Learning Loop Invariants for Program Verification

Xujie Si
University of Pennsylvania
xsi@cis.upenn.edu

Hanjun Dai
Georgia Tech
hanjundai@gatech.edu

Mukund Raghothaman
University of Pennsylvania
rmukund@cis.upenn.edu

Mayur Naik
University of Pennsylvania
mhnai@cis.upenn.edu

Le Song
Georgia Tech and Ant Financial
lsong@cc.gatech.edu

Abstract

A fundamental problem in program verification concerns inferring loop invariants. The problem is undecidable and even practical instances are challenging. Inspired by how human experts construct loop invariants, we propose a reasoning framework that constructs the solution by multi-step decision making and querying an external program graph memory block. By training with reinforcement learning, we are able to capture rich program features and avoid the need for ground truth solutions as supervision. Compared to previous learning tasks in domains with graph-structured data, we address unique challenges, such as a binary objective function and an extremely sparse reward that is given by an automated theorem prover only after the complete loop invariant is proposed. We evaluate our approach on a suite of 133 benchmark problems and compare it to three state-of-the-art systems. It solves 106 problems compared to 73 by a stochastic search-based system, 77 by a heuristic search-based system, and 100 by a decision tree learning-based system. Moreover, the strategy learned can be generalized to new programs: compared to solving new instances from scratch, the pre-trained agent is more sample efficient in finding solutions.

1 Introduction

The growing ubiquity and complexity of software has led to a dramatic increase in software bugs and security vulnerabilities that pose enormous costs and risks. Program verification technology enables programmers to prove the absence of such problems at compile-time before deploying their program. One of the main activities underlying this technology involves inferring a loop invariant—a logical formula that constitutes an abstract specification of a loop—for each loop in the program. Obtaining loop invariants enables a broad and deep range of correctness and security properties to be proven automatically by a variety of program verification tools spanning type checkers, static analyzers, and theorem provers. Notable examples include Microsoft Code Contracts for .NET programs [1] and the Verified Software Toolchain spanning C source code to machine language [2].

Many different approaches have been proposed in the literature to infer loop invariants. The problem is undecidable, however, and even practical instances are challenging, which greatly limits the benefits of program verification technology. Existing approaches suffer from key drawbacks: they are purely search-based, or they use hand-crafted features, or they are based on supervised learning. The performance of search-based approaches is greatly hindered by their inability to learn from past mistakes. Hand-crafted features limit the space of possible invariants, e.g., Garg et al. [3] is limited to features of the form $x \pm y \leq c$ where $c$ is a constant, and thus cannot handle invariants that involve $x + y \leq z$ for program variables $x, y, z$. Finally, obtaining ground truth solutions needed by supervised learning is hindered by the undecidability of the loop invariant generation problem.

In this paper, we propose an end-to-end learning-based approach to infer loop invariants. Our approach has the ability to automatically learn rich latent representations of desirable invariants, and can avoid

*Both authors contributed equally to the paper.

32nd Conference on Neural Information Processing Systems (NIPS 2018), Montréal, Canada.
repeating similar mistakes. Furthermore, it leverages reinforcement learning to discover invariants by partial feedback from trial-and-error, without needing ground truth solutions for training.

Our framework is inspired by the reasoning exercised by human experts. Given a program, a human expert first maps the program to well-organized structural representation, and then composes the loop invariant step by step. Based on such reasoning, different parts of the representation get highlighted at each step. To mimic this procedure, we utilize a graph neural network model (GNN) to construct the structural external memory representation of the program. The multi-step decision making is implemented by an autoregressive model, which queries the external memory using an attention mechanism. The decision at each step is a syntax- and semantics-guided decoder which generates subparts of the loop invariant.

Since it is computationally intensive to obtain ground truth solutions, we address this challenge by setting up a novel reinforcement learning problem. Although reinforcement learning algorithms have shown remarkable success in domains like combinatorial optimization \cite{3, 4} (see Section 6 for more discussion on related work), our setting differs in two crucial ways: first, it has a non-continuous objective function (i.e., a proposed loop invariant is correct or not); and second, the positive reward is extremely sparse and given only after the correct loop invariant is proposed, by an automated theorem prover \cite{6}. We therefore model the policy learning as a multi-step decision making process: it provides a fine-grained reward at each step of building the loop invariant, followed by continuous feedback in the last step based on counterexamples collected by the agent itself during trial-and-error learning.

We evaluate our approach, called CODE2INV, on a suite of 133 benchmark problems from recent works \cite{3, 7, 8} and the 2017 SyGuS program synthesis competition \cite{9}. We also compare it to three state-of-the-art systems: C2I \cite{10}, a stochastic search-based system; LOOPINVGEN \cite{8}, a heuristic search-based system; and ICE-DT \cite{3}, a decision tree learning-based system. CODE2INV solves 106 problems, versus 73 by C2I, 77 by LOOPINVGEN, and 100 by ICE-DT. Moreover, CODE2INV exhibits better learning, making orders-of-magnitude fewer calls to the theorem prover than these systems.

2 Background

We formally define the loop invariant inference and learning problems by introducing Hoare logic \cite{1}, which comprises a set of axioms and inference rules for proving program correctness assertions. Let \( P \) and \( Q \) denote predicates over program variables and let \( S \) denote a program. We say that \textit{Hoare triple} \( \{ P \} \ S \{ Q \} \) is valid if whenever \( S \) begins executing in a state that satisfies \( P \) and finishes executing, then the resulting state satisfies \( Q \). We call \( P \) and \( Q \) the pre-condition and post-condition respectively of \( S \). Hoare rules allow to derive such triples inductively over the structure of \( S \). The rule most relevant for our purpose is that for loops:

\[
\begin{align*}
P &\Rightarrow I \ (pre) \\
\{ I \land B \} &\ S \{ I \} \ (inv) \\
\{ I \land \neg B \} &\Rightarrow Q \ (post)
\end{align*}
\]

Predicate \( I \) is called a \textit{loop invariant}, an assertion that holds before and after each iteration, as shown in the premise of the rule. We can now formally state the loop invariant inference problem:

\textbf{Problem 1 (Loop Invariant Inference):} Given a pre-condition \( P \), a post-condition \( Q \) and a program \( S \) containing a single loop, can we find a predicate \( I \) such that \( \{ P \} \ S \{ Q \} \) is valid?

Given a candidate loop invariant, it is straightforward for an automated theorem prover such as Z3 \cite{6} to check whether the three conditions denoted \textit{pre}, \textit{inv} and \textit{post} in the premise of the above rule hold, and thereby prove the property asserted in the conclusion of the rule. If any of the three conditions fails to hold, the theorem prover returns a concrete counterexample witnessing the failure.

The loop invariant inference problem is undecidable. Moreover, even seemingly simple instances are challenging, as we illustrate next with the program shown in Figure 1(b). The goal is to prove that assertion \( y > 0 \) holds at the end of the program, for every input value of integer variable \( y \). In this case, the pre-condition \( P \) is \textit{true} since the input value of \( y \) is unconstrained, and the post-condition \( Q \) is \( y > 0 \), the assertion to be proven. Using predicate \( x < 0 \lor y > 0 \) as the loop invariant \( I \) suffices to prove the assertion, as shown in Figure 1(b). Notation \( \phi[e/x] \) denotes the predicate \( \phi \) with each occurrence of variable \( x \) replaced by expression \( e \). This loop invariant is non-trivial to infer. The reasoning is simple in the case when the input value of \( y \) is non-negative, but far more subtle in the case when it is negative: regardless of how negative it is at the beginning, the loop will iterate at least as many times as to make it positive, thereby ensuring the desired assertion upon finishing. Indeed, a state-of-the-art loop invariant generator \textsc{LoopInvGen} \cite{8} crashes on this problem instance after making 1,119 calls to Z3, whereas our approach successfully generates it after only 26 such calls.
We propose to use a neural network to mimic the reasoning used by human experts as described above. We observe that the entire reasoning process consists of three key components: 1) organize the program which they are updated in the loop. Instead of reasoning about the entire assertion at once, an expert is likely to focus on updates to one variable at a time. This reasoning yields the observation that a,b \in \{-1,0,1\},c \in \mathbb{Z}. In [8], these features are generalized by systematic enumeration. In [10], stochastic search is performed over a set of constraint templates. While such features or templates perform well in specific domains, they may fail to adapt to new domains. Moreover, even in the same domain, they do not benefit from past experiences: successfully inferring the loop invariant for one program does not speed up the process of inferring other similar ones. We hereby formulate the second problem that our approach aims to address:

Problem 2 (Loop Invariant Learning): Given a set of programs \( \{ S_i \} \sim \mathcal{P} \) that are sampled from some unknown distribution \( \mathcal{P} \), can we learn from them and generalize the strategy we learned to other programs \( \{ S_i \} \) that are from the same distribution?

3 End-to-End Reasoning Framework

3.1 The reasoning process of a human expert

We start out by illustrating how a human expert might typically accomplish the task of inferring a loop invariant. Consider the example in Figure 2 chosen from our benchmarks.

An expert usually starts by reading the assertion (line 15), which contains variables \( x \) and \( y \), then determines the locations where these two variables are initialized, and then focuses on the locations where they are updated in the loop. Instead of reasoning about the entire assertion at once, an expert is likely to focus on updates to one variable at a time. This reasoning yields the observation that \( x \) is initialized to zero (line 2) and may get incremented in each iteration (line 5,9). Thus, the sub goal “\( x < 4 \)” may not always hold, given that the loop iterates non-deterministically. This in turn forces the other part “\( y > 2 \)” to be true when “\( x > 4 \)”.

The key idea is to replace the above three components with corresponding differentiable modules:

- a structured external memory representation which encodes the program;
- a multi-step autoregressive model for incremental loop invariant construction; and
- a hierarchical-structured way rather than a sequence of tokens; 2) compose the loop invariant step by step; and 3) focus on a different part of the program at each step, depending on the inference logic, e.g., abduction and induction.

3.2 Programming the reasoning procedure with neural networks

We propose to use a neural network to mimic the reasoning used by human experts as described above. The example in Figure 2 is given as an example from our benchmarks. "*" denotes non-deterministic choice.

```
1  int main() {
2   int x = 0, y = 0;
3   while (*) {
4     if (*) {
5       x++;
6     } else if (*) {
7       y = 100;
8       if (x >= 4) {
9         x++;
10      }
11    } else if (*) {
12      y--;
13    }
14   } assert( x < 4 || y > 2);
15  }
```

Figure 2: An example from our benchmarks. "*" denotes non-deterministic choice.
an attention component that mimics the varying focus in each step.

As shown in Figure 3, these modules together build up the network that constructs loop invariants from programs, while being jointly trained with reinforcement learning that described in Section 4. At each step, the neural network will generate a partial loop invariant. Then given the current generated partial tree, a TreeLSTM module summarizes what have been generated so far, and the summarization is used to read the memory using attention. Lastly, the summarization, together with the read memory is fed into next time step. In the following sections, we will elaborate these three components.

### 3.2.1 Structured external memory

The loop invariant is built within the given context of program. Thus it is natural to encode the program with external memory module. However, different from the traditional memory networks [19] [20], where the memory slots are organized as linear array, here the program has rich structure information. Though theoretically using a chain LSTM over program tokens would capture the information in the code, it is very hard for neural networks to understand with limited data. Inspired by Allamanis et al. [21], we instead use a graph-structured memory representation. Such representation will allow us to preserve rich semantic information of the program such as control and data flows.

More concretely, we first convert a given program into static single assignment (SSA) form [22], and construct a control flow graph, each of whose nodes represents a single program statement. We then transform each node into an abstract syntax tree (AST) representing the corresponding statement. Thus a program can be represented by a graph $G = (V, E)$, where $V$ contains terminals and nonterminals of the ASTs, and $E = \{(e_x^{(i)}, e_y^{(i)}, e_t^{(i)}) \mid i \in 1 \}$ is the set of edges. The directed edge $(e_x^{(i)}, e_y^{(i)}, e_t^{(i)})$ starts from node $e_x^{(i)}$ to $e_y^{(i)}$, with $e_t^{(i)} \in \{1, 2, ..., K\}$ representing edge type. In our construction, the program graph contains 3 different edge types (and 6 after adding reversed edges).

![Figure 3: Overall framework of neuralizing loop invariant inference.](image)

![Figure 4: Diagram for source code graph as external structured memory. We convert a given program into a graph $G$, where nodes correspond to syntax elements, and edges indicate the control flow, syntax tree structure, or variable linking. We use embedding neural network to get structured memory $f(G)$.](image)
To convert the graph into vector representation, we follow the general message passing operator introduced in graph neural network (GNN) \([23]\) and its variants \([21, 24, 25]\). Specifically, the graph network will associate each node \(v \in V\) with an embedding vector \(\mu_v \in \mathbb{R}^d\). The embedding is updated iteratively using the general neighborhood embedding as follows:

\[
\mu^{(t+1)}_v = h(\{\mu^{(t)}_u \mid u \in N^k(v), k \in \{1, 2, ..., K\}\})
\]

Here \(h(\cdot)\) is a nonlinear function that aggregates the neighborhood information to update the embedding. \(N^k(v)\) is the set of neighbor nodes connected to \(v\) with edge type \(k\), i.e., \(N^k(v) = \{u \mid (u, v, k) \in E\}\).

Such process will be repeated for \(L\) steps, and the node embedding \(\mu_v\) is set to \(\mu^{(L)}_v\) \(\forall v \in V\). Our parameterization takes the edge types into account. The specific parameterization used is shown below:

\[
\mu^{(t+1), k}_v = \sigma(\sum_{u \in N^k(v)} W_2 \mu^{(t)}_u), \forall k \in \{1, 2, ..., K\}
\]

\[
\mu^{(t+1)}_v = \sigma(W_1 [\mu^{(t+1), 1}_v, \mu^{(t+1), 2}_v, ..., \mu^{(t+1), K}_v])
\]

with the boundary case \(\mu^{(0)}_v = W_1 x_v\). Here \(x_v\) represents the syntax information of node \(v\), such as token or constant value in the program. Matrices \(W_{1,2,3}\) are learnable model parameters, and \(\sigma\) is some nonlinear activation function. Figure 4 shows the construction of graph structured memory using iterative message passing operator in Eq (1), \(f(G) = \{\mu_v\}_{v \in V}\) denotes the structured memory.

### 3.2.2 Multi-step decision making process

A loop invariant itself is a mini-program that contains expressions and logical operations. Without loss of generality, we define the loop invariant to be a tree \(T\), in a form with conjunctions of disjunctions:

\[
T = (T_1 \land T_2 \ldots) \land (T_{t+1} \land T_{t+2} \ldots) \land \ldots (\ldots T_{T-1} \land T_{T})
\]

Each subtree \(T_i\) is a simple logic expression (i.e., \(x < y \ast 2 + 10 - z\)). Given this representation form, it is natural to use Markov decision process (MDP) to model this problem, where the corresponding \(T\)-step finite horizon MDP is defined as \(\mathcal{M}_T = (S_1, a_1, r_1, s_2, a_2, \ldots, s_T)\). Here \(s_1, a_1, r_1\) represent the state, action and reward at time step \(t = 1, \ldots, T-1\), respectively. Here we describe the state and action used in the inference model, and describe the design of reward and termination in Section 4.

**action:** As defined in Eq \([4]\), a loop invariant tree \(T\) consists of multiple subtrees \(\{T_i\}\). Thus we model the action at time step \(t\) as \(a_t = (op_t, T_t)\), where \(op_t\) can either be \(\land\) or \(\lor\). That is to say, at each time step, the agent first decides whether to attach the subexpression \(T_t\) to an existing disjunction, or create a new disjunction and add it to the list of conjunctions. We use \(T^{(<t)}\) to denote the partial tree generated by time \(t\) so far. So the policy \(\pi(T|G)\) is decomposed into:

\[
\pi(T|G) = \prod_{t=1}^{T} \pi(a_t|T^{(<t)}, G) = \prod_{t=1}^{T} \pi(op_t, T_t|T^{(<t)}, G)
\]

where \(T^{(<t)}\) is empty at the first step. The generation process of subtree \(T_t\) is also an autoregressive model implemented by LSTM. However, generating a valid program is nontrivial, since strong syntax and semantics constraints should be enforced. Recent advances in neural program synthesis \([26, 27]\) utilize formal language information to help the generation process. Here we use the Syntax-Directed decoder proposed in \([28]\) to guarantee both the syntax and semantics validity. Specifically,

- **Syntax constraints:** The AST generation follows the grammar of loop invariants described in Eq \([4]\). Operators such as +, -, \ast, \ast are non-terminal nodes in the AST while operands such as constants or variables are leaf nodes.

- **Semantic constraints:** We regulate the generated loop invariant to be meaningful. For example, a valid loop invariant must contains all the variables that appear in the given assertion. Otherwise, the missing variables can take arbitrary values, causing the assertion to be violated. In contrast to offline checking which discards invalid programs after generation, such online regulation restricts the output space of the program generative model, which in turn makes learning efficient.

**state:** At time step \(t = 1\), the state is simply the weighted average of structured memory \(f(G)\). At each later time step \(t > 1\), the action \(a_t\) should be conditioned on graph memory, as well as the partial tree generated so far. Thus \(s_t = (G, T^{(<t)})\).

### 3.2.3 Memory query with attention

At different time steps of inference, human usually focuses on different parts of program. Thus the attention mechanism is a good choice to mimic such process. Specifically, at time step \(t\), to summarize
what we have generated so far, we use TreeLSTM \cite{DBLP:conf/icml/Kipf16} to embed the partial tree $T^{(<t)}$. Then the embedding of partial tree $v_{T^{(<t)}} = \text{TreeLSTM}(T^{(<t)})$ is used as the query to read the structured memory $f(G)$. Specifically, read$(f(G), v_{T^{(<t)}}) = \sum_{v \in V} \alpha_v \mu_v$ and $\alpha_v = \exp(\mu_v) v_{T^{(<t)}}$ are the corresponding attention weights.

4 Learning

The undecidability of the loop invariant generation problem hinders the ability to obtain ground truth solutions as supervisions for training. Inspired by recent advances in combinatorial optimization \cite{DBLP:conf/icml/Kipf16, DBLP:conf/icml/Kipf17}, where the agent learns a good policy by trial-and-error, we employ reinforcement learning to learn to propose loop invariants. Ideally, we seek to learn a policy $\pi(T|G)$ that proposes a correct loop invariant $T$ for a program graph $G$. However, directly solving such a model is practically not feasible, since:

- In contrast to problems tackled by existing work, where the objective function is continuous (e.g., tour length of traveling salesman problem), the proposed loop invariant only has binary objective (i.e., correct or not). This makes the loss surface of the objective function highly non-smooth.
- Finding the loop invariant is a bandit problem where the binary reward is given only after the invariant is proposed. Also, in contrast to two player games \cite{DBLP:conf/nips/Silver17} where a default policy (e.g., random rollout) can be used to estimate the reward, it is a single player game with an extremely sparse reward.

To tackle the above two challenges, the multi-step decision making model proposed in Section 3.2.2 is used, where a fine-grained reward is also designed for each step. In the last step, a continuous feedback is provided based on the counterexamples collected by the agent itself.

4.1 Reinforcement learning setup

Section 3.2.2 defines the state and action representation used for inference. We next describe our setup of the environment which is important to properly train a reinforcement learning agent.

**reward:** In each intermediate step $t \in 1, \ldots, T-1$, an intermediate reward $r_t$ is given to regulate the generation process. For example, a subexpression should be non-trivial, and it should not contradict $T^{(<t)}$. In the last step, the generated loop invariant $T$ is given to a theorem prover, which returns success or failure. In the latter case, the theorem prover also tells which step (pre, inv, post) failed, and provides a counterexample. The failure step can be viewed as a “milestone” of the verification process, providing a coarse granularity feedback. To achieve continuous (i.e., fine granularity) reward within each step, we exploit the counterexamples collected so far. For instance, the ratio of passed examples is provided as a coarse indicator of the learning progress. Appendix A.1 describes the reward design in detail.

**termination:** There are several conditions that may trigger the termination of tree generation: (1) the agent executes the “stop” action, as illustrated in Figure 3 (2) the generated tree has the maximum number of branches allowed; or (3) the agent generates an invalid action.

4.2 Training of the learning agent

We use advantage actor critic (A2C) to train the above reinforcement learning policy. Specifically, let $\theta = \{W_{\psi}\}$ be the parameters in graph memory representation $f(\cdot; \theta)$, and $\phi$ be the parameter used in $\pi(a_t|T^{(<t)}, G; \phi)$, our objective is to maximize the expected policy reward:

$$\max_{\theta, \phi} \mathbb{E}_{\pi_{\text{opt}}, T_t|T^{(<t)}, G; \phi} \left( \sum_{t'=t}^T \gamma^{t'-t} r_{t'} - b(T^{(<t)}, G; \psi) \right)$$

(6)

The baseline function $b(T^{(<t)}, G; \psi)$ parameterized by $\psi$ is used to estimate the expected return, so as to reduce the variance of policy gradient. It is trained to minimize $\mathbb{E}_{\pi, t} \| b(T^{(<t)}, G; \psi) \|$.

**termination:** We simply apply two layer fully connected neural network to predict the expected return. $\gamma$ is the discounting factor. Since the MDP is finite horizon, we use $\gamma = 1$ to address the long-term reward.

5 Experiments

We evaluate our approach, called Code2Inv \cite{DBLP:journals/corr/abs-1805-00496}, on a suite of 133 benchmark programs from recent works \cite{DBLP:conf/pldi/Cavaretta13, DBLP:journals/pacmpl/Sharma17} and the 2017 SyGuS competition \cite{DBLP:journals/pldi/Decker19}. Each program consists of three parts: a number of assumption or assignment statements, one loop which contains nested if-else statements with arithmetic

\footnote{Code and data are available at: https://github.com/PL-ML/code2inv}
We next study the effectiveness of two key components in our framework via ablation experiments: counterexamples and attention mechanism. We use the same dataset as in Section 5.1. Table 4 shows our ablation study results. We see that besides providing a continuous reward, the use of counterexamples (CE) significantly reduces the verification cost, i.e., number of Z3 queries. On the other hand, the attention mechanism helps to reduce the training cost, i.e., number of parameters updates. Also, it
helps to reduce the verification cost modestly. CODE2INV achieves the best performance with both components enabled, and we use this configuration for evaluations in other places.

Additionally, to test the effectiveness of neural graph embedding, we study a simpler encoding, that is, view a program as a sequence of tokens and encode the sequence using an LSTM. The performance of this setup is shown in the last row of Table 1. With a simple LSTM embedding, CODE2INV solves 13 fewer instances but requires much more number of parameter updates.

### Table 1: Ablation study for different configurations of CODE2INV.

<table>
<thead>
<tr>
<th>configuration</th>
<th>#solved instances</th>
<th>max #Z3 queries</th>
<th>max #parameter updates</th>
</tr>
</thead>
<tbody>
<tr>
<td>without CE, without attention</td>
<td>91</td>
<td>415K</td>
<td>441K</td>
</tr>
<tr>
<td>without CE, with attention</td>
<td>94</td>
<td>147K</td>
<td>162K</td>
</tr>
<tr>
<td>with CE, without attention</td>
<td>95</td>
<td>392</td>
<td>337K</td>
</tr>
<tr>
<td>with CE, with attention</td>
<td>106</td>
<td>276</td>
<td>290K</td>
</tr>
<tr>
<td>LSTM embedding + CE + attention</td>
<td>93</td>
<td>32</td>
<td>661K</td>
</tr>
</tbody>
</table>

#### 5.3 Boosting the search with pre-training

We next address the question: given an agent that is pre-trained on programs $P_{\text{train}} = \{p_i\} \sim \mathcal{P}$, can the agent solve new programs $P_{\text{test}} = \{\tilde{p}_i\} \sim \mathcal{P}$ faster than solving from scratch? We prepare the training and testing data as follows. We take the programs solved by CODE2INV as the initial set and augment it by creating 100 variations for each of them by introducing confounding variables and statements in such a way that any valid loop invariant for the original program is still valid. Further details are provided in Appendix B. Finally, 90% of them serves as $P_{\text{train}}$, and the rest are used for $P_{\text{test}}$.

After pre-training the agent on $P_{\text{train}}$ for 50 epochs, we save the model and then reuse it for “fine tuning” (or active search [4]), i.e., the agent continues the trial-and-error reinforcement learning, on $P_{\text{test}}$. Figures 6a and 6b compare the verification costs between the pre-trained model and untrained model on datasets augmented with 1 and 5 confounding variables, respectively. We observe that, on one hand, the pre-trained model has a clear advantage over the untrained model on either dataset; but on the other hand, this gap reduces when more confounding variables are introduced. This result suggests an interesting future research direction: how to design a learning agent to effectively figure out loop invariant related variables from a potentially large number of confounding variables.

#### 5.4 Attention visualization

Figure 6c and 6d show the attention highlights for two example programs. The original highlights are provided on the program graph representation described in Section 3.2.1. We manually converted the graphs back to source code for clarity. Figure 6c shows an interesting example for which CODE2INV...
learns a strategy of showing the assertion is actually not reachable, and thus holds trivially. Figure 6d shows another interesting example for which CODE2INV performs a form of abductive reasoning.

5.5 Discussion of limitations

We conclude our study with a discussion of limitations. Most of the problems that CODE2INV fails to solve have loop invariants in a compact disjunctive normal form (DNF) representation, which is more suited for the decision tree learning approach with hand-crafted features. However, CODE2INV is designed to produce loop invariants in the conjunctive normal form (CNF). The reduction of loop invariants from DNF to CNF could incur an exponential blowup in size. An interesting future research direction concerns designing a learning agent that can flexibly switch between these two forms.

6 Related Work

We survey work in program synthesis, program learning, learning loop invariants, and learning combinatorial optimizations.

Program synthesis  Automatically synthesizing a program from its specification has been a key challenge problem since Manna and Waldinger’s work [32]. In this context, syntax-guided synthesis (SuGuS) [9] was proposed as a common format to express these problems. Besides several implementations of SyGuS solvers [9, 33–35], a number of probabilistic techniques have been proposed to model syntactic aspects of programs and to accelerate synthesis [36–38]. While logical program synthesis approaches guarantee semantic correctness, however, they are chiefly limited by their scalability and requirement of rigorous specifications.

Program learning  There have been several attempts to learn general programs using neural networks. One large class of projects includes those attempting to use neural networks to accelerate the discovery of conventional programs [39–42]. Most existing works only consider specifications which are in the form input-output examples, where weak supervision [43–45] or more fine grained trace information is provided to help training. In our setting, there is no supervision for the ground truth loop invariant, and the agent needs to be able to compose a loop invariant purely from trial-and-error. Drawing inspiration from both programming languages and embedding methods, we build up an efficient learning agent that can perform end-to-end reasoning, in a way that mimics human experts.

Learning loop invariants  Our work is closely related to two recent work [46, 47] that learn loop invariants from either labeled ground truth or active interactions with human experts. Brockschmidt et al. [46] concern learning shape invariants for data structures (e.g. linked list, trees). Their approach first extracts features using n-gram and reachability statistics over program heap graph and then applies supervised learning to train a neural network to mapping features to shape invariants. While our work concerns general loop invariant generation, which uses graph embedding directly on the source code AST and learns a generation policy without using groundtruth as supervision. Bounov et al. [47] propose inferring loop invariants through gamification and crowdsourcing, which relieves the requirement of expertise on software verification but still requires significant human effort. In contrast, an automated theorem prover like Z3 [6] is sufficient for our approach.

Learning combinatorial optimizations  Our work is also related to recent advances in combinatorial optimization with machine learning [4, 5, 48, 49]. However, as elaborated in Section 4, the problem we study is significantly more difficult, in the sense that the objective function is non-smooth (binary objective), and the positive reward is extremely sparse due to the exponentially growing size of the search space with respect to program size.

7 Conclusion

We studied the problem of learning loop invariants for program verification. Our proposed end-to-end reasoning framework learns to compose the solution automatically without any supervision. It solves a comparable number of benchmarks as the state-of-the-art solvers while requiring much fewer queries to a theorem prover. Moreover, after being pre-trained, it can generalize the strategy to new instances much faster than starting from scratch. In the future, we plan to extend the framework to discover loop invariants for larger programs which present more confounding variables, as well as to discover other kinds of program correctness properties such as ranking functions for proving program termination [50] and separation predicates for proving correctness of pointer-manipulating programs [51].

Acknowledgments. We thank the anonymous reviewers for insightful comments. We thank Ningning Xie for useful feedback. This project was supported by DARPA #FA8750-15-2-0009 and NSF CCF #1526270. Le Song and Hanjun Dai was supported in part by NSF IIS-1218749, NIH BIGDATA 1R01GM108341, NSF CAREER IIS-1350983, NSF IIS-1639792 EAGER, NSF CNS-1704701, ONR N00014-15-1-2340, NSF CCF-1836822, NSF IIS-1841351 EAGER, Intel ISTC, NVIDIA, Siemens and Amazon AWS.
References


Appendix

A  Details about learning

A.1  Reward Design

Our reward function consists of two parts: early reward and continuous reward.

**Early reward**  The early reward constitutes quick feedback obtained by performing lightweight structure checks during the process of loop invariant generation. The goal is to quickly remove meaningless predicates that are trivially true (e.g. "e==e") or false (e.g. "e<e") or missing variables (e.g. "l<2"), or simple contradictions like "e1<e2 & & e1>e2". Early reward is computed at the end of each action; if the partially generated invariant fails to pass the above checks, the generation process terminates immediately by returning a large negative reward \(-4\); otherwise, a positive reward \(0.5\) is given. Note that one promising future work could be taking advantage of UNSAT cores from counterexamples to identify contradictory parts of the candidate invariant. These contradictory parts will be "non-trivial" contradictions, compared to trivial patterns we have considered.

**Continuous reward**  The goal of continuous reward is to reflect proof progress smoothly. It is computed after the loop invariant is generated and is based on three kinds of counterexamples. Let \(ce_{pre}, ce_{inv}, ce_{post}\) denote the sets of counterexamples accumulated so far at the pre, inv, post step, respectively. Similarly, let \(pass_{pre}, pass_{inv}, pass_{post}\) be the sets of counterexamples passed by current loop invariant candidate. The continuous reward is modeled as a function that takes these six sets of counterexamples as input and produces a scalar value. We used a simple but effective function, that is, the sum of ratios. Specifically, in the case no new counterexample is introduced, we used the sum of passed ratios of counterexamples:

\[
\frac{|pass_{pre}|}{|ce_{pre}|} + \frac{|pass_{inv}|}{|ce_{inv}|} + \frac{|pass_{post}|}{|ce_{post}|}
\]

When a new counterexample is returned, we used the staged sum:

\[
\frac{|pass_{pre}|}{|ce_{pre}|} + \frac{|pass_{pre}=ce_{pre}|}{|ce_{inv}|} + \frac{|pass_{inv}|}{|ce_{inv}|} + \frac{|pass_{inv}=ce_{pre}||pass_{post}=ce_{inv}|}{|ce_{post}|} + \frac{|pass_{post}|}{|ce_{post}|}
\]

where \([\cdot]\) is Iverson bracket. It examines counterexamples in an ordered way (i.e. pre, inv, post) so that counterexamples in the next step are considered only after all counterexamples in the previous step get passed. When we get the highest continuous reward, which is 3, we invoke the theorem prover to verify the current loop invariant candidate; if the theorem prover accepts it, then a correct loop invariant is found; otherwise, a new counterexample is returned, and we recompute the continuous reward according to the above reward function.

A.2  Hyperparameters

By default, the embedding size used throughout the paper is 128. Batch size is set to 10. To compute the graph structured external memory representation, we run the message passing operator (as described in Equation (1)) for 20 steps. Learning rate is set to 0.001 and fixed.

We maintain a circular buffer for the counterexamples. The buffer size is set to 100, i.e., we remove the old counterexamples when the buffer size is exceeded (although we seldom reached the 100 limit in our experiments). We use the counterexample to compute continuous feedback only after we collect 5 or more of them.

B  Dataset

Our dataset is collected from recent literature [2][7] and the 2017 SyGuS competition [31]. Dillig et al. [7] create a suite of 46 C programs for evaluation of loop invariant inference, on top of which Garg et al. [3] introduce 40 more benchmarks. The 2017 SyGuS competition consists of 74 benchmarks, which is in the SMT-LIB like format [52]. We manually convert benchmarks from SyGuS competition to C programs, which have some overlaps with the above two benchmark suite, so we remove the overlapped ones. Figure 7 shows some example programs in the SyGuS challenge dataset.
B.1 Training data augmentation

We augment the training dataset on top of the set of programs that Code2Inv can solve. Given a program, we first randomly select an integer K ranging from 1 to 5, which is the number of confounding variables to insert. Then, we initialize each newly created variable with a value ranging from -100 and 100. After that, we insert a statement after each statement in the loop body. The newly inserted statement only uses confounding variables and constants so that any valid loop invariant in the original program is still valid after augmentation. The lvalue of the statement is randomly and uniformly sampled from confounding variables, and for the rvalue expression of statement, we first randomly choose a depth (either 1 or 2) for the AST tree of the expression, then randomly and uniformly pick an operator from \{+, -, \ast\}, and operands from confounding variables and constants ranging between -100 and 100. For each program and each chosen parameter K, we repeat the above process a 100 times.

C Attention score interpretation

The learned attention scores measure the importance of different nodes in the program graph memory. In Figure 6(c) and 6(d), we converted the attention into the raw program file. Here we include the original graphs, together with the attentions that represented by different scale of colors. See Figure 8 and 9.

![Code snippets for Figure 7: Examples of programs in SyGuS challenge dataset (after converting to C).](image-url)
Figure 8: Attention over program graph, which converts to Figure 6c in main text.
Figure 9: Attention over program graph, which converts to Figure 6d in main text.