}[\Phi, \psi, \gamma]$ also maintains Property 4 as an invariant.

Proof. Let $\gamma$ be a proper, invertible generalizer. We will proceed by contradiction. Assume that we have run the algorithm for some amount of time and paused its execution, freezing the state of $\text{Pruned}$. Suppose that $\text{gCG}_{\sim}[\Phi, \psi, \gamma]$ satisfies Property 3 at this point, but that it does not satisfy Property 4. From the negation of Property 4, we have at this point in the execution two assignments $\tau$ and $\tau'$ such that (1) $\tau \simeq \tau'$, (2) $\tau \in \text{Pruned}$, (3) $\tau' \notin \text{Pruned}$, and (4) $\tau' \notin \text{Sol}$.
There are two cases that fall out of (2). Either \( \tau \) was pruned using a call to \( \gamma \), or exactly \([\tau] \) was pruned. In the second case, we quickly reach a contradiction since it implies that \( \tau' \in \text{Pruned} \), violating assumption (3).

So instead, we assume \( \tau \models \gamma(\sigma) \) for some \( \sigma \) and that this call to \( \gamma \) was invoked at some point in the past. So \( \sigma \equiv \gamma^{-1}(\tau) \). But then by invertibility and (1) there exists \( \sigma' \simeq \sigma \) such that \( \sigma' \equiv \gamma^{-1}(\tau') \) and hence \( \tau' \equiv \gamma(\sigma') \). Property 3 tells us then that \( \tau' \in \text{Pruned} \), but this conclusion also violates assumption (3). \( \Box \)

It can be shown that the generalizer \( \gamma_{\text{LTS}} \) is invertible. Essentially, this is because \( \gamma_{\text{LTS}} \) does not depend on state names (for example, the structure of cycles and paths is independent of state names). Still, \( \text{GCG}_{\equiv}[\Phi, \psi, \gamma_{\text{LTS}}] \) satisfies only Property 1 above. Therefore, we will next describe an optimized generalization method that exploits isomorphism to satisfy all properties.

4.4 Optimized Generalization

**Equivalence Closure.** If \( \gamma \) is a generalizer and \( \simeq \) is an equivalence relation, then let
\[
\tilde{\gamma}(\varrho) := \bigvee_{\sigma \in [\varrho]} \gamma(\sigma)
\]
be the equivalence closure of \( \gamma \). If \( \gamma(\sigma) \equiv \tilde{\gamma}(\sigma) \) for all \( \sigma \), we say that \( \gamma \) is closed under equivalence.

Note that \( \tilde{\gamma} \) is itself a generalizer. An instance of \( \text{GCG}_{\equiv} \) that uses \( \tilde{\gamma} \) is correct and satisfies all the efficiency properties identified above:

**Theorem 4.** If \( \gamma \) is a proper generalizer, then \( \text{GCG}_{\equiv}[\Phi, \psi, \tilde{\gamma}] \) is sound, terminating, and complete up to isomorphisms.

**Theorem 5.** If \( \gamma \) is proper, then \( \text{GCG}_{\equiv}[\Phi, \psi, \tilde{\gamma}] \) maintains Properties 1 and 2. Furthermore, the algorithm maintains Property 3 as an invariant.

**Theorem 6.** If \( \gamma \) is both proper and invertible, then: (1) \( \tilde{\gamma} \) is invertible; (2) \( \text{GCG}_{\equiv}[\Phi, \psi, \tilde{\gamma}] \) maintains Property 4 as an invariant.

**Computation Options for \( \tilde{\gamma} \).** The naive way to compute \( \tilde{\gamma} \) is to iterate over all \( \sigma_1, \sigma_2, \ldots, \sigma_k \in [\varrho] \), compute each \( \gamma(\sigma_i) \), and then return the disjunction of all \( \gamma(\sigma_i) \). We call this the naive generalization approach. The problem with this approach is that we have to call \( \gamma \) as many as \( n! \) times, where \( n \) is the number of permutable states. The experimental results in Sect. 5 indicate empirically that this naive method does not scale well.

We thus propose a better approach, which is incremental, in the sense that we only have to compute \( \gamma \) once, for \( \gamma(\sigma_1) \); we can then perform simple syntactic transformations on \( \gamma(\sigma_1) \) to obtain \( \gamma(\sigma_2) \), \( \gamma(\sigma_3) \), and so on. As we will show, these transformations are much more efficient than computing each \( \gamma(\sigma_i) \) from scratch. So-called permuters formalize this idea:
Permuters. A permuter is a function \( \pi \) that takes as input an assignment \( \varrho \) and the generalization \( \gamma(\sigma) \) for some \( \sigma \simeq \varrho \), and returns a propositional logic formula \( \pi(\sigma, \gamma(\sigma)) \) such that \( \forall \varrho \models \Phi, \forall \sigma \simeq \varrho \models M_\varrho \not\models \psi : M_\varrho \not\models \pi(\sigma, \gamma(\sigma)) \equiv \gamma(\varrho) \). That is, assuming \( \varrho \) is "bad" \( (M_\varrho \not\models \psi) \), \( \pi(\varrho, \gamma(\varrho)) \) is equivalent to \( \gamma(\varrho) \). However, contrary to \( \gamma \), \( \pi \) can use the extra information \( \gamma(\sigma) \) to compute the generalization of \( \varrho \). Then, instead of \( \tilde{\gamma}(\varrho) \), we can compute the logically equivalent formula

\[
\gamma_\pi(\varrho) := \bigvee_{\sigma \in [\varrho]} \pi(\sigma, \gamma(\varrho)).
\]

**Theorem 7.** Theorems 4, 5, and 6 also hold for \( \text{gCG}_{\simeq}[\Phi, \psi, \gamma_\pi] \).

**Proof.** Follows from the fact that for any \( \varrho, \gamma_\pi(\varrho) \equiv \tilde{\gamma}(\varrho) \). \( \square \)

A Concrete Permuter for LTS. We now explain how to compute \( \pi \) concretely in our application domain, namely LTS. Let \( M_0 \) be an incomplete LTS. Let \( \sigma_1, \sigma_2 \) be two assignments encoding completions \( M_{\sigma_1} \) and \( M_{\sigma_2} \) of \( M_0 \). Suppose \( M_{\sigma_1} \simeq M_{\sigma_2} \). Recall that \( A \) is the set of permutable states (the non-initial states with no incoming/outgoing transitions by default). Then there is a permutation \( f : A \to A \), such that applying \( f \) to the states of \( M_{\sigma_1} \) yields \( M_{\sigma_2} \). \( f \) allows us to transform one LTS to another, but it also allows us to transform the generalization formula for \( \sigma_1 \), namely \( \gamma(\sigma_1) \), to the one for \( \sigma_2 \), namely \( \gamma(\sigma_2) \).

For example, let \( M_0 \) be the leftmost LTS in Fig. 4, with alphabet \( \Sigma = \{a\} \), states \( Q = \{p_0, p_1, p_2, p_3\} \), initial state \( p_0 \), and the empty transition relation. Let \( M_{\sigma_1} \) and \( M_{\sigma_2} \) be the remaining LTSs shown in Fig. 4. Let \( A = \{p_1, p_2, p_3\} \) and let \( f \) be the permutation mapping \( p_1 \) to \( p_3 \), \( p_3 \) to \( p_2 \), and \( p_2 \) to \( p_1 \). Then \( M_{\sigma_1} \simeq M_{\sigma_2} \) and \( f \) is the witness to this isomorphism.

Let \( \gamma(\sigma_1) = (p_0 \models_a p_1) \land (p_1 \models_a p_2) \land (p_2 \models_a p_3) \). \( \gamma(\sigma_1) \) captures the four LTSs in Fig. 5. The key idea is that we can compute \( \gamma(\sigma_2) \) by transforming \( \gamma(\sigma_1) \) purely syntactically. In particular, we apply the permutation \( f \) to all \( p_i \) appearing in the variables of the formula. Doing so, we obtain \( \gamma(\sigma_2) = (p_0 \models_a p_3) \land (p_3 \models_a p_1) \land (p_1 \models_a p_2) \). This formula in turn captures the four LTSs in Fig. 6, which are exactly the permutations of those in Fig. 5 after applying \( f \).

We now describe this transformation formally. Observe that \( M_{\sigma_1} \) and \( M_{\sigma_2} \) have the same set of states, say \( Q \). We extend the permutation to \( f : Q \to Q \) by defining \( f(q) = q \) for all states \( q \notin A \). Now, we extend this permutation of states to permutations of the set \( V \) (the set of boolean variables encoding transitions). Specifically we extend \( f \) to permute \( V \) by defining: \( f(p \models_a q) := f(p) \models_a f(q) \) and we extend it to propositional formulas by applying it to all variables in the formula. Then we define \( \pi_{\text{LTS}}(\sigma_2, \gamma(\sigma_1)) := f(\gamma(\sigma_1)) \).

In essence, the permuter \( \pi_{\text{LTS}} \) identifies the permutation \( f \) witnessing the fact that \( \sigma_1 \simeq \sigma_2 \). It then applies \( f \) to the variables of \( \gamma(\sigma_1) \). Applying \( f \) to \( \gamma(\sigma_1) \) is equivalent to applying \( f \) to all assignments that satisfy \( \gamma(\sigma_1) \).

It can be shown that \( \pi_{\text{LTS}} \) is a permuter for LTS. It follows then that the concrete instance \( \text{gCG}_{\simeq}[\Phi, \psi, \gamma_\pi] \) (where \( \gamma := \gamma_{\text{LTS}} \) and \( \pi := \pi_{\text{LTS}} \)) satisfies
Theorem 7, i.e., it is sound, terminating, complete up to isomorphisms, and satisfies all Properties 1–4.

5 Implementation and Evaluation

Implementation and Experimental Setup. We evaluate the three algorithms discussed so far: the unoptimized algorithm $\text{gcg}([\Phi, \psi, \gamma_{\text{LTS}}]$ of [2,4] (Sect. 3.2); and the naive optimization $\text{gcg}_{\sim}[\Phi, \psi, \gamma]$ and permuter optimization $\text{gcg}_{\sim}[\Phi, \psi, \gamma_{\pi}]$ algorithms of Sect. 4.4. These are respectively labeled ‘unopt.’, ‘naive opt.’, and ‘perm. opt.’ in the tables that follow.

In addition, we evaluate the unoptimized algorithm outfitted with an additional optimization, which we call the dead transition optimization. We say that a transition of an LTS is dead if this transition is never taken in any run. If $M$ with states $Q$ is correct and has $k$ dead transitions, then there are $|Q|^k$ solutions that are equivalent modulo dead transitions, since we can point a dead transition anywhere while maintaining correctness. The dead transition optimization prunes all solutions which are equivalent modulo dead transitions. It is equivalent to the unoptimized algorithm in cases where there are no solutions or where we are looking for only one solution. Therefore, we evaluate the dead transition optimization side-by-side with the unoptimized solution only when we are enumerating all correct completions. The naive and permuter optimizations both include the dead transition optimization.
We use [28], the Python implementation of gcg[Φ, ψ, γ_{LTS}] made publicly available by the authors of [2,4], and we implement our optimizations on top of [28] in order to keep the comparison fair. The tool can handle completion of distributed systems, rather than of single LTSs. Distributed systems are represented as networks of communicating LTSs similar to those in [4]. Specifications are represented using safety and liveness (Büchi) monitors, again similar to those in [4]. However, let us again mention that our approach is not specific to any particular specification logic; it should allow for performance gains whenever the cost of model-checking is greater than the cost of the simple syntactic transformations applied by the permuter. We use the SAT solver Z3 [7] to pick candidates from the search space. Our experimental results can be reproduced using a publicly available artifact [9].

For our experiments we use the ABP case study as presented in [4] as well as our own two phase commit (2PC) case study. We consider three use cases: (1) completion enumeration: enumerate all correct completions; (2) realizable 1-completion: return the first correct completion and stop, where we ensure that a correct completion exists; and (3) unrealizable 1-completion: return the first correct completion, except that we ensure that none exists (and therefore the tool has to explore the entire candidate space in vain).

We consider a many-process synthesis scenario, where the goal is to synthesize two or more processes, and a 1-process synthesis scenario, where the goal is to synthesize a single process. In both of these scenarios across both the ABP and 2PC case studies, the synthesized processes are composed with additional environment processes and safety and liveness monitors. The results of the many-process synthesis scenario are presented shortly. Due to lack of space, the results of the 1-process synthesis scenario are presented in Appendix A.2 of [11]. The latter results do not add much additional insight, except that 1-process synthesis tends to take less time.

Each experiment was run on a dedicated 2.40 GHz CPU core located on the Northeastern Discovery Cluster. All times are in seconds, rounded up to the second.

**Many-Process Synthesis Experiments.** In all these experiments, there are multiple LTSs that must both be completed. In the case of ABP: (1) the incomplete ABP Receiver₀ of Fig. 1 without further modification; (2) an incomplete sender process, which is obtained by removing some set of transitions from process Sender of Fig. 3. The set of transitions removed from Sender are all incoming and all outgoing transitions from all states designated as permutable for that experiment (column A in the tables that follow). For instance, in experiment \{s₁, s₂\} of Table 1 we remove all incoming and outgoing transitions from states s₁ and s₂ of Sender, and similarly for the other experiments. And in the case of 2PC: (1) two incomplete 2PC database managers (see Fig. 8 in Appendix A.1 of [11]) (2) an incomplete transaction manager, which is obtained by removing some set of transitions from a complete transaction manager (see Fig. 7 in Appendix A.1 of [11]).
Completion Enumeration. Table 1 presents the results for the completion enumeration use case and many-process synthesis scenario. Columns labeled sol. and iter. record the number of solutions (i.e., |Sol|) and loop iterations of Algorithm 2 (i.e., the number of candidates |Cand|, i.e., the number of times the SAT routine is called), respectively. Pilot experiments showed negligible variance across random seeds, so reported times are for one seed. TO denotes a timeout of 4 h, in which case $p/q$ means the tool produced $p$ out of the total $q$ solutions. For the dead opt. column, we know that $q = 24 \cdot n$, where $n$ is the number of solutions/equivalence classes found by the permuter optimization and $24 = 4!$ is the number of isomorphisms for 4 states. Since the naive optimization produces equivalence classes, $q = n$ for the naive opt. column.

The results in Table 1 are consistent with our theoretical analyses. When there are 2 permutable states, the naive and permuter optimizations explore about half the number of candidates as the dead transitions method. For 3 permutable states, the optimized methods explore about 3! = 6 times fewer candidates. For 4 permutable states, the optimized methods explore about 4! = 24 times fewer candidates than the dead transitions method in the only experiment where the unoptimized method does not timeout. Notably, the permuter optimization does not timeout on any of these experiments.
Realizable 1-Completion. Table 2 presents the results for the realizable 1-completion use case (return the first solution found and stop) and many-process synthesis scenario. Our experiments and those of [4] suggest that there is more time variability for this task depending on the random seed provided to Z3. Thus, for Table 2 we run the tools for 10 different random seeds and report average times and number of iterations, rounded up. In one case (last row of Table 2), for a single seed out of the 10 seeds, the program timed out before finding a solution. As the true average is unknown in this case, we report it as TO.

<table>
<thead>
<tr>
<th>Case Study; A</th>
<th>unopt.</th>
<th>naive opt.</th>
<th>perm. opt.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>iter.</td>
<td>time</td>
<td>iter.</td>
</tr>
<tr>
<td>2PC; {p_1, p_2}</td>
<td>199</td>
<td>19</td>
<td>157</td>
</tr>
<tr>
<td>2PC; {p_2, p_3}</td>
<td>483</td>
<td>47</td>
<td>429</td>
</tr>
<tr>
<td>2PC; {p_3, p_4}</td>
<td>798</td>
<td>72</td>
<td>696</td>
</tr>
<tr>
<td>2PC; {p_4, p_5}</td>
<td>380</td>
<td>37</td>
<td>319</td>
</tr>
<tr>
<td>ABP; {s_1, s_2}</td>
<td>111</td>
<td>4</td>
<td>110</td>
</tr>
<tr>
<td>ABP; {s_2, s_3}</td>
<td>220</td>
<td>9</td>
<td>205</td>
</tr>
<tr>
<td>ABP; {s_3, s_4}</td>
<td>106</td>
<td>5</td>
<td>102</td>
</tr>
<tr>
<td>ABP; {s_4, s_5}</td>
<td>1669</td>
<td>75</td>
<td>909</td>
</tr>
<tr>
<td>ABP; {s_5, s_6}</td>
<td>102</td>
<td>5</td>
<td>95</td>
</tr>
<tr>
<td>ABP; {s_6, s_7}</td>
<td>507</td>
<td>28</td>
<td>294</td>
</tr>
<tr>
<td>2PC; {p_2, p_3, p_4}</td>
<td>440</td>
<td>48</td>
<td>590</td>
</tr>
<tr>
<td>2PC; {p_3, p_4, p_5}</td>
<td>954</td>
<td>94</td>
<td>861</td>
</tr>
<tr>
<td>ABP; {s_1, s_2, s_3}</td>
<td>332</td>
<td>12</td>
<td>225</td>
</tr>
<tr>
<td>ABP; {s_2, s_3, s_4}</td>
<td>2462</td>
<td>108</td>
<td>904</td>
</tr>
<tr>
<td>ABP; {s_3, s_4, s_5}</td>
<td>2267</td>
<td>102</td>
<td>1040</td>
</tr>
<tr>
<td>ABP; {s_4, s_5, s_6}</td>
<td>2735</td>
<td>130</td>
<td>1513</td>
</tr>
<tr>
<td>ABP; {s_5, s_6, s_7}</td>
<td>361</td>
<td>21</td>
<td>264</td>
</tr>
<tr>
<td>2PC; {p_1, p_2, p_3, p_4}</td>
<td>806</td>
<td>81</td>
<td>495</td>
</tr>
<tr>
<td>ABP; {s_1, s_2, s_3, s_4}</td>
<td>1957</td>
<td>85</td>
<td>1068</td>
</tr>
<tr>
<td>ABP; {s_3, s_4, s_5, s_6}</td>
<td>5425</td>
<td>261</td>
<td>1003</td>
</tr>
<tr>
<td>ABP; {s_4, s_5, s_6, s_7}</td>
<td>16098</td>
<td>1088</td>
<td>TO</td>
</tr>
</tbody>
</table>

Unrealizable 1-Completion. Table 3 presents the results for the unrealizable 1-completion use case and many-process synthesis scenario. For these experiments, we artificially modify the ABP Sender by completely removing state $s_7$, which results in no correct completion existing. A similar change is applied to tx. man.
in the case of 2PC. Thus, the tools explore the entire search space and terminate without finding a solution. As can be seen, the permuter optimization significantly prunes the search space and achieves considerable speedups.

<table>
<thead>
<tr>
<th>Case Study; $A$</th>
<th>unopt.</th>
<th>naive opt.</th>
<th>perm. opt.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>iter.</td>
<td>iter.</td>
<td>iter.</td>
</tr>
<tr>
<td></td>
<td>time</td>
<td>time</td>
<td>time</td>
</tr>
<tr>
<td>2PC; ${p_1,p_2}$</td>
<td>3207</td>
<td>1658</td>
<td>1655</td>
</tr>
<tr>
<td></td>
<td>292</td>
<td>206</td>
<td>175</td>
</tr>
<tr>
<td>2PC; ${p_2,p_3}$</td>
<td>9792</td>
<td>4996</td>
<td>4982</td>
</tr>
<tr>
<td></td>
<td>978</td>
<td>646</td>
<td>552</td>
</tr>
<tr>
<td>2PC; ${p_3,p_4}$</td>
<td>14911</td>
<td>7645</td>
<td>7589</td>
</tr>
<tr>
<td></td>
<td>1527</td>
<td>1053</td>
<td>878</td>
</tr>
<tr>
<td>2PC; ${p_4,p_5}$</td>
<td>5123</td>
<td>2537</td>
<td>2555</td>
</tr>
<tr>
<td></td>
<td>494</td>
<td>339</td>
<td>282</td>
</tr>
<tr>
<td>ABP; ${s_1,s_2}$</td>
<td>1650</td>
<td>879</td>
<td>853</td>
</tr>
<tr>
<td></td>
<td>58</td>
<td>52</td>
<td>33</td>
</tr>
<tr>
<td>ABP; ${s_2,s_3}$</td>
<td>4300</td>
<td>2384</td>
<td>2374</td>
</tr>
<tr>
<td></td>
<td>173</td>
<td>171</td>
<td>106</td>
</tr>
<tr>
<td>ABP; ${s_3,s_4}$</td>
<td>327</td>
<td>173</td>
<td>164</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>11</td>
<td>7</td>
</tr>
<tr>
<td>ABP; ${s_4,s_5}$</td>
<td>3108</td>
<td>1592</td>
<td>1710</td>
</tr>
<tr>
<td></td>
<td>143</td>
<td>130</td>
<td>89</td>
</tr>
<tr>
<td>ABP; ${s_5,s_6}$</td>
<td>333</td>
<td>172</td>
<td>168</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>15</td>
<td>9</td>
</tr>
<tr>
<td>2PC; ${p_2,p_3,p_4}$</td>
<td>66088</td>
<td>19717</td>
<td>19850</td>
</tr>
<tr>
<td></td>
<td>TO</td>
<td>10867</td>
<td>9610</td>
</tr>
<tr>
<td>2PC; ${p_3,p_4,p_5}$</td>
<td>70586</td>
<td>26343</td>
<td>26516</td>
</tr>
<tr>
<td></td>
<td>TO</td>
<td>14340</td>
<td></td>
</tr>
<tr>
<td>ABP; ${s_1,s_2,s_3}$</td>
<td>20858</td>
<td>3705</td>
<td>3668</td>
</tr>
<tr>
<td></td>
<td>1022</td>
<td>798</td>
<td>253</td>
</tr>
<tr>
<td>ABP; ${s_2,s_3,s_4}$</td>
<td>58974</td>
<td>10516</td>
<td>10496</td>
</tr>
<tr>
<td></td>
<td>4021</td>
<td>2673</td>
<td>1052</td>
</tr>
<tr>
<td>ABP; ${s_3,s_4,s_5}$</td>
<td>12323</td>
<td>2231</td>
<td>2167</td>
</tr>
<tr>
<td></td>
<td>596</td>
<td>504</td>
<td>146</td>
</tr>
<tr>
<td>ABP; ${s_4,s_5,s_6}$</td>
<td>11210</td>
<td>2104</td>
<td>1985</td>
</tr>
<tr>
<td></td>
<td>557</td>
<td>491</td>
<td>136</td>
</tr>
<tr>
<td>2PC; ${p_1,p_2,p_3,p_4}$</td>
<td>67659</td>
<td>10365</td>
<td>12308</td>
</tr>
<tr>
<td></td>
<td>TO</td>
<td>TO</td>
<td></td>
</tr>
<tr>
<td>ABP; ${s_1,s_2,s_3,s_4}$</td>
<td>129264</td>
<td>12096</td>
<td>14739</td>
</tr>
<tr>
<td></td>
<td>TO</td>
<td>TO</td>
<td></td>
</tr>
<tr>
<td>ABP; ${s_3,s_4,s_5,s_6}$</td>
<td>45056</td>
<td>2466</td>
<td>2004</td>
</tr>
<tr>
<td></td>
<td>2869</td>
<td>2392</td>
<td>339</td>
</tr>
</tbody>
</table>

6 Related Work

Synthesis of Distributed Protocols: Distributed system synthesis has been studied both in the reactive synthesis setting [23] and in the setting of discrete-event systems [29,30]. More recently, synthesis of distributed protocols has been studied using completion techniques in [2–4,17]. [2,4] study completion of finite-state protocols such as ABP but they do not focus on enumeration. [3] considers infinite-state protocols and focus on synthesis of symbolic expressions (guards and assignments). None of [2–4] propose any reduction techniques. We propose reduction modulo isomorphisms.

[17] studies synthesis for a class of parameterized distributed agreement-based protocols for which verification is efficiently decidable. Another version of the
paper [16] considers permutations of process indices. These are different from our permutations over process states.

Synthesis of parameterized distributed systems is also studied in [21] using the notion of cutoffs, which guarantee that if a property holds for all systems up to a certain size (the cutoff size) then it also holds for systems of any size. Cutoffs are different from our isomorphism reductions.

**Bounded Synthesis:** The bounded synthesis approach [12] limits the search space of synthesis by setting an upper bound on certain system parameters, and encodes the resulting problem into a satisfiability problem. Bounded synthesis is applicable to many application domains, including distributed system synthesis, and has been successfully used to synthesize systems such as distributed arbiters and dining philosophers [12]. Symmetries have also been exploited in bounded synthesis. Typically, such symmetries encode similarity of processes (e.g., all processes having the same state-transition structure, as in the case of dining philosophers). As such, these symmetries are similar to those exploited in parameterized systems, and different from our LTS isomorphisms.

**Symmetry Reductions in Model-Checking:** Symmetries have been exploited in model-checking [5]. The basic idea is to take a model $M$ and construct a new model $M_G$ which has a much smaller state space. This construction exploits the fact that many states in $M$ might be functionally equivalent, in the sense of incoming and outgoing transitions. The key distinction between this work and ours is that our symmetries are over the space of models rather than the space of states of a fixed model. This distinction allows us to exploit symmetries for completion enumeration rather than model-checking.

**Symmetry-Breaking Predicates:** Symmetry-breaking predicates have been used to solve SAT [6], SMT [8], and even graph search problems [14], more efficiently. Our work is related in the sense that we are also trying to prune a search space. But our approach differs both in the notion of symmetry used (LTS isomorphism) as well as the application domain (distributed protocols). Moreover, rather than trying to eliminate all but one member of each equivalence class at the outset, say, by somehow adding a global (and often prohibitively large) symmetry-breaking formula $\Xi$ to $\Phi$, we do so on-the-fly for each candidate solution.

**Canonical Forms:** In program synthesis work [25], a candidate program is only checked for correctness if it is in some normal form. [25] is not about synthesis of distributed protocols, and as such the normal forms considered there are very different from our LTS isomorphisms. In particular, as with symmetry-breaking, the normal forms used in [25] are global, defined a-priori for the entire program domain, whereas our generalizations are computed on-the-fly. Moreover, the approach of [25] may still generate two equivalent programs as candidates (prior to verification), i.e., it does not satisfy our Property 2.
Sketching, CEGIS, OGIS, Sciduction: Completion algorithms such as GCG belong to the same family of techniques as sketching [27], counter-example guided inductive synthesis (CEGIS) [1,13,26,27], oracle-guided inductive synthesis (OGIS) [18], and sciduction [24].

7 Conclusions

We proposed a novel distributed protocol synthesis approach based on completion enumeration modulo isomorphisms. Our approach follows the guess-check-generalize synthesis paradigm, and relies on non-trivial optimizations of the generalization step that exploit state permutations. These optimizations allow to significantly prune the search space of candidate completions, achieving speedups of factors approximately 2 to 10 and in some cases completing experiments in minutes instead of hours. To our knowledge, ours is the only work on distributed protocol enumeration using reductions such as isomorphism.

As future work, we plan to employ this optimized enumeration approach for the synthesis of distributed protocols that achieve not only correctness, but also performance objectives. We also plan to address the question where do the incomplete processes come from? If not provided by the user, such incomplete processes might be automatically generated from example scenarios as in [2,4], or might simply be “empty skeletons” of states, without any transitions. We also plan to extend our approach to infinite-state protocols, as well as application domains beyond protocols, as Algorithm 2 is generic and thus applicable to a wide class of synthesis domains.

Acknowledgements. Derek Egolf’s research has been initially supported by a Northeastern University PhD fellowship. This material is based upon work supported by the National Science Foundation Graduate Research Fellowship under Grant No. (1938052). Any opinion, findings, and conclusions or recommendations expressed in this material are those of the authors(s) and do not necessarily reflect the views of the National Science Foundation. We thank Christos Stergiou for his work on the distributed protocol completion tool that we built upon. We also thank the anonymous reviewers for their helpful comments and feedback.

References