Unrealizability Logic

ANONYMOUS AUTHOR(S)

We consider the problem of establishing that a program-synthesis problem is unrealizable (i.e., has no solution in a given search space of programs). Prior work on unrealizability has developed some automatic techniques to establish that a problem is unrealizable; however, these techniques are all black-box, meaning that they conceal the reasoning behind why a synthesis problem is unrealizable.

In this paper, we present a reasoning system, called unrealizability logic for establishing that a program-synthesis problem is unrealizable. To the best of our knowledge, unrealizability logic is the first proof system for overapproximating the execution of an infinite set of imperative programs. The logic provides a general, logical system for building checkable proofs about unrealizability. Similar to how Hoare logic distills the fundamental concepts behind algorithms and tools to prove the correctness of programs, unrealizability logic distills into a single logical system the fundamental concepts that were hidden within prior tools capable of establishing that a program-synthesis problem is unrealizable.

1 INTRODUCTION

Program synthesis refers to the task of discovering a program, within a given search space, that satisfies a behavioral specification (e.g., a logical formula, or a set of input-output examples). While there have been many advances in program synthesis, especially in domain-specific settings [6, 8, 21], program synthesis remains a challenging task with many properties that are not yet well understood.

While tools are becoming better at synthesizing programs, one property that remains difficult to reason about is the unrealizability of a synthesis problem, i.e., the non-existence of a solution that satisfies the behavioral specification within the search space of possible programs. The ability to prove that a problem is unrealizable has many applications; for example, one can show that a certain synthesized solution is optimal with respect to some metric by proving that a better solution to the synthesis problem does not exist—i.e., by proving that the synthesis problem where the search space contains only programs of lower cost is unrealizable [12]. Unrealizability is also used to prune program paths in symbolic-execution engines for program repair [16].

Example 1.1. Consider the synthesis problem $sy_{\text{first}}$ where the goal is to synthesize a function $f$ that takes as input a state $(x, y)$, and returns a state where $y = 10$. Assume, however, that the search space of possible programs in $sy_{\text{first}}$ is defined using the following grammar $G_{\text{first}}$:

$Start \rightarrow y := E \quad E \rightarrow x \mid E + 1$

Clearly $y := 10 \notin L(\text{Start})$; moreover, all programs in $L(\text{Start})$ are incorrect on at least one input. For example, on the input $x = 15$ every program in the grammar sets $y$ to a value greater than 15. Consequently, $sy_{\text{first}}$ is unrealizable.

While it is trivial for a human to establish that $sy_{\text{first}}$ is indeed unrealizable, only a small number of known techniques can prove this fact automatically [10, 11, 14]. However, a common drawback of these techniques is that they do not produce a proof artifact. In particular, Kim et al. [14] and Hu et al. [10] rely on external constraint solvers and program verifiers to prove unrealizability. While a solver-based approach has worked well in practice, without extensive knowledge of the internals of the external solvers, it is difficult to understand exactly why a synthesis problem is unrealizable.

This paper presents unrealizability logic, a proof system for reasoning about the unrealizability of synthesis problems. In addition to the main goal of reasoning about unrealizability, unrealizability logic is designed with the following goals in mind:
• to be a general logic, capable of dealing with various synthesis problems;
• to be amenable to machine reasoning, as to enable both automatic proof checking and to open future opportunities for automation;
• to provide insight into why certain synthesis problems are unrealizable through the process of completing a proof tree.

Via unrealizability logic, one is able to (i) reason about unrealizability in a principled, explicit fashion, and (ii) produce concrete proofs about unrealizability.

In this paper, unrealizability logic is formulated for synthesis problems over a deterministic, imperative programming language with statements involving Boolean and integer expressions. There are several challenges to creating unrealizability logic, which are illustrated in §2. One such challenge is already illustrated in Example 1.1: because of the recursive definition of nonterminal E, the search space of programs $L(G_{\text{first}})$ is an infinite set. In unrealizability logic, one reasons about infinite sets of programs en masse—as opposed to reasoning about each program in the set separately. Proofs in unrealizability logic must thus establish judgements of the following kind:

For a given a set of input-output examples, no matter which program is chosen (out of a possibly infinite set of programs), there is at least one input-output example that is handled incorrectly.

The proof system for unrealizability logic has sound underpinnings, and provides a way to build proofs of unrealizability similar to the way Hoare logic [9] provides a way to build proofs that a given program cannot reach a set of bad states.

Contributions. In summary, this paper makes the following contributions:
• Unrealizability logic, the first logical proof system for overapproximating the execution of an infinite set of imperative programs (§3).
• A proof of soundness and relative completeness for unrealizability logic (§4).
• Examples that illustrate the proving power of unrealizability logic: in particular, unrealizability logic can be used to prove unrealizability for problems out of reach for previous methods; e.g., those for which the proof requires reasoning about an infinite number of examples (§5).

§6 discusses related work. §7 concludes. Proofs for theorems in the paper may be found in the supplementary material (Appendix A).

2 MOTIVATING EXAMPLES

In this section, we give several key examples that describe how proof trees in unrealizability logic work, and also illustrate two key challenges behind unrealizability logic (§2.1, §2.2). Unrealizability logic shares much of the intuition behind Hoare logic and its extension toward recursive programs. However, as we will illustrate in §2.3, these concepts alone are insufficient to model unrealizability, which motivated us to develop the new concepts that we introduce in this paper.

Hoare logic is based on triples that overapproximate the set of states that can be reached by a program $s$; i.e., the Hoare triple

$$\{P\} s \{Q\}$$

asserts that $Q$ is an overapproximation of all states that may be reached by executing $s$, starting from a state in $P$. The intuition in Hoare logic is that one will often attempt to prove a triple like $\{P\} s \{\neg X\}$ for a set of bad states $X$, which ensures that execution of $s$ cannot reach $X$.

Unrealizability logic operates on the same overapproximation principle, but differs in two main ways from standard Hoare logic. The differences are motivated by how synthesis problems are typically defined, using two components: (i) a search space $S$ (i.e., a set of programs), and (ii) a (possibly infinite) set of related input-output pairs $\{(i_1, o_1), (i_2, o_2), \cdots \}$. 
To reason about sets of programs, in unrealizability logic, the central element (i.e., the program $s$) is changed to a set of programs $S$. The unrealizability-logic triple

$$\{P\} \rightarrow \{Q\}$$

thus asserts that $Q$ is an overapproximation of all states that are reachable by executing any possible combination of a pre-state $p \in P$ and a program $s \in S$. More formally, the following theorem holds for any unrealizability triple $\{P\} \rightarrow \{Q\}$:

**Theorem 2.1.** The unrealizability triple $\{P\} \rightarrow \{Q\}$ for a precondition $P$, postcondition $Q$, and set of programs $S$, holds iff for each program $s \in S$, the Hoare triple $\{P\} s \{Q\}$ holds.

The second difference concerns input-output pairs: in unrealizability logic, we wish to place the input states in the precondition, and overapproximate the set of states reachable from the input states (through a set of programs) as the postcondition. Unfortunately, the input-output pairs of a synthesis problem cannot be tracked using standard pre- and postconditions; nor can they be tracked using auxiliary variables, because of a complication arising from the fact that unrealizability logic must reason about a set of programs (see §2.2).

To keep the input-output relations in check, the predicates of unrealizability logic talk instead about (potentially infinite) vector-states, which are sets of states in which each individual state is associated with a unique index. Variable $x$ of the state with index $i$ is referred to as $x_i$.

**Example 2.2 (Vector-States).** Assume we are given a set of input-output state pairs $\{(x = i_1, x = o_1), (x = i_2, x = o_2), \ldots, (x = i_n, x = o_n)\}$. Then the input vector-state $I$ is denoted by $(x_1 = i_1) \land (x_2 = i_2) \land \cdots \land (x_n = i_n)$. The output vector-state $O$ is denoted by $(x_1 = o_1) \land (x_2 = o_2) \land \cdots \land (x_n = o_n)$. Once $I$ and $O$ have been constructed this way, the proof steps of an unrealizability-logic proof would relate $x_i$ in the precondition to $x_i$ in the postcondition; one has effectively expressed the relation given by the input-output pairs by renaming each input-output pair to be unique.

Keeping these two differences in mind, let us turn to proving unrealizability. Recall that a synthesis problem is given as a search space $S$ and a set of input-output pairs $Ex = \{(i_1, o_1), \ldots\}$. To prove unrealizability, one must prove that for every program $s \in S$, there is at least one input-output pair $(i_k, o_k) \in Ex$ such that $s$ does not map $i_k$ to $o_k$. Note that $\neg O$ denotes the set of all output vector-states for which at least one input-output pair does not hold. Then, because of Theorem 2.1, proving $\{I\} s \{
eg O\}$ for all $s \in S$ is equivalent to proving the unrealizability triple

$$\{I\} \rightarrow \neg \{O\}.$$  

The goal of unrealizability logic is to prove such triples in a principled logical system, without having to descend to the level of individual programs or input-output pairs.

Fig. 1 summarizes what we have discussed so far. In general, in unrealizability logic the input vector-state need not be finite, and the spec need not be functional as well—for example, a synthesis problem that should assign some value $o > x$ to $x$, for all possible $x$, can be proved unrealizable via the triple $\forall i. x_i = i \rightarrow L(G) \forall i. x_i \leq i$.

### 2.1 Challenge 1: Infinite Sets of Programs

Compared to ordinary Hoare logic, the first challenge is that unrealizability logic needs to reason about infinite sets of programs. Fortunately, the set of programs in a program-synthesis problem is typically formulated as a regular tree grammar (RTG), which defines the set of programs in an inductive manner. Unrealizability logic uses the structure of the RTG to develop proof trees that mimic structural induction.
which is a set of triples that stores all the induction hypotheses that have been introduced up to

The idea is that instead of reasoning about the provability of triples directly, we wish to reason

That is,$\ G \ ⌦\grammar$.

\begin{align*}
\text{Precondition:} & \quad \text{multiple possible inputs} \quad \text{Body:} \quad \text{Set of programs} \quad \text{Postcondition:} \quad \text{at least one incorrect output} \\
\begin{cases}
x_1 = i_1 \land x_2 = i_2 \land x_3 = i_3 \land \cdots \\
\end{cases} & \quad L \quad \begin{cases}
\text{Start} \to \cdots \\
E \to \cdots \\
\end{cases} & \quad \begin{cases}
x_3 \neq o_1 \lor x_2 \neq o_2 \lor \cdots \\
\end{cases}
\end{align*}

\text{Vector-state (I)} \quad \text{Grammar} \quad \text{Negated vector-state (¬O)}

Fig. 1. An unrealizability triple with a negated post-vector-state asserts that a synthesis problem is unrealizable.

Observe how the vectorized version of ¬O asserts that there is at least one output example that does not satisfy the desired input-output relation.

As illustrated earlier, the unrealizability triple $\{P\} S \{Q\}$ captures information about the set of programs $S$. If $S$ is specified in a recursive manner via an RTG, a triple $\{P\} S \{Q\}$ can also be used as an induction hypothesis in a proof tree for unrealizability logic, as we show in Example 2.3.

\textbf{Example 2.3.} Consider a simple synthesis problem $sy_e$ with the following grammar:

\begin{align*}
\text{Start} & \to \text{S2} | \text{S3} \\
\text{S2} & \to \text{S2}; \text{S2} | x := x + 2 \\
\text{S3} & \to \text{S3}; \text{S3} | x := x + 3
\end{align*}

That is, $sy_e$ consists of programs that either (i) repeatedly add 2 to $x$, or (ii) repeatedly add 3 to $x$.

Now suppose that the input specification to $sy_e$ was given as $x \equiv_6 0$ (we use $x \equiv_r p$ as shorthand for $x \equiv r \mod p$); i.e., that $x$ is equivalent to $r$ modulo $p$ and the output specification given as $x \equiv_6 1$; that is, the goal is to reach a number of the form $6k' + 1$ when starting from a number $6k$. This problem is unrealizable, because one can only reach $6k'$, $6k' + 2$, $6k' + 3$, or $6k' + 4$ by repeatedly adding 2 or 3 (but not both) to a multiple of 6. We formalize this reasoning as a proof tree in unrealizability logic.

\textbf{Starting the Proof Tree.} To prove the synthesis problem $sy_e$ unrealizable, one wishes to prove the following triple, where the output is negated from the specification:

\begin{align*}
\{x \equiv_6 0\} \quad \text{Start} \quad \{x \not\equiv_6 1\}
\end{align*}

From this point on, a nonterminal as the center element of an unrealizability triple refers to the language of that nonterminal; e.g., $\{x \equiv_6 0\} \quad \text{Start} \quad \{x \not\equiv_6 1\}$ refers to $\{x \equiv_6 0\} \quad L(\text{Start}) \quad \{x \not\equiv_6 1\}$.

Note that the postcondition $x \not\equiv_6 1$ is bigger than our previously discussed reachable states of $6k'$, $6k' + 2$, $6k' + 3$, and $6k' + 4$. Hence, the target triple can be proved by proving the following triple and then weakening it (Weaken in Fig. 7):

\begin{align*}
\{x \equiv_6 0\} \quad \text{Start} \quad \{x \equiv_6 0 \lor x \equiv_6 2 \lor x \equiv_6 3 \lor x \equiv_6 4\}
\end{align*}

To prove this triple in unrealizability logic, we must first introduce the concept of a context $\Gamma$, which is a set of triples that stores all the induction hypotheses that have been introduced up to some point in a proof tree. Consequently, the judgements of the proof tree have the form:

\begin{align*}
\Gamma \vdash \{P\} S \{Q\}
\end{align*}

The idea is that instead of reasoning about the provability of triples directly, we wish to reason about the provability of a triple assuming that every hypothesis inside $\Gamma$ is true.

In our case, we wish to prove that $\{x \equiv_6 0\} \quad \text{Start} \quad \{x \equiv_6 0 \lor x \equiv_6 2 \lor x \equiv_6 3 \lor x \equiv_6 4\}$ without assuming anything (i.e., starting from the empty context). This triple can be established by proving that the following judgement holds (where the blank LHS denotes an empty context):

\begin{align*}
\vdash \{x \equiv_6 0\} \quad \text{Start} \quad \{x \equiv_6 0 \lor x \equiv_6 2 \lor x \equiv_6 3 \lor x \equiv_6 4\}
\end{align*}
The key point in taking the next step is to notice that the language of the nonterminal \( \text{Start} \), \( L(\text{Start}) \), is the union of \( L(S2) \) and \( L(S3) \). Because unrealizability logic deals with sets of programs, it is equipped with rules for merging triples over different sets of programs. In particular, we can apply the grammar-disjunction rule of unrealizability logic (\text{GrmDisj} in Fig. 7), which states that if two program sets satisfy the same pre- and postcondition pair, their union also satisfies the aforementioned pair. In this case, \text{GrmDisj} is applied on our target triple as follows:

\[
\Gamma_{S2} \vdash \{ x \equiv 2 \} S2 \{ x \equiv 2 \} \]

This violates a hypothesis, because \( S2 \) is defined recursively, taking a naive consideration of the productions from \( S2 \) and \( S3 \) will result in an infinite proof tree. To avoid this problem, one must introduce the triples one wishes to prove as hypotheses in the context, and validate them in a procedure similar to structural induction.

**Introducing Hypotheses.** To see how hypotheses are introduced, consider the nonterminal \( S2 \). The idea is that one wishes to introduce the target triple \( \{ x \equiv 0 \} S2 \{ x \equiv 0 \} \) as an induction hypothesis about nonterminal \( S2 \), and prove that this triple holds in a way similar to structural induction. Introducing a new hypothesis can be done using the HP rule in Fig. 7, which splits the proof according to nonterminal \( N \)'s productions: in this case, nonterminal \( S2 \) is split into \( x := x + 2 \) and \( S2; S2 \) (the first application of HP in Fig. 2).

As the hypothesis for \( S2 \), we introduce the triple \( \{ x \equiv 0 \} S2 \{ x \equiv 0 \} \) via an application of Weaken (in fact, \( \{ x \equiv 0 \} S2 \{ x \equiv 0 \} \) will not work as a hypothesis directly for \( S2 \), as we will explain later in this section).

We will use \( \Gamma_{S2} \) to denote the singleton context \( \{ x \equiv 0 \} S2 \{ x \equiv 0 \} \). Fig. 2 depicts the proof tree for \( \Gamma_{S2} \), where the application of HP at the root of the proof tree introduces the \( \Gamma_{S2} \) context in the two premises.

**Proving Hypotheses.** If one were proving a property about \( S2 \) using standard structural induction, one would proceed to show that the property holds on the two sub-cases, \( x := x + 2 \) and \( S2; S2 \)—i.e., the two productions from \( S2 \)—while assuming that the property holds as a hypothesis. The same approach is used here: we assume \( \{ x \equiv 2 \} S2 \{ x \equiv 2 \} \) as a hypothesis (in context \( \Gamma_{S2} \)), and attempt to prove that \( x \equiv 2 \) is a valid pre- and postcondition of both \( x := x + 2 \) and \( S2; S2 \).

First, consider proof goal \( 1 \) for \( x := x + 2 \). The set of programs generated by the right-hand side of this production is completely independent of how \( S2 \) is defined; thus, for the purpose of performing structural induction on \( S2 \), it is a base case. Here, we invoke the basic rule for assignment to prove \( 1 \). Auxiliary variable \( e_I \) stores the result of the expression \( x + 2 \), which is then assigned
to $x$ through the Assign rule (in which the postcondition of the conclusion mimics that of the forwards-based assignment rule in Hoare logic). The resulting postcondition can then be weakened to obtain $x \equiv 2$, which completes the proof that $\{ x \equiv 2 \} \ x := x + 2 \ \{ x \equiv 2 \}$.

Next, consider proof goal \(2\) for \(S2\); \(S2\). Here, nonterminal \(S2\) appears directly, and provides us with a chance to apply the induction hypothesis via the rule \(\text{ApplyHP}\) in Fig. \(7\). In Figure \(2\), the derivation for \(2\) is the sub-proof tree on the right. Notice how \(S2\); \(S2\) is first decomposed using the \(\text{Seq}\) rule for sequential composition (identical to that in Hoare logic), which requires us to prove two instances of the proof goal \(2\); in turn, these two instances are proved by directly applying the induction hypothesis through \(\text{ApplyHP}\).

Returning to nonterminal \(\text{Start}\), the second premise $\{ x \equiv 0 \} \ S3 \{ x \equiv 0 \lor x \equiv 0 \land x \equiv 3 \land x \equiv 0 \land 4 \}$ can be similarly proved by introducing the triple $\{ x \equiv 3 \} \ S3 \{ x \equiv 3 \}$ as a hypothesis for nonterminal \(S3\), and weakening it to get the target triple about \(S3\). This step concludes our proof.

One take-away from Example 2.3 is the importance of choosing an appropriate induction hypothesis. For instance, attempting to use the proof goal $\{ x \equiv 0 \} \ S2 \{ x \equiv 0 \lor x \equiv 0 \land x \equiv 3 \land x \equiv 0 \land 4 \}$ directly as a hypothesis for \(S2\) would make the proof fail on the production \(S2\); \(S2\). This example indicates that, similar to how identifying appropriate invariants for loops is a key component of writing Hoare logic proofs, identifying appropriate hypotheses for nonterminals is an essential part in completing a proof in unrealizability logic.

### 2.2 Challenge 2: Tracking (Infinite) Input-Output Relations

The second challenge in unrealizability logic is that the specification of a synthesis problem is typically given as a set of input-output \textit{pairs}: a specific input value is associated with a specific output value. (Even if the specification is given as a universally quantified formula, one can understand such a formula as an infinite set of input-output pairs.) The standard way to address this problem in Hoare logic is to introduce auxiliary variables that freeze the values of program variables in the precondition, and to allow the postcondition to refer to these auxiliary variables. However, this approach alone is unsuitable for unrealizability logic, as illustrated by the following example.

\begin{quote}
\textbf{Example 2.4.} Consider the identity assignment $x := x$. The Hoare triple for this program is typically given as $\{ x = x_{\text{aux}} \} \ x := x \ \{ x = x_{\text{aux}} \}$; that is, starting from $x = x_{\text{aux}}$, where $x_{\text{aux}}$ is an \textit{auxiliary variable}, one ends up in $x = x_{\text{aux}}$. Strictly speaking, the auxiliary variable $x_{\text{aux}}$ is quantified \textit{outside} the Hoare triple: $\forall x_{\text{aux}} \{ x = x_{\text{aux}} \} x := x \ \{ x = x_{\text{aux}} \}$; this position for the quantifier indicates that the triple should hold for every value of $x_{\text{aux}}$.

Now suppose that we are given a synthesis problem $\text{sy}_{\text{id}}$, where the goal is to synthesize a program equivalent to $x := x$, using the grammar $G_{\text{id}}$ below:

\[
\begin{align*}
\text{Start} & \rightarrow x := E \\
E & \rightarrow 0 \mid E + 1 \mid E - 1
\end{align*}
\]

For every integer $i$, the set $L(E)$ contains a constant expression that evaluates to $i$, and thus $L(\text{Start})$ consists of exactly the set of all constant assignments. However, synthesizing a statement that is computationally equivalent to $x := x$ is \textit{impossible} because the set only contains constant assignments—i.e., $\text{sy}_{\text{id}}$ is unrealizable.

Suppose that one tries to specify $\text{sy}_{\text{id}}$ using an auxiliary variable, so that the goal is to prove $\{ x = x_{\text{aux}} \} \ \text{Start} \ \{ x \neq x_{\text{aux}} \}$. Unfortunately, this triple is \textit{invalid} in unrealizability logic, in the sense that starting from the precondition $x = x_{\text{aux}}$, one can actually reach a state where still, $x = x_{\text{aux}}$.

To understand this seemingly counterintuitive fact, we will attempt to prove the triple $\{ x = x_{\text{aux}} \} \ \text{Start} \ \{ \exists k. x = k \}$ (where $k$ indicates that $x$ may have any value in the post-state).

To do so, let us first characterize the behavior of all programs in the language of $E$. In doing so, one will generate the following hypothesis (where, again, $e_t$ is an auxiliary variable for storing the
value obtained from executing $E$):

$$\{x = x_{aux}\} E \{x = x_{aux} \land \exists k. e_t = k\}.$$  

The best one can say about terms in $E$ is that there exists an integer $k$ whose value is $e_t$. Applying Assign and Weaken to the triple, one can derive the following (precise) triple:

$$\{x = x_{aux}\} \text{Start} \{\exists k. x = k\}.$$  

Like in Hoare logic, the quantification for $x_{aux}$ is outside the unrealizability triple, which yields:

$$\forall x_{aux}. \{x = x_{aux}\} \text{Start} \{\exists k. x = k\}.$$  

This triple says that for every value of $x_{aux}$, there is some $k$ (and a corresponding program) that works; thus, this triple actually asserts that the problem is realizable (which is clearly not true)!

The problem is that, while for every individual value of $x_{aux}$ there does indeed exist a suitable $k$ (corresponding to a specific expression $t_k \in L(E)$ that always evaluates to $k$), any such value of $k$ (and expression $t_k$) fails to work for other values of $x_{aux}$—i.e., the use of a single auxiliary variable fails to capture the fact that the multiple input-output pairs must all be satisfied simultaneously. In terms of synthesis, for each input, some program in the search space will work: but this does not guarantee the existence of a program that works for all inputs (such a program does not exist).

The issue illustrated in Example 2.4—where one must ensure that each input must map to some specific output, but all via the same program—has appeared in other work on unrealizability. For example, Nay [11] uses semi-linear sets over LIA to capture this relation (albeit for a specific class of synthesis problems), while Nope [10] constructs a program that executes each example in lockstep.

In this paper, we show that these relations can be elegantly expressed as unrealizability triples by (i) merely renaming the set of variables to which each example refers to be unique; (ii) conjoining all the renamed states into a single, big state, and (iii) modifying the semantics of programs to execute over the renamed variables. As discussed in Example 2.2, we refer to the renamed, conjoined big states as vector-states because the renaming and conjoining process can be intuitively understood as vectorizing the input states, and then executing the program on the single vector. As shown in Example 2.4, and as we will later show in §5, having a simple logical representation allows us to extend the vector-states toward infinite examples, which allows us to prove unrealizability for problems beyond the reach of previous work [10, 11, 14].

**Example 2.5 (Two examples).** Consider again the synthesis problem $sy_{id}$ and grammar $G_{id}$ from Example 2.4. Suppose that the specification for $sy_{id}$ is given as a set of two input-output examples: $\{(x = 1 \mapsto x = 1), (x = 2 \mapsto x = 2)\}$. Then the input and output specifications can both be expressed as the vector-state $\{x_1 = 1 \land x_2 = 2\}$, where $x_1$ corresponds to the first example and $x_2$ corresponds to the second example. The following triple is valid in unrealizability logic, i.e., the two examples suffice to demonstrate that $sy_{id}$ is unrealizable:

$$\{x_1 = 1 \land x_2 = 2\} L(\text{Start}) \{x_1 \neq 1 \lor x_2 \neq 2\}.$$  

In turn, this triple may be derived from the triple:

$$\{x_1 = 1 \land x_2 = 2\} L(\text{Start}) \{\exists k. x_1 = k \land x_2 = k\},$$  

which states that there must exist a $k$ for which both $x_1$ and $x_2$ are equivalent to $k$ in the post-state. This condition implies that $x_1$ and $x_2$ are identical, and thus implies that $x_1 \neq 1 \lor x_2 \neq 2$.

Example 2.5 illustrates how unrealizability can be proved using two examples; in §5, we present problems for which proving unrealizability requires infinitely many examples.

The fact that the input-output examples can be packed into a single vector-state is important: because the starting precondition contains only a single vector-state, all examples inside the single
vector-state are guaranteed to be executed on the same program in the grammar. Likewise, because all the output examples are packed into a single vector-state, the negation of this vector-state is guaranteed to contain all vector-states that are wrong on at least one input example.

### 2.3 Why Not Recursive Hoare Logic?

At this point, readers familiar with Hoare logic extended toward recursive procedures [1, 18] may notice that the proof structure described in §2.1 is similar to proofs in recursive Hoare logic. In fact, the similarity between program-synthesis problems and nondeterministic, recursive procedures has already been exploited in Nope [10], which constructs a recursive program from a synthesis problem, then relies on an external verifier to check whether the problem is unrealizable.

Then what is the problem with applying recursive Hoare logic to programs translated in this way? The answer is that some features of synthesis problems are difficult to model as a nondeterministic recursive program—e.g., loops and infinite examples (both of which Nope cannot support).

With while loops, the problem is that a nondeterministic modelling as described in [10] must have a way of recording the unbounded choices that were selected when synthesizing the while-loop body, due to the fact that a loop body must stay fixed throughout multiple iterations.

**Example 2.6 (Multiple Loop Bodies).** Consider a variant of $s_y_e$ from Example 2.3, where the grammar has been modified to contain while loops instead of sequential composition:

```
Start → while B do S     B → x < 100     S → x := x + 2 | x := x + 3
```

$s_y_e$ still consists of programs that repeatedly add either 2 or 3 to $x$. However, the repeated addition is performed within a loop (until $x \geq 100$). The search space consists of exactly two programs: one in which the loop body is $x := x + 2$, and one in which the loop body is $x := x + 3$. Starting from $x \equiv_0 0$, $x \equiv_2 0$ is an invariant of the first program, and $x \equiv_3 0$ is an invariant of the second program.

Nope [10] constructs a nondeterministic, recursive program from a synthesis problem, where each nonterminal is translated into a procedure. The basic idea is that executing the translated procedure returns the result of executing that nonterminal—where the nondeterministic choices of an RTG are mimicked by nondeterministic choices in the procedure.

A naive translation of $s_y_e$ into a nondeterministic program following this idea would result in a program like the one in Figure 3. The problem with Figure 3 is that there is no machinery present to ensure that the same loop body is repeated for each iteration—thus, an analysis of Figure 3 would report that states in which, e.g., $x \equiv_6 1$ holds are possible! To fix this, Figure 3 would require, e.g., a list capable of recording the nondet() choices in $S()$ directly embedded in the program—moreover, this list must be unbounded, because, in general, a term within a RTG may be of unbounded size.

In unrealizability logic, one does not need such complex machinery—instead, one can perform simple invariant-based reasoning. Because unrealizability logic is tailored for synthesis problems, one can first split the search space through GrmDisj, as illustrated in Example 2.3, to consider the two loops “while $B$ do $x := x + 2$” and “while $B$ do $x := x + 3$” separately. At this point, it becomes clear that $\{x \equiv_0 0 \} x := x + 2 \{x \equiv_2 0 \}$ and $\{x \equiv_3 0 \} x := x + 3 \{x \equiv_3 0 \}$ are invariants for each of the loops. An additional application of Weaken yields the desired triple $\{x \equiv_6 0 \} Start \{x \equiv_2 0 \lor x \equiv_3 0 \}$. (While it is possible to reason about both loops via a single invariant, as suggested in §3.3, such an invariant is likely to be too complex; see §3.3 and Lemma 4.3 for details.)
Fig. 4. The base grammar \( G_{imp} \), which defines a universe of terms that we are interested in for this paper.

The second problem with trying to apply recursive Hoare logic has to do with dealing with infinitely many examples, or more generally, with vector-states themselves: vector-states provide unrealizability logic a way to ensure that multiple examples are executed along the same program. Nope [10] creates copies of sets of variables for each different example when translating the synthesis problem into a program. However, creating copies of variables for each example requires an infinite number of variables in the program to support infinite examples. Programming languages, much less program verifiers, typically do not support—or struggle to support—programs with infinite variables, which is why previous attempts such as Nope fail to support cases with infinite examples.

It is true that, if one is willing to develop a logic supporting all necessary features: recursion, nondeterminism, both local and global variables, infinite data structures, and infinite vector-states, then it would be possible to prove unrealizability via an extended Hoare logic. However, to the best of our knowledge, there is no comprehensive study of a system containing all of these features at once, whereas this paper proves soundness, relative completeness, and some other decidability results related to unrealizability and unrealizability logic.

Moreover, such a logical system would be more complex than required to reason about unrealizability—for example, a record-and-replay encoding of while loops as suggested in Example 2.6 completely hides the fact that one is processing a while-loop production, and thus prevents simple invariant-based reasoning about loops. Such drawbacks are in direct conflict with the goal of unrealizability logic, which—as stated in §1—is to provide a simple logical system that distills the essence of proving unrealizability. True to this goal, the While rule for loops in unrealizability logic does allow one to perform invariant-based reasoning for loops, and provides similar direct reasoning principles for other constructs as well.

3 UNREALIZABILITY LOGIC

In this section, we formally define unrealizability logic and some necessary preliminaries.

3.1 Preliminary Definitions

In this paper, we consider synthesis problems where the search space is a subset of all terms producible by the imperative grammar \( G_{imp} \) (Figure 4)—that is, deterministic, expression-based or imperative synthesis problems defined over integer arithmetic expressions. We assume a function \([\cdot] \) that defines the standard semantics of every term \( t \in L(G) \). We leave supporting synthesis problems involving more complex operations, e.g., recursive data structures, to future work; this paper lays the foundations for making such extensions possible.

**Definition 3.1 (Regular Tree Grammar).** A (typed) regular tree grammar (RTG) is a tuple \( G = (\mathcal{N}, \mathcal{A}, S, a, \delta) \), where \( \mathcal{N} \) is a finite set of nonterminals; \( \mathcal{A} \) is a ranked alphabet; \( S \in \mathcal{N} \) is an initial nonterminal; \( a \) is a type assignment that gives types for members of \( \mathcal{A} \cup \mathcal{N} \); and \( \delta \) is a finite set of productions of the form \( N_0 \rightarrow a^{(i)}(N_1, ..., N_i) \), where for \( 0 \leq j \leq i \), each \( N_j \in \mathcal{N} \) is a nonterminal such that if \( a^{(i)} = (\tau_0, \tau_1, ..., \tau_i) \) then \( a_{A_j} = \tau_j \).
In our setting, the alphabet consists of constructors for each of the constructs of $G_{imp}$ (although for simplicity we write, e.g., $x := 0$, rather than $\vdash (x, 0)$). $G_{imp}$ contains three types of nonterminals: statement nonterminals, expression nonterminals, and Boolean-expression nonterminals.

We assume grammars use productions that differ from the ones in $G_{imp}$ only due to the nonterminal names. We say that a production $N_0 := a(N_1, \ldots, N_i)$ is valid with respect to $G_{imp}$ iff replacing each nonterminal $N_j$ with the nonterminal of the same type in the set $\{S, E, B\}$ yields a production in $G_{imp}$, e.g., production $S_1 := S_2 \cdot S_3$ is valid with respect to $G_{imp}$.

**Definition 3.2 (Synthesis Problem).** A synthesis problem is a 4-tuple $sy = (G, f, I, \psi)$, where

- $G$ is a regular-tree grammar consisting of productions that are valid with respect to $G_{imp}$,
- $f$ is the name of the function to synthesize,
- $I$ is the set of allowed input states of $f$ (i.e., the domain of $f$),
- $\psi$ is a Boolean formula that describes a behavioral specification that $f$ must satisfy.

The goal of a synthesis problem is to find $f^* \in L(G)$ such that $\forall r \in I. \psi([f^*](r), r)$. If such an $f^* \in L(G)$ exists, synthesis problem $sy$ is realizable; otherwise, $sy$ is unrealizable.

A key point from Definition 3.2 is that the search space is defined as an RTG. As noted in §2.1, this property is used by unrealizability logic to build proof trees that mimic structural induction.

### 3.2 Basic Definitions for Unrealizability Logic

We now introduce some concepts that are specific to unrealizability logic.

In this paper, we will use (and have used) the following notation for different kinds of states:

- Lowercase letters (e.g., $p, q, r$) for ordinary states,
- Uppercase letters (e.g., $P, Q$) for sets of ordinary states (and also predicates over states),
- Lowercase Greek letters (e.g., $\sigma, \pi$) for vector-states (as shown in §2, defined in Definition 3.4),
- Cursive uppercase letters (e.g., $\mathcal{P}, \mathcal{Q}$) for sets of (and predicates describing) vector-states.

Sometimes, uppercase letters are used also to denote nonterminals, i.e., sets of programs, and lowercase letters used to denote single programs. It should be clear from context, in these cases, what the upper- and lowercase letters denote.

In unrealizability logic, the semantics of expressions are extended such that an expression does not evaluate to a value, but evaluates to a state that stores the value $v$ inside a (reserved) auxiliary variable $e_t$ (or $b_t$ for Boolean expressions). This non-standard approach is taken because, as we will see in §3.3, simply generating values will lose some information that is required to precisely compute the set of states that a nonterminal can generate.

**Definition 3.3 (Semantics of Expressions).** Let $[\cdot]_{ext}$ be a semantics for expressions that evaluates an expression to a state instead of a value. Intuitively, we will store the value resulting from computing an expression to a reserved variable $e_t$ in the state.

Given a ‘standard’ semantics $[\cdot]$ for expressions that evaluates expressions to values, let $[e]_{ext}(\sigma) = \sigma[e_t \mapsto [e](\sigma)]$ if $e$ is an atomic expression (0, 1, or $x$). (If $e$ is an atomic Boolean expression, true or false, the assignment is to $b_t$ instead).

If $e$ is a $n$-ary operation, with $e = e_1 + e_2$ as an example, let $[e_1 + e_2]_{ext}(\sigma) = \sigma[e_t \mapsto [e_1]_{ext}(\sigma)[e_t] + [e_2]_{ext}(\sigma)[e_t]]$; that is, $[\cdot]_{ext}$ is defined recursively such that the extended semantics of operators such as $\cdot$, i.e., $[\cdot]_{ext}$, are state transformers as well. These semantics work by referencing the value of $e_t$ stored in the state that each sub-expression $e_1$ and $e_2$ evaluates to (likewise, if $e$ is a $n$-ary Boolean operation, the final assignment is to $b_t$ instead; Boolean sub-expressions will also reference $b_t$ instead of $e_t$).

2In this paper, we sometimes write a production in which some terminals are in-lined in place of nonterminals—e.g., we write $S := x := x$ in place of the two productions $S := x := \text{Ex}, E_{x} := x$. 
We define the extended semantics recursively, instead of simply stating that \( \overline{[\mathit{e}]_\mathit{ext}(\mathit{\sigma}) = \mathit{\sigma}[\mathit{e}] \rightarrow \overline{[\mathit{e}]_{\mathit{ext}}(\mathit{\sigma})} \), because we wish the rules of unrealizability logic to be recursive, and thus need to define operations such as addition on states. In the rest of this paper, we will take \( \overline{[\mathit{e}]_{\mathit{ext}}} \) from Definition 3.3 to be the standard semantics given to a term, and thus drop the subscript \( e \) for clarity.

As we showed in §2, to capture input-output relations, unrealizability logic relies on vector-states and a semantics modified to run on vector-states, which we now formalize.

**Definition 3.4 (Vector-State).** Let \( r_1, \ldots, r_n \) be a collection of states defined over the same set of variables \( V \). A vector-state \( \mathit{\sigma} \) over \( r_1, \ldots, r_n \), denoted by \( \mathit{\sigma} = \langle r_1, \ldots, r_n \rangle \), is a state defined over the set of variables \( \bigcup_{1 \leq i \leq n} V_i \), where

- \( V_i = \{ v_i \mid v \in V \} \) is the set of variables in which each variable in \( V \) is subscripted with symbol \( i \).
- For all \( v \in V \) and \( 1 \leq i \leq n \), \( \mathit{\sigma}(v_i) = r_i(v) \).

A vector-state may also be defined over an infinite collection of states indexed by the elements of an (infinite) domain \( D \), in which case \( \mathit{\sigma} \) is a state defined over the set of variables \( \bigcup_{i \in D} V_i \), for \( V_i = \{ v_i \mid v \in V \} \), and for all \( v \in V \) and \( i \in D \), \( \mathit{\sigma}(v_i) = r_i(v) \).

A vector-state \( \mathit{\sigma} \) over the states \( r_1, \ldots, r_n \) is itself an ordinary state over an expanded vocabulary, and may be understood as a vector of individual states. Executing a program on a vector-state produces a vector-state equivalent to the vector obtained by running each individual state through the program separately. This idea is reflected in Def. 3.5 below, which extends the program semantics to a semantics that works on vector-states, and further to sets of vector-states and programs.

**Definition 3.5 (Vector-State Semantics).** The semantics of a program construct \( t \) on a single vector-state \( \mathit{\sigma} = \langle r_1, \ldots, r_n \rangle \) is defined as \( \overline{[t](\mathit{\sigma})} = \langle \overline{[t](r_1)} \rangle, \ldots, \overline{[t](r_n)} \rangle \). The semantics of \( t \) on a set of vector-states \( \mathcal{P} \) is defined as \( \overline{[t](\mathcal{P})} = \bigcup_{\mathit{\sigma} \in \mathcal{P}} \overline{[t](\mathit{\sigma})} \). The semantics of a set of programs \( T \) on a set of vector-states \( \mathcal{P} \) is defined as \( \overline{[T](\mathcal{P})} = \bigcup_{\mathit{\sigma} \in \mathcal{P}} \overline{[T](\mathit{\sigma})} \).

The semantics of a set of programs on a set of input states can be understood as producing the set of all states that may arise from taking any combination of a program \( t \in T \) and a (vector-) state \( \mathit{\sigma} \in \mathcal{P} \). This semantics allows us to define the validity of unrealizability triples: a triple \( \{ \mathcal{P} \} \uparrow \{ \mathcal{Q} \} \) is valid iff \( \mathcal{Q} \) overapproximates the states that may result from any combination of \( \mathit{\sigma} \in \mathcal{P} \) and \( t \in T \).

**Definition 3.6 (Validity).** Given a precondition over vector-states \( \mathcal{P} \), and a postcondition over vector-states \( \mathcal{Q} \), an unrealizability triple \( \{ \mathcal{P} \} \uparrow \{ \mathcal{Q} \} \) is valid for a set of programs \( T \), denoted by \( \models \{ \mathcal{P} \} \uparrow \{ \mathcal{Q} \} \), iff \( \overline{[T](\mathcal{P})} \subseteq \overline{[T](\mathcal{Q})} \).

As previously stated as Theorem 2.1, \( \models \{ \mathcal{P} \} \uparrow \{ \mathcal{Q} \} \) iff for all \( t \in T \), \( \{ \mathcal{P} \} \models \{ \mathcal{Q} \} \) is a valid Hoare triple. Connecting all the definitions, we state that:

A synthesis problem \( sy = \langle G, f, I, \psi \rangle \) is unrealizable if \( \models \{ I(r) \} \models N \{ \neg \psi(f(r), r) \} \) is a valid unrealizability triple. Here, \( N \) is the initial nonterminal of \( G \), and \( I \) and \( \psi \) are predicates that describe the vectorized input and output conditions of the synthesis problem.

### 3.3 The Rules of Unrealizability Logic

We now present the inference rules of unrealizability logic. One issue to discuss before presenting the rules is the choice of assertion language—that is, the language used for the pre- and postconditions of unrealizability triples. The additional predicates generated by the rules of unrealizability logic itself are within first-order Peano arithmetic (FO-PA), which means that one must choose an assertion language at least as expressive as FO-PA; if not, the predicates occurring in a proof tree may be beyond the power of the assertion language. If one does choose an assertion language at least as expressive as FO-PA, then the assertions occurring in a proof tree are guaranteed to stay within that
language. Unrealizability logic itself is parametric in the choice of assertion language, as long as it is at least as expressive as FO-PA—e.g., one may choose to use FO-PA, or use a logic that extends FO-PA with infinite variables to model infinite input examples (as we will do in §5, Example 5.1).

The goal of unrealizability logic is to prove unrealizability for synthesis problems defined over an RTG. Therefore, the rules that we state in Figures 5, 6, and 7 are for sets of programs defined as $L(N)$ for some RTG nonterminal $N$, or as the language of the right-hand side of an RTG production.

### 3.3.1 Rules for Expressions

Recall that in Definition 3.3 we defined the semantics of expressions to update the value of a reserved auxiliary variable $e_t$ instead of generating a value. The rules for expressions reflect this fact: in every expression rule, the postcondition of the conclusion takes the form $\exists e'_t.P[e'_t/e_t] \land e_t = e$, where $P$ is some predicate and $e$ is a vector that encodes the values that may be generated by an expression in the set of expressions considered. Observe that the form of this predicate mimics the postcondition in the forwards-assignment rule of Hoare logic [7], where we are updating the vector-variable $e_t$: the assignment is to a vector-variable because we are working with vector-states (as opposed to single states, as in Definition 3.3).

The intuition that $e_t$ contains the value generated by the expression nonterminals can be formalized into an invariant about expression nonterminals:

**Lemma 3.7.** Given an expression nonterminal $E$, if an unrealizability triple $E \vdash P \cdot E \cdot Q$ is derivable using the rules of unrealizability logic under some context $\Gamma$, then for every $e \in L(E)$ and for every $\sigma \in P$, the formula $Q[\langle e \rangle(\sigma)/e_t]$ is true assuming all triples in $\Gamma$ are true (where in this case, $[\langle e \rangle(\sigma)$ refers to the standard semantics that evaluates $e$ to a value).
Lemma 3.7 is important, because it allows the postcondition of the conclusion to refer to the values computed by expression nonterminals through use of the variable $e_i$ (or $b_i$). In particular, we assume that $e_i$ and $b_i$ are reserved for the purposes of storing these values. (More precisely, we assume that $e_i$ and $b_i$ are included in the set of program variables $\text{vars}(N)$, and thus rules such as Sub1 cannot substitute these variables.)

Figure 5 presents the rules for each expression-based operator in unrealizability logic. Having articulated the key intuition behind the rules, let us now look at each rule in detail.

0-ary operators ($0, 1, x, t, f$). Rules for 0-ary operators do not rely on the result of another set of programs, and can be computed directly by assigning the correct values ($0, 1, x, \text{etc.}$) to the auxiliary (vector-)variable $e_i$. The symbol $x$ in the rule Var refers to the vector of values generated by taking $x$ from each sub-state of $\sigma = \langle r_1, r_2, \cdots \rangle$; i.e., $\langle r_1(x_1), r_2(x_2), \cdots \rangle$.

Unary Operators ($\text{!}$). $G_{\text{imp}}$ only contains a single instance of a unary operator, Not ($\text{!}$), which takes the value produced by a nonterminal $B$ and negates it. The rule Not mirrors this behavior: it first requires that the behavior of the nonterminal $B$ is captured by the premise $\{P\} \ B \ \{Q\}$. Following Lemma 3.7, the result of executing $B$ is stored in the variable-vector $b_i$; that is, by referring to the variable-vector $b_i$ in $Q$, one can refer to the (set of possible) values created by $B$. The conclusion of the rule negates the value in $b_i$ and re-assigns it to $b_i$ (captured in the postcondition predicate $\exists b_i'. Q[b_i'/b_i] \land b_i = \neg b_i'$).

Binary Operators ($E_1 + E_2, E_1 - E_2, E_1 \cdot E_2, E_1/E_2, B_1 \land B_2, E_1 < E_2, E_1 == E_2$). Binary operators operate in a similar manner to unary operators in that they rely on the premise triples to refer to the values generated by the sub-nonterminals $E_1$ and $E_2$. However, they also pose a unique challenge in that one needs to be careful in how these values are composed, as (partially) described in §2.

Take Plus as an example. A naive version of Plus might be written as following:

$$\left(\{P\} \ E_1 \ \{Q_1\} \cdot \ \{P\} \ E_2 \ \{Q_2\}\right) \text{ Plus-bad}$$

The problem arises in resolving the set corresponding to $Q_1 + Q_2$: the simplest way is to generate pairs by taking the cartesian product of the two sets, then add each pair to produce a set of values. However, this approach is imprecise, because it also generates pairs generated by different vector-states in the precondition.

Example 3.8 (Plus-bad). Consider an application of the Plus rule where $E_1 := x, E_2 := y$, and the input precondition is $P = \{(1, 3), (3, 1)\}$; i.e., there are two possible single-example vector-states: $(x, y) = (1, 3)$ and $(x, y) = (3, 1)$. (We omit $e_i$ in input states; its value is irrelevant.)

Because the only term in $E_1 + E_2$ is $x + y$, the postcondition should only contain states in which $e_t = 4$. However, because there are two possible input states in $P$, the predicate $Q_1$ contains two states—one in which $e_t = 3$ and another in which $e_t = 1$. Likewise, the predicate $Q_2$ contains two states, one in which $e_t$ is 1 and one in which it is 3. If one takes the cartesian product of the states in $Q_1$ and $Q_2$, then the predicate $Q$ ends up having 3 states—in which $e_t = 2, 4, \text{ or } 6$. The problem is that the two possible input states (1, 3) and (3, 1) are mixed by taking cartesian product.

To remedy this problem, in the Plus rule in unrealizability logic, each original state in the precondition is appended with a copy of itself, where we refer to the copied part as the ‘ghost (vector-state)’, and the original part as the original (vector)-state. This idea is captured in the preconditions of the premises, e.g., $P \land (v_1 = v)$; by taking a set of fresh variables $v_1$ and setting $v_1 = v$, one has essentially extended each state in $P$ with a copy of each variable.

Example 3.9 (Extended States). Consider the precondition $P = \{(1, 3), (3, 1)\}$, the same set of vector-states used in Example 3.8. Observe that $P \land (v_1 = v)$ results in the set of vector-states...
(x, y, x_1, y_1) = \{(1, 3, 1, 3), (3, 1, 3, 1)\}; note that states such as (1, 3, 1, 3) are not included in P \land (v_1 = v) because they violate the conjunct "(v_1 = v)."

Because the variables of the ghost state have been renamed, execution through a program in E will leave these variables unchanged according to the semantics of E. Thus, one can say that a state in, e.g., Q_1 is an extended state—where the ‘original’ part of the state has executed through E—and the ‘ghost’ part is left unchanged. By this device, one can check via the ghost parts whether two extended states from Q_1 and Q_2 should be added. Because the ghost-state portion of each extended state remains unchanged, one can deduce that two extended states must be added if and only if the ghost-state portions of the states are identical.

In the Plus rule, the postcondition of the conclusion illustrates the idea of matching vector-states on ghost-state portions. In particular, the constraint v_1 = v_2 filters out those pairs of extended states in which the ghost-state portions are different! The vocabulary shifts Q_1[v/v] and Q_2[v/v] move the ‘original’ program variables in Q_1 and Q_2 to v_1’ and v_2’ , respectively. The values of the original variables are unneeded, except for the value of e_i inside these states (available as e_i’ , respectively, after the vocabulary shifts.) The conjunction with P \land (v = v_1 = v_2) restores the values of the original program variables. The value of e_i is established by the conjunction with e_i = e_i’ + e_i’ . Finally, all of the additionally introduced variables are quantified out, leaving (vector-)states over the original variables, plus e_i.

Example 3.10 (Correcting Plus with Extended States). Consider again the grammar and preconditions from Example 3.8. As illustrated in Example 3.9, the extended precondition for E_1 is a set of vector-states of the form (x, y, x_1, y_1, e_i), namely, \{(1, 3, 1, 3), (3, 1, 3, 1)\}. Similarly, the extended precondition for E_2 is a set of vector-states of the form (x, y, x_2, y_2, e_i), namely, \{(1, 3, 1, 3), (3, 1, 3, 1)\}.

Because E_1 ::= x, the predicate Q_1—the result of executing E_1—has vector-states of the form (x, y, x_1, y_1, e_i) and equals \{(1, 3, 1, 3), (3, 1, 3, 1)\}. Similarly, because E_2 ::= y, the predicate Q_2—the result of executing E_2—has vector-states of the form (x, y, x_2, y_2, e_i) and equals \{(1, 3, 1, 3), (3, 1, 3, 1)\}.

The predicate Q_1[v/v'] creates a set of vector-states of the form (x_1', y_1', x_1, y_1, e_i'), i.e., \{(1, 3, 1, 3), (3, 1, 3, 1)\} (original program variables v are shifted to v_1'). Similarly, the predicate Q_2[v/v] creates a set of vector-states of the form (x_2', y_2', x_2, y_2, e_i'), i.e., \{(1, 3, 1, 3), (3, 1, 3, 1)\}. These are conjoined with P \land (v = v_1 = v_2), which leaves e_i unconstrained (as e_i was already unconstrained in P), and produces a set of vector-states of the form (x, y, x_1', y_1', x_1, y_1, e_i', x_2', y_2', x_2, y_2, e_i'), i.e., \{(1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3)\}, (3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1)\}. Original program variables are colored green, introduced ghost variables are colored cyan, and the results of executing E_1 and E_2 (e_i' and e_i', respectively) are colored red.

Once the set of states is conjoined with e_i = e_i' + e_i', and the auxiliary variables are quantified out, we obtain exactly the set of states that E_1 + E_2 can produce: (x, y, e_i) = \{(1, 3, 4), (3, 1, 4)\}.

At this point, it becomes possible to answer the question: why do we not simply produce sets of values as the postcondition for expression nonterminals, and instead introduce states with an auxiliary variable e_i? The reason is that simply producing sets of values renders it impossible to track the origin state as we have done in our Plus rule; thus, to keep track of this information, we instead opt to update the (vector-)variable e_i in our rules.

3.3.2 Rules for Statements. Unrealizability logic considers four kinds of statements: assignment, sequential composition, branches, and loops, as shown in Figure 6.
Assign and Seq can be explained using the same principles that we used to explain rules for expressions. In Assign, the result of the nonterminal $E$ is stored in the variable $e_1$ of $Q$: this value gets referenced and assigned to $x$. Seq is the same as in Hoare logic, where the sequentiability of the statements are captured by sharing the pre/postcondition $Q$.

If-Then-Else. Branches pose a similar challenge to operators such as Plus: one requires a mechanism for composing the states generated by two different nonterminals while ensuring that they come from the same ‘origin’ state. Similarly to what we did for Plus, the solution is to extend the input states with a ghost state: observe that the premise triples are of the same form $P_B \land (v_1 = v)$, where $P_B$ is identical to $P$ except that $b_1$ now stores the result of the branch condition.

The additional complication in the ITE rule is that in a given vector-state, certain examples must pass through the true branch, while others must pass through the false branch. In the ITE rule, we achieve this synchronization by first passing an input state through both the true and false branches (separately)—this step is captured by the two premises about $Q_1$ and $Q_2$, which simply push the ghost-state extended preconditions through the respective branches to obtain $Q_1$ and $Q_2$.

When merging the states from $Q_1$ and $Q_2$, we project out the examples that took the wrong branch—e.g., in $Q_1$, the postcondition of the true branch, the examples that should go through the false branch are projected out. This projecting out is captured by the conditional substitution $[v_1'[i]/v[i]]$ where $b_{t_1}[i] = false]^4$, which substitutes a variable $v[i]$ with a fresh variable $v_i[i]'$ only if $b_{t_1}[i] = false$—that is, if the branch condition evaluated to false for that example. (We reference $b_{t_1}$, the ghost-version of $b_1$, because the value of $b_1$ may change through the execution of $S_1$.)

The quantifier-free segment of the postcondition $Q_1[v_1'[i]/v[i]]$ where $b_{t_1}[i] = false] \land Q_2[v_2'[i]/v[i]]$ where $b_{t_2}[i] = true] \land (v_1 = v_2)$ is thus an extended state with five ‘copies’ of state, of which only one is retained: the examples that took the correct branches (named via $v$, and the ones that will be retained), the examples that took the incorrect branches (named via $v_1'$ and $v_2'$), and the two ghost states (named via $v_1$ and $v_2$). Quantifying out the auxiliary variables $v_1', v_2', v_1$ and $v_2$ leaves just the examples that took the correct branches.

Example 3.11 (If-then-Else with Extended States). Consider the set of states $P$ given by $(x_1, x_2) = \{(−1, 1), (2, −2)\}$; that is, $P$ denotes a set of two-example configurations, which could be

Conditional substitution may be applied simply by replacing all occurrences of $v[i]$ with if $b_{t_1}[i]$ then $v[i]$ else $v_i'[i]$.
specified by the formula \((x_1 = -1 \land x_2 = 1) \lor (x_1 = 2 \land x_2 = -2)\). Consider the If-Then-Else statement
if \(x > 0\) then \(x := x\) else \(x := 0 - x\) (we use a single program as it is sufficient to illustrate the ITE
rule); this program sets \(x\) to its absolute value. Observe that after executing \(x > 0\) (corresponding to
\(B\), \(P_B\) becomes the set of states \((x_1, x_2, b_{t_1}, b_{t_2}) = \{(−1, 1, \text{false}, \text{true}), (2, −2, \text{true}, \text{false})\}\). After
conjoining the ghost state and running through \(S_1\), we get the following set (the ghost state is
marked in cyan):
\[
(x_1, x_2, b_{t_1}, b_{t_2}, x_1, x_2, b_{t_1}, b_{t_2}) = \{(−1, 1, \text{false}, \text{true}, −1, 1, \text{false}, \text{true}), (2, −2, \text{true}, \text{false}, 2, −2, \text{true}, \text{false})\}
\]
Applying the conditional substitution to this set yields the following set of states, where non-
substituted variables are green, variables substituted with \(v'_1\) are red, and the ghost state is cyan:
\[
\{(−1, 1, \text{false}, \text{true}, −1, 1, \text{false}, \text{true}), (2, −2, \text{true}, \text{false}, 2, −2, \text{true}, \text{false})\}
\]
Similarly, executing \(S_2\) and applying substitution yields the following set:
\[
\{(−1, 1, \text{false}, \text{true}, −1, 1, \text{false}, \text{true}), (2, −2, \text{true}, \text{false}, 2, −2, \text{true}, \text{false})\}
\]
Again, note that the substitution happens for variables highlighted in red, while the green variables
are the original program variables. Taking the conjunction and quantifying out all unnecessary
variables leaves only the variables highlighted in green, which yields:
\[
(x_1, x_2, b_{t_1}, b_{t_2}) = \{(1, 1, \text{false}, true), (2, 2, \text{true}, false)\},
\]
Which is exactly the set of states that are computed by the given If-Then-Else statement.

Loops. The basic intuition behind the While rule is identical to that in Hoare logic—it requires the
existence of an invariant \(I\). The difference with Hoare logic is that, in our work, \(I\) must work as an
invariant for all possible completions of the loop body \(S\).

In unrealizability logic, a vector-state must repeat the loop body until all examples cause the loop
condition to evaluate to false, which is why the postcondition of the While rule has the condition
\(b_t = f\): all the loop conditions of all examples (stored in \(b_t\) of \(I_B\)) evaluate to false.

Because the invariant \(I\) spans multiple examples, the way the invariant is checked is also different
from in Hoare logic. First, we take a similar approach as in ITE, and push examples through the loop
body \(S\), regardless of the loop guard (in the premise \(\{I_B \land b_{loop} = b_t\} \models S \{I'_B\}\)). Then, the implication
checks whether \(I'_B \models I_B\) only on the examples where the loop guard is true: this effect is again
achieved through a conditional substitution, which substitutes variables for which \(b_{loop}[i] = \text{false}\), and
quantifies out the substituted variables again (as well as the auxiliary variables \(e_t\) and \(b_t\), which
are subject to change).\(^5\) For the examples that are substituted out, \(I_B\) is an invariant because these
examples are left unchanged—thus, one only needs to check the invariant condition for examples
that pass the loop guard and execute the body, which is captured via the implication premise.

The reader may find it surprising that a single invariant capturing the behavior of all possible loop
bodies suffices for relative completeness. A single invariant does suffice for relative completeness
because one can actually write an invariant that talks about the choice of loop body itself. However,
to pull off this trick, one needs a highly complex encoding whose details are beyond the scope
of this paper (see §4.1 for details). In practice, the use of this complex encoding will often result
in an invariant too complex for a proof to be completed. Thus, when writing actual proofs in
unrealizability logic, it is often beneficial to split the loop bodies into smaller sets, and reason about
them separately (as we have done in Example 2.6 of §2) through the use of the structural rules.

\(^5\) The additional assignment \(b_{loop} = b_t\) before executing the loop body, as well as referencing \(b_{loop}\) in the postcondition, is
again due to the fact that \(b_t\) may change during the execution of \(S\).
Weaken, Conj. These rules operate like their counterpart in Hoare logic. Weaken can shrink the precondition or enlarge the postcondition following the principle that the postcondition overapproximates the set of all states that the precondition can generate. Weaken can also shrink the set of considered programs. Conj takes the conjunction of the two postconditions.

GrmDisj. GrmDisj allows us to split sets of programs: if two sets of programs, \( N_1 \) and \( N_2 \), satisfy the same pre- and postcondition, then their union also satisfies those same pre- and postcondition. This rule is not required for the completeness of the logic. However, it helps greatly in simplifying actual unrealizability proofs: a clever division of the search space often results in simpler predicates.

Inv, SubOne, SubTwo. Inv, Sub1, and Sub2 are rules that are necessary for our completeness proof. Inv states that if a precondition does not share any free variables with any program in the set \( N \) (i.e., \( \text{vars}(P) \cap \text{vars}(N) = \emptyset \)), then it is an invariant—clearly this holds, because any program \( N \) will be unable to access or modify the variables used in \( P \). Sub1 and Sub2 perform \( \alpha \)-renaming of variables inside the pre- and postconditions. Sub1 states that free variables inside preconditions or postconditions that do not appear in the set of programs \( N \) may be renamed at will to a set of fresh variables. Sub2 states that a set of variables appearing in the precondition \( P \), and not appearing in the set of programs \( N \) or the postcondition \( Q \), may be renamed as well.

HP, ApplyHP. HP and ApplyHP allow us to perform structural induction in the proof tree. HP introduces a new hypothesis into the context \( \Gamma \), while ApplyHP allows us to apply an induction hypothesis. (These rules were explained in §2.1).

Definition 3.12 (Derivability). Given a precondition over vector-states \( P \), a postcondition over vector-states \( Q \), a set of programs \( S \), and a set of hypotheses \( \Gamma \), we say that a triple \( \{P\} S \{Q\} \) is derivable assuming \( \Gamma \), denoted by \( \Gamma \vdash \{P\} S \{Q\} \), if there exists a proof tree deriving \( \Gamma \vdash \{P\} S \{Q\} \) using the rules of unrealizability logic in Figures 5, 6, and 7.

We say that a triple \( \{P\} S \{Q\} \) is derivable, if it can be derived with an empty set of hypotheses.
4 SOUNDNESS, COMPLETENESS, AND OTHER THEORETICAL RESULTS

Unrealizability logic is a sound logic in the sense that any derivable triple \( |P| \# |Q| \) is also valid.

**Theorem 4.1 (Soundness).** Given a nonterminal \( N \) in a grammar \( G \), the following is true:

\[
\vdash |P| \# |Q| \implies |P| \# |Q|
\]

Soundness can be proved via structural induction, which shows that the conclusion triple of each rule is sound given that the premises are sound (see Appendix A of the supplementary material for the full proof). While reasoning about some cases is complex due to the vectorized semantics, the overall structure of the proof is a simple structural-induction argument.

Surprisingly, unrealizability logic is also relatively complete, in the sense that all valid triples \( |P| \# |Q| \) are derivable (modulo completeness of the assertion language).

**Theorem 4.2 (Completeness).** Given a nonterminal \( N \) in a grammar \( G \), the following is true:

\[
|P| \# |Q| \implies \vdash |P| \# |Q|
\]

Completeness follows from two lemmas that we state later (Lemmata 4.4 and 4.5), which state that (i) a **strongest triple** that precisely describes the behavior of a nonterminal is derivable, and (ii) that any sound triple about a nonterminal can be derived from the strongest triple.

In the rest of this section, we give a sketch of the proof of completeness, and discuss some other theoretical results. We will present proof sketches for the theorems listed in this section, for the full proofs, we again refer the reader to Appendix A of the supplementary material.

4.1 A Sketch of the Proof of Completeness

Completeness of unrealizability logic is a two-step process: first we wish to prove that the non-structural rules (expression and statement rules) of unrealizability logic are complete, in the sense that, given a set of programs generated by a production \( \{P\} \# \{Q\} \), if all sound premise triples about \( N_1, \ldots, N_k \) are derivable, then all sound triples about \( op(N_1, \ldots, N_k) \) are also derivable.

**Lemma 4.3 (Completeness of Expression and Statement Rules).** Let \( G \) be a regular tree grammar and \( N \) be a set of programs generated by the RHS of a production. Then, the expression and statement rules of unrealizability logic preserve completeness, in the sense that, if all (sound) required premise triples are derivable, then all (sound) triples about \( N \) are derivable in unrealizability logic.

Lemma 4.3 can be proved by showing that the conclusion of the postcondition of each rule precisely captures the semantics of the corresponding operator.

One thing to note about the proof of Lemma 4.3 is that it relies on the existence of a predicate that expresses exactly the weakest precondition of a set of while loops for an arbitrary postcondition, often called the expressibility of the weakest precondition. This is related to the complex invariant of while loops mentioned in §3.3; the expressibility of the weakest precondition implies the expressibility of the invariant. In this paper, we take what is known as the extensional approach and assume that the weakest precondition can be expressed within the assertion language of choice.

While Lemma 4.3 would be sufficient as a proof of completeness in normal Hoare logic, it is insufficient for unrealizability logic because we are working over an RTG; without the use of the HP rule, the proof tree will become infinite. The next step in showing completeness remedies this fact by proving that through use of the HP rule, we can prove the strongest triple for a nonterminal within a finite number of steps.

\[\text{The invariant can, in fact, be expressed in Peano arithmetic, but the proof of this fact is beyond the scope of this paper.}\]
Lemma 4.4 (Derivability of the Strongest Triple). Let \( N \) be a nonterminal from a RTG \( G \) and \( z \) be a set of auxiliary symbolic variables. Let \( Q_0 \equiv [N](x = z); \) that is, \( Q_0 \) is a formula that precisely captures the behavior of the set of programs \( L(N) \) on the symbolic vector-state \( x_1 = z_1 \land \cdots \land x_n = z_n \).\(^7\)

We refer to \( \{x = z\} N \{Q_0\} \) as the strongest triple for \( N \). Then \( \vdash \{x = z\} N \{Q_0\} \) is derivable.

The proof of Lemma 4.4 performs induction over the number of hypotheses in the context: the proof relies on the fact that one only needs to insert the strongest triple for each nonterminal into the context (because the strongest triple can derive any other triple), thus the HP rule need only be applied at most \(|G|\) times (the number of nonterminals inside \( G \)). When all \(|G|\) hypotheses are established, one relies on Lemma 4.3 to show that the strongest hypothesis can actually be derived.

The proof of Lemma 4.4, as well as the final step in arguing completeness, requires a lemma that shows one can derive any triple from the strongest triple.

Lemma 4.5 (Derivability of General Triples). Let \( G \) be a grammar and \( N \) be any nonterminal in \( G \). Given the strongest triple \( H_N \) for the nonterminal \( N \) (as defined in Lemma 4.4), if \( \Gamma \vdash H_N \), then \( \Gamma \vdash \{P\} N \{Q\} \implies \Gamma \vdash \{P\} N \{Q\} \).

Lemma 4.5 can be proved using the substitution rules \( \text{Sub1} \) and \( \text{Sub2} \). Relative completeness (Theorem 4.2) then follows from Lemma 4.4 and Lemma 4.5.

4.2 Undecidability of Unrealizability and Decidable Fragments

Although we have proved relative completeness, proving unrealizability is an undecidable problem, even when limited to synthesis problems without loops.

Theorem 4.6 (Undecidability of Unrealizability). Let \( \text{sy}_u \) be a synthesis problem with a grammar \( G_u \) that does not contain productions of the form \( S ::= \) while \( B \) do \( S_1 \). Checking whether \( \text{sy}_u \) is unrealizable is an undecidable problem.

The proof of Theorem 4.6 is a reduction from the halting problem for two-counter machines. Theorem 4.6 shows that proving unrealizability of synthesis problems is undecidable, even when while loops are outside of the question. On the other hand, when one is limited to synthesis over finite domains, proving unrealizability becomes decidable—even when the synthesis problem may contain an unbound number of loops.

Theorem 4.7 (Decidability of Unrealizability over Finite Domains). Determining whether a synthesis problem \( \text{sy}_{\text{fin}} \) is realizable, where the grammar \( G_{\text{fin}} \) is valid with respect to \( G_{\text{imp}0} \), is decidable if the semantics of programs in \( G_{\text{fin}} \) is defined over a finite domain.

The proof of Theorem 4.7 relies on the fact that if the domain is finite, one can perform grammar-flow analysis [17] to obtain the greatest-fixed point of values that a nonterminal may generate; this computation is guaranteed to terminate because the domain is finite.

Furthermore, if \( \text{sy}_{\text{fin}} \) is unrealizable, then there exists a proof of this fact in unrealizability logic.

5 THE POWER OF UNREALIZABILITY LOGIC

In this section, we give some example proofs that highlight the capabilities of unrealizability logic.

5.1 Dealing with an Infinite Number of Examples

As stated in §2 and §3, one of the major features of unrealizability logic is that it is capable of dealing with synthesis problems which require an infinite number of examples to prove unrealizable. We illustrate one such example in this section.

\(^7\)We assume that state is defined over a single variable \( x \); it is trivial to extend this to multiple-variable states.
Example 5.1 (Proof with Infinitely Many Examples). Consider a synthesis problem $\text{sy}_{\text{id ITE}}$, with the grammar $G_{\text{id ITE}}$ given below:

\begin{align*}
\text{Start} & \rightarrow \text{if } B \text{ then } A \text{ else } \text{Start} | A \\
B & \rightarrow y == N \\
N & \rightarrow 0 | N + 1 \\
A & \rightarrow x := N
\end{align*}

$\text{sy}_{\text{id ITE}}$ aims to synthesize a function $f$ which takes as input a state $(x, y)$, and return a state where $x$ is equivalent to $y$.

$\text{sy}_{\text{id ITE}}$ is unrealizable, and one needs an infinite number of examples to prove this fact. This is because a specification over $n$ examples for $\text{sy}_{\text{id ITE}}$ will be realizable by a term that contains $n$ If-then-Elses. However, a term of finite size in $G_{\text{id ITE}}$ can only assign to $x$ a finite number of constants; thus it is impossible to have a function in $G_{\text{id ITE}}$ that sets $x$ to $y$ in the general case. $\text{sy}_{\text{id ITE}}$ is, in fact, an imperative variant of an example often used to show that there are synthesis problems that cannot be proven unrealizable using only a finite number of examples [10]; previous approaches [10, 11, 14] thus cannot prove $\text{sy}_{\text{id ITE}}$ unrealizable. We show that a proof tree for $\text{sy}_{\text{id ITE}}$ can be constructed in unrealizability logic.

Consider a set of inputs $(x, y)$ given by the predicate $\forall i \in \mathbb{N}, x_i = -1 \land y_i = i$. That is, the input is an infinite set of examples where $y$ spans over the positive integers, and $x$ is assigned the fixed value $-1$ (this implies $x_i \neq y_i$ for every $i \in \mathbb{N}$). The output specification for this input is given as $\forall i. x_i = i \land y_i = i$; the infinite vector-state where $x_i = y_i = i$ for the $i$-th example. This infinite set of examples does not encompass the entire input state; however, it is sufficient to prove unrealizability.

To prove unrealizability, first negate the postcondition to obtain the triple that we wish to prove:

$$\{ \forall i. x_i = -1 \land y_i = i \} \text{ Start } \{ \exists i. x_i \neq i \land y_i \neq i \}$$

Instead of proving this triple directly, we will prove the following triple (from which we can obtain the target triple via Weaken):

$$\{ \forall i. y_i = i \land \text{ only a finite number of } i \text{ such that } x_i = y_i \} \text{ Start } \{ \forall i. y_i = i \land \text{ only a finite number of } i \text{ such that } x_i = y_i \}$$

Let $I$ denote the condition $\forall i. y_i = i$ only a finite number of $i$ such that $x_i = y_i$. To see the implication, observe that: (i) $\forall i. x_i = -1 \land y_i = i \implies I$ as there are $0$ (a finite number) $i$ for which $x_i = y_i$; (ii) $I \implies \exists i. x_i \neq i \land y_i \neq i$, because if $x_i = y_i$ for only a finite number of $i$, then there must exist some $i$ for which $x_i \neq i$.

We will prove that $\{ I \} \text{ Start } \{ I \}$ holds by introducing this triple as a hypothesis for $\text{Start}$ via the HP rule. Let $\Gamma_I$ denote the context containing only the triple $\{ I \} \text{ Start } \{ I \}$.

\[
\begin{align*}
\Gamma_I & \vdash \{ I \} A \{ I \} \\
\Gamma_I & \vdash \{ I \} \text{ if } B \text{ then } A \text{ else } \text{Start } \{ I \} \\
& \vdash \{ I \} \text{ Start } \{ I \} \\
& \vdash \{ I \} \text{ Start } \{ I \} \\
& \vdash \{ I \} \text{ Start } \{ I \} \\
& \vdash \{ I \} \text{ Start } \{ I \}
\end{align*}
\]

Consider first the base case $\{ I \} A \{ I \}$, where $A$ is the simple assignment $x := N$. The hypothesis in this case can be proved simply via Assign and Weaken:

\[
\begin{align*}
\Gamma_I & \vdash \{ I \} N \{ \exists e_i \cdot I \{ e_i = e_i \} \land \exists k. k \geq 0 \land e_i = k \} \\
\Gamma_I & \vdash \{ I \} N \{ I \land \exists k. k \geq 0 \land e_i = k \} \\
\Gamma_I & \vdash \{ I \} A \{ \exists e_i \cdot I \{ e_i = e_i \} \land \exists k. k \geq 0 \land \forall i. x_i = k \} \\
\Gamma_I & \vdash \{ I \} A \{ I \}
\end{align*}
\]
The ellipses over the top-level HP rule indicates that we can prove that $N$ results in a value above 0 via the HP rule, through the induction hypothesis $\{I\} N \{e'_i, I[e'_i/e_i] \land \exists k. k \geq 0 \land e_i = k\}$ (the exact reasoning is omitted). The final application of Weaken works as, if all $x_i = k$ for some $k \geq 0$, then there is at most one (a finite number) $i$ for which $x_i = y_i$.

The inductive case requires an application of the ITE rule. We first write:

$$\Gamma_T + \{I\} B \{\{I\}\} \quad \Gamma_T + \{I \land v_1 = v\} A \{\{I\}\} \quad \Gamma_T + \{I \land v_2 = v\} \text{ Start } \{\{I\}\}$$

ITE

$$\Gamma_T + \{I\} \text{ if } B \text{ then } A \text{ else } \text{ Start } \{\{I\}\}$$

Weaken

Observe that the first premise $\{I\} B \{\{I\}\}$ seems to do nothing. This is the result of weakening the postcondition generated by $B$, and effectively ‘forgetting’ the value of the branch condition as done in the following proof tree, where the postcondition of the premise represents the exact postcondition one would have obtained through a precise reasoning of Eq:

$$\Gamma_T + \{I\} B \{\exists b_1, v_1, v_2, v_1', v_2', \exists e'_i, I[v_1'/v] \land e'_i = y \land (v = v_1 = v_2) \land I[v_2'/v] \land \exists k. k = x \land \exists b_1. (e'_i = e_i) \}$$

Eq

Weaken

Finally, the third premise can be derived with a simple combination of ApplyHP and Weaken, where ApplyHP applies the induction hypothesis that $\{I\} \text{ Start } \{\{I\}\}$.

$$\Gamma_T + \{I\} A \{\{I\}\} \quad \text{ApplyHP}$$

Weaken

Returning to the application of ITE, observe that $I$ lacks any occurrence of $v_1$ and $v_2$. This is again because our triples for $A$ and Start in the premises were not exact; $I$ is an overapproximation of the set of states that may occur when, e.g., executing $\text{Start}$ over the input precondition $I \land v_2 = v$.

Although the derived postcondition is thus also not exact, it is still a sound overapproximation that is precise enough for the proof. To see this, observe that mixing examples from two states where $\forall i. y_i = i \land$ only a finite no. of $i$ such that $x_i = y_i$ holds (the postcondition of the conclusion of ITE) still results in a state where $\forall i. y_i = i \land$ only a finite no. of $i$ such that $x_i = y_i$ holds. Thus the final application of Weaken that derives $\{I\}$ if $B$ then $A$ else $\text{Start } \{I\}$ is a valid application.

By proving that $\Gamma + \{I\} A \{\{I\}\}$ and $\Gamma + \{I\}$ if $B$ then $A$ else $\text{Start } \{I\}$, we have proven the induction hypothesis; thus $\{I\} \text{ Start } \{\{I\}\}$ holds, which can further be weakened down into the target triple $\{v_i, x_i = -1 \land y_i = i\}$ Start $\exists i. x_i = i \lor y_i = i$. Hence $s_{\text{ITE, ITE}}$ is unrealizable, and we have proved this fact quite simply via some imprecise reasoning.

In Example 5.1, we used predicates such as $\forall i. x_i = i \land y_i = i$, or ‘only a finite no. of $i$ such that $x_i = y_i$’; whether or not such predicates are supported is dictated by the choice of the assertion language. As mentioned in §3, the choice of assertion language is parametric in unrealizability logic, as long as it contains the operators used in the rules.
5.2 Loops and Expressing Proof Strategies from Other Frameworks

In this section, we give an example of how loops are dealt with in unrealizability logic, and also show that the reasoning behind other frameworks for proving unrealizability (e.g., Nay [11] or MESSY [14]) can be captured as a proof strategy for completing a unrealizability logic proof tree.

Example 5.2 (Proof with Loops). Consider a synthesis problem \(sy_{\text{sum}}\) where the goal is to synthesize a function \(f\) that takes as input a state \((x, y)\), and assigns to \(y\) the sum of all integers between 1 and \(x\). Let us assume that \(sy_{\text{sum}}\) is given the following grammar \(G_{\text{sum}}\):

\[
\begin{align*}
\text{Start} & \rightarrow \text{while } B \text{ do } S \\
B & \rightarrow E < E \\
S & \rightarrow x := E \mid y := E \mid S; S \\
E & \rightarrow x \mid y \mid E + E \mid E - E
\end{align*}
\]

Then, the problem \(sy_{\text{sum}}\) is unrealizable because if \(x\) and \(y\) are both even, then \(E\) can only produce even values. This fact conflicts with cases where, e.g., \(x = 2\), in which case \(y\) must be assigned 3. \(sy_{\text{sum}}\) is introduced as an unrealizable problem in Kim et al. [14], where the solver MESSY exploits this fact to prove that \(sy_{\text{sum}}\) is indeed unrealizable when given the single input example \((x, y) = (2, 0)\).

We show that this argument can be mimicked directly as a proof tree for unrealizability logic.

Let \(I\) denote the condition \(x \equiv 0 \land y \equiv 0\), i.e., that \(x\) and \(y\) are both even (because we use a single example, we temporarily drop the vector notation). We wish to use \(I\) as an invariant for the loop while \(B\) do \(S\). Begin with an application of While for Start, where, similar to Example 5.1, the loop condition is irrelevant to the proof and thus can be skipped:

\[
\begin{align*}
\Gamma & \vdash \{ I \} \ B \ \{ I \} \quad \Gamma & \vdash \{ I \} \ S \ \{ I \} \\
\Gamma & \vdash \{ I \} \text{ while } B \text{ do } S \ \{ I \} \text{ b}_1 = \text{false} \quad \text{While}
\end{align*}
\]

The first premise can be proved via Weaken, as we did in Example 5.1. The implication condition of the While rule has been omitted, as in this case \(I_B' = I_B = I\) and thus the implication is trivial.

We wish to prove that \(\vdash \{ I \} \ S \ \{ I \}\); let us introduce \(\{ I \} \ S \ \{ I \}\) as a hypothesis. We denote the context containing only this triple as \(\Gamma_S\). We then have the proof obligation:

\[
\begin{align*}
\Gamma_S & \vdash \{ I \} \ x := E \ \{ I \} \\
\Gamma_S & \vdash \{ I \} \ y := E \ \{ I \} \\
\Gamma_S & \vdash \{ I \} \ S \ \{ I \}
\end{align*}
\]

The first two premises can be proved by introducing a hypothesis \(\{ x \equiv 0 \land y \equiv 0\} \ E \ \{ e_t \equiv 0\}\). The third premise can be proved via two applications of ApplyHP. This completes that \(\{ I \} \ S \ \{ I \}\), and therefore that \(\{ I \}\) while \(B\) do \(S\) \(\{ I \land b_1 = \text{false}\}\).

Finally, we apply Weaken to \(\{ I \}\) while \(B\) do \(S\) \(\{ I \land b_1 = \text{false}\}\) to obtain the triple \(\{ x = 2 \land y = 0\} \ \text{Start} \ \{ y \neq 3\}\). We have thus proved that \(sy_{\text{sum}}\) is unrealizable, mainly by using an invariant that is valid across the entire set of possible loop bodies.

In §2, specifically Example 2.3, we highlighted the importance of finding good hypotheses and invariants for completing a proof in unrealizability logic. In Example 5.2 above, knowing the invariant \(x \equiv 0 \land y \equiv 0\) resulted in a very simple proof tree. The algorithms implemented by external solvers (such as Spacer [15] for MESSY, or the semilinear-set approach from Nay [11]) may be thought of as proof strategies for finding these hypotheses or invariants: they remain parametric of the logic itself, while supplying users with critical information to complete the proof trees.

Although not the focus of this paper, we hope that this view will allow future work in automating unrealizability logic to draw from a significant body of work in grammar-flow analysis [17] and other program/constraint-solving techniques.
5.3 Working with Symbolic Examples and Auxiliary Variables

In §2.2, we saw that auxiliary variables are insufficient to model unrealizability. However, auxiliary variables can still be used to set the input examples of an unrealizability triple to be symbolic. A triple derived in unrealizability logic using symbolic examples indicates that the said triple must hold for any instantiation of the symbolic examples. In unrealizability logic, this can be used to avoid having to search for hard-to-find examples, instead completing a symbolic proof tree and checking at the end whether there are examples that can be used to show unrealizability.

Example 5.3 (Proof with Symbolic Variables). Recall the synthesis problem $sy_{id\_ite}$ from Example 5.1, where the goal is to synthesize a function that assigns to $x$ the (initial) value of $y$. We will consider a variant of $sy_{id\_ite}$, named $sy_{id\_const}$, where the goal is the same but the supplied grammar $G_{id\_const}$ is different:

$$
\begin{align*}
\text{Start} & \rightarrow \text{if } B \text{ then } A \text{ else } \text{Start} \mid A \\
B & \rightarrow y == E \\
E & \rightarrow 0 \mid E + 1 \\
N & \rightarrow 1 \mid 2 \mid \cdots \mid 999 \\
A & \rightarrow x := N
\end{align*}
$$

In $G_{id\_const}$, the nonterminal $N$ may generate only a fixed set of integers from 1 to 999 (as opposed to $G_{inf}$, which could generate any positive integer). $sy_{id\_const}$ is unrealizable, and this time only requires one example to prove so: for example, $(x, y) = (-1, 1000)$. However, this specific example may be difficult to find, because it uses large constants. We show that one can avoid having to explicitly find this example by completing a proof tree in unrealizability logic using a single symbolic example—which may then be instantiated (perhaps using a constraint solver)—to find a concrete example for which $sy_{id\_const}$ is unrealizable.

Our goal this time is to prove the following triple (we again drop the vector-subscripts here as we only have one example):

$$\begin{align*}
\{ x = -1 \land y = y_{aux} \} & \text{ Start } \{ \exists k. k < 1000 \land x = k \land y = y_{aux} \}
\end{align*}$$

This triple states that: starting from a single example $(x, y) = (-1, y_{aux})$, we will only be able to reach states in which $x < 1000$. Note that the given single example is made symbolic through the use of the auxiliary variable $y_{aux}$. This time, we will use the following hypothesis for Start:

$$\begin{align*}
\{ \exists k. k < 1000 \land x = k \land y = y_{aux} \} & \text{ Start } \{ \exists k. k < 1000 \land x = k \land y = y_{aux} \}
\end{align*}$$

Denote the triple above as $I$. In a similar process to the one used in Example 5.1, one can see that the hypothesis holds for the base case (assignment) (we omit the application of the HP rule):

$$
\begin{align*}
\Gamma_T \vdash \{ I \} & N \{ \exists e'.I'[e'_e/e_t] \land \exists k.0 < k < 1000 \land e_t = k \} & \text{ HP } \\
\Gamma_T \vdash \{ I \} & N \{ I \land \exists k. k < 1000 \land e_t = k \} & \text{ Weaken }
\end{align*}
$$

And also for the inductive case, If-Then-Else (where we omit the reasoning for the premises):

$$
\begin{align*}
\Gamma_T \vdash \{ I \} \text{ if } B \text{ then } A \text{ else } \text{Start } & \{ \exists v_1, v_2, v'_1, v'_2. I[v'_1[i]/v[i] \land b_1[i] = \text{false}] \land I[v'_2[i]/v[i] \land b_2[i] = \text{true}] \land (v_1 = v_2) \} & \text{ ITE } \\
\Gamma_T \vdash \{ I \} & \text{ if } B \text{ then } A \text{ else } \text{Start } & \{ I \} & \text{ Weaken }
\end{align*}
$$

Thus $\{ \exists k. k < 1000 \land x = k \land y = y_{aux} \} \text{ Start } \{ \exists k. k < 1000 \land x = k \land y = y_{aux} \}$ is a valid triple.
At this point, observe that $\exists k. k < 1000 \land x = k \land y = y_{aux}$ does not immediately imply the negation of the specification, i.e., $x \neq y_{aux} \lor y \neq y_{aux}$. However, when setting $y_{aux} = 1000$, it does become clear that $\exists k. k < 1000 \land x = k \land y = y_{aux} \implies x \neq 1000 \lor y \neq 1000$.

To understand this more formally, recall that as shown in Example 2.4, the quantification for auxiliary variables happens outside the triple:

$$\forall y_{aux}. (\exists k. k < 1000 \land x = k \land y = y_{aux})$$

This, in turn, means that the triple holds for all configurations of $y_{aux}$, each of which constitutes a different example. For synthesis, the program must work for all examples: thus it is sufficient that there exists an example for which the synthesis problem is unrealizable, i.e., the derived postcondition implies the negation of the specification. Thus to check unrealizability in this scenario where we have used an auxiliary variable, we can check whether the following formula is valid:

$$\exists y_{aux}. (\exists k. k < 1000 \land x = k \land y = y_{aux} \implies x \neq 1000 \lor y \neq 1000)$$

And this formula is certainly valid, as witnessed by $y_{aux} = 1000$. Thus $sy_{id\_const}$ is unrealizable.

In general, when using a specification with symbolic examples denoted using the variables $v_{aux}$, one can check whether $\exists v_{aux}. Q \implies \neg O$ is a valid formula, where $Q$ is the derived postcondition and $O$ denotes the desired postcondition of the synthesis problem. As shown in Example 5.3, the existential quantifier over $v_{aux}$ asks whether there exists a concrete instantiation of the symbolic examples such that $Q \implies \neg O$. Although this approach will not be able to prove unrealizability if the supplied number of symbolic examples is less than the number of examples required to show unrealizability (as in Example 2.4), it will succeed in proving unrealizability if the supplied number of examples is sufficient. This can be very useful if the examples required to prove unrealizability are difficult to find, as in Example 5.3.

Note that it is still sound if one decides to drop the existential quantifier and simply ask whether $Q \implies \neg O$; adding the existential simply makes the final query more precise.

6 RELATED WORK

Unrealizability. There has been limited work that focuses on proving the unrealizability of synthesis problems. NAY [11] and NOPE [10] can prove unrealizability for syntax-guided synthesis (SyGuS) problems where the input grammar only contains expressions. Both NAY and NOPE reduce an unrealizability problem to a program-verification problem, and present techniques for solving the reduced problem. Kamp and Philippsen [13] use some of the ideas presented in NOPE to design specialized unrealizability-checking algorithms for problems involving bit-vector arithmetic. When a grammar is not given as part of the input, CVC4 [22] is also capable of detecting unrealizability. These works only focus on expression-synthesis problems. MESSY [14] proposes a general algorithm for proving whether a given SemGuS problem is unrealizable. SemGuS is a general framework for specifying synthesis problems, which also allows one to define synthesis problems involving imperative constructs. MESSY is currently the only tool that can prove unrealizability for problems involving imperative programs. Farzan et al. [5] have a technique for proving unrealizability, which they use as part of a synthesis technique; however, their technique is limited to a very specific class of functional programs and specifications.

While previous approaches all provide ways to solve variants of unrealizability problems, these approaches are embedded within a specific system that employs a fixed solver or algorithm. With the exception of NAY and its use of grammar-flow analysis, these tools do not produce a proof artifact that can be separately verified. For example, in MESSY, one is at the mercy of an external constraint solver, which makes it difficult for researchers to develop new solvers tailored towards...
unrealizability, or even understand why certain problems can be proved unrealizable while others cannot. In contrast, unrealizability logic provides a general, logical system for (both human and machine-based) reasoning about unrealizability. While NAY can produce proof artifacts, it is limited to SyGuS problems over expressions; similar to what we showed in Example 5.2, the GFA algorithm of NAY may be understood as a proof strategy to discover hypotheses over nonterminals (where in this case, the assertion language is over semilinear sets).

Hyperproperties. The way we synchronize between multiple examples in unrealizability logic, using vector-states, is similar to the concept of hyperproperties, which are, in essence, sets of properties [3]. Hyperproperties are used to model, for example, $k$-safety properties, which are properties that should hold over $k$ separate runs of a program [23] (for example, transitivity is a $3$-safety property).

There is a subtle but fundamental difference between properties in unrealizability logic and standard hyperproperties: properties in unrealizability logic are 'properties over vector-states'; that is, 'properties over (sets of states)', whereas standard hyperproperties are 'sets of (properties over states)'. The difference between the two is highlighted when considering nondeterminism: when verifying $k$-safety properties for a nondeterministic program, one will want to let different states execute on different paths. In contrast, unrealizability logic introduces vector-states to synchronize the paths—corresponding to one specific program within the set $S$—that each constituent state in a vector-state follows. For example, given a grammar $E 	o x := x + 1 \mid x := x + 2$, the unrealizability triple \( \{x_1 = 0 \land x_2 = 10\} E \{(x_1 = 1 \land x_2 = 11) \lor (x_1 = 2 \land x_2 = 12)\}\) is derivable. However, a standard hyperproperty approach would likely wish to treat the above triple as invalid (taking a nondeterministic-program interpretation of the different productions of $E$).

Hoare Logic for Recursive Procedures. The rules of unrealizability logic have much in common with the rules of Hoare logic extended towards recursive procedures. However, as discussed in §2.3, one requires many features to fully support the range of features in a synthesis problem; for example, nondeterminism, mutual recursion, both local and global variables, and infinite data structures. Combinations of some of these features have been studied previously, such as local variables and mutual recursion [20], or nondeterminism and recursion [18]. There is a vast amount of work on variants of Hoare logic; Apt and Olderog [2] provides a survey of how the original Hoare logic [9] has evolved throughout the years.

Despite this body of work, we are unaware of a study of a system that contains all of the features listed above, and proves soundness, completeness, and decidability results as we have. Also as discussed in §2.3, even though one does have an extended Hoare logic, such a logic would hide the fact that we are dealing with synthesis problems and trying to prove unrealizability—whereas unrealizability logic takes advantage of this fact through rules like GrmDisj.

7 CONCLUSION

We presented unrealizability logic, the first proof system for overapproximating the execution of an infinite set of programs. Unrealizability logic is both sound and relatively complete; it is also the first approach that allows one to prove unrealizability for synthesis problems that require infinitely many inputs to be proved unrealizable. We believe unrealizability logic will prove to be essential in further developments having to do with unrealizability.

A natural open question that follows from this paper is the development of a realizability logic: “Can a similar logic be constructed for program synthesis, i.e., for proving realizability?” Because program synthesis requires a guarantee that a certain state is reachable, one must devise suitable principles of underapproximation (like the ones discussed in reverse-Hoare (aka incorrectness) logic [4, 19]) instead of overapproximation as used in this paper. We believe the results presented in this paper will also be useful in designing a realizability logic.
REFERENCES


