Using Dynamically Inferred Invariants to Analyze Program Runtime Complexity

ThanhVu Nguyen  Didier Ishimwe  Alexey Malyshev
University of Nebraska-Lincoln  University of Nebraska-Lincoln  University of Nebraska-Lincoln
USA  USA  USA

Timos Antonopoulos  Quoc-Sang Phan
Yale University  Synopsys
USA  USA

ABSTRACT
Being able to detect program runtime complexity can help identify security vulnerabilities such as DoS attacks and side-channel information leakage. In prior work, we use dynamic invariant generation to infer nonlinear numerical relations to represent runtime complexity of imperative programs. In this work, we propose a new dynamic analysis approach for learning recurrence relations to capture complexity bounds for recursive programs. This approach allows us to efficiently infer simple linear recurrence relations that represent nontrivial, potentially nonlinear, complexity bounds. Preliminary results on several popular recursive programs show that we can learn precise recurrence relations capturing worst-case complexity bounds such as $O(n \log n)$ and $O(c^n)$.

CCS CONCEPTS
• Software and its engineering → Software testing and debugging; • Security and privacy → Software security engineering.

KEYWORDS
dynamic invariant generation, complexity analysis, recurrence relations, numerical relations

ACM Reference Format:

1 INTRODUCTION
The automated discovery of program invariants—relations among variables that are guaranteed to hold at certain locations of a program—is an important research area in program analysis, verification, and synthesis. Generated invariants can be used to understand undocumented programs, prove correctness assertions, establish security properties, provide formal documentation, and more [5, 13–15, 25, 29].

In [32, 34], we developed DIG, a dynamic invariant generation tool that learns numerical invariants involving relations among numerical program variables. In particular, DIG supports nonlinear polynomial relations, e.g., $x \leq y^q, x = qy + r$. These relations arise in many scientific, engineering, and safety- and security-critical software, e.g., to verify the absence of errors in Airbus avionic systems [11]. A rather surprising use of DIG’s nonlinear invariants is that they can help characterize program runtime complexity, by instrumenting a counter for the number of blocks executed and inferring a relationship involving that counter and the program’s input variables, at the end of the program's execution [32]. For example, it can be shown this way that a program runs in $O(n^2 + 2m)$ for certain inputs and $O(m)$ for other inputs.

In this paper, we propose a new dynamic analysis for learning recurrence relations to capture complexity bounds for recursive programs. At high level, a recurrence relation defines the complexity to solve a problem in terms of the complexities to solve its subproblems. The dynamic technique allows us to efficiently infer simple linear recurrence relations that represent nontrivial, potentially nonlinear, complexity bounds. When applied to several classical divide-and-conquer algorithms, we were able to learn precise recurrence relations capturing worst-case complexity bounds such as $O(n \log n)$ or $O(c^n)$ from execution traces obtained by running the programs using few randomly generated inputs.

What distinguishes our work from other complexity analyses (e.g., [21, 22, 27, 35] and those reviewed in Section 4) is the use of dynamic, instead of static, analysis to learn program complexity bounds. In general, a static analysis can reason about all program paths soundly, but doing so is often expensive and is only possible for relatively simple forms of invariant relations or restricted classes of programs. Dynamic analyses limit their attention to only some of a program’s paths, and thus provide no guarantee that those invariants are correct, but can often be more efficient and produce more expressive results [16, 34]. We can also improve correctness by using symbolic execution techniques to check for spurious results [33] and generate worst-case complexity inputs leading to high-complexity program paths [6, 30, 35].
When solving this equation (finding the roots of (potentially nonlinear) numerical invariants, which describe re-
gram to run in different time complexities. The example also shows

As shown in many works [21, 22, 27, 35], complexity analysis, in particular through worst-case execution time (WCET) analysis [41] and high-security input dependent resource analysis, can help detect several important security vulnerabilities [9, 12, 19], e.g., by allowing an attacker to exhaust the system’s resources (time or memory) and perform Denial-of-Service attacks on servers or by exhibiting side-channel information leakage. By knowing the execution times of different high-security dependent branches (e.g., one branch takes linear time while the other takes quadratic time), the developer can mitigate an attack by “padding” the computation so that all executions take the same time (e.g., instrumenting the program to add dummy loops, instructions, or delays).

2 LEARNING POLYNOMIAL RELATIONS

In [32, 34], we developed DIG, a dynamic analysis tool that learns (potentially nonlinear) numerical invariants, which describe relations over numerical variables at arbitrary program locations. DIG’s invariants can help understand programs and characterize their runtime complexities, which is useful for identifying possible security problems [4, 31].

Example. Figure 1 shows trip ple, a program adapted from Figure 2 of [22] with nontrivial input complexity. At first, trip ple appears to take O(NMP) due to the three nested loops. A closer analysis [22] shows a more precise bound O(N + NM + P) because the inner most loop, which is updated each time the middle loop executes, changes the behavior of the outer most loop.

When given this program, DIG discovers an interesting and complex postcondition at location L about the variable t, which is a ghost variable introduced to count loop iterations:

\[
\begin{align*}
\text{P}^3\text{Mt} + \text{PM}^2t - \text{PMT} - M^2\text{Lt} - \text{PMT}^2 + \text{MNT}^2 + \text{PMTL} = \\
\text{PNT} - 2\text{MNT} + \text{Pt}^2 + \text{M}^2 + \text{N}^2 - t^3 - \text{N}t + t^2 = 0.
\end{align*}
\]

This nonlinear inequality is valid, but incomprehensible and quite different than the expected bound N + NM + P or even NMP. However, when solving this equation (finding the roots of t), we obtain three solutions that describe the exact bounds of this program:

\[
t = \begin{cases} 
0 & \text{when } N = 0 \\
\text{P} + \text{M} + 1 & \text{when } N \leq \text{P} \\
\text{N} - \text{M}(\text{P} - \text{N}) & \text{when } N > \text{P}
\end{cases}
\]

These results are more precise than the bound N + NM + P given in [22] and can help developers reason about inputs causing the program to run in different time complexities. The example also shows that complexity analysis can help detect side-channel information leakage, e.g., if some of the inputs from M, N and P are high-security and some are public, an attacker can infer valuable information about the high-security inputs by observing the running time of the program.

3 LEARNING RECURRENCE RELATIONS

Polynomial relations can help capture general program complexity. However, for recursive, e.g., divide-and-conquer, programs we can generate recurrence relations [10] to compute complexity more precisely. Using dynamic analysis to infer recurrent relations is relatively straightforward and a linear recurrence relation can capture complex program bounds such as those involving log or nonlinear degrees.

A recurrence relation (or simply recurrence) defines the complexity to solve a problem in terms of the complexities to solve its subproblems. For example, we can compute the recurrence for the standard mergesort algorithm as \( T(n) = 2T\left(\frac{n}{2}\right) + O(n) \), i.e., the algorithm splits the problem into two subproblems of half the sizes of the original problem and merges the results of the subproblems in linear time. Next, solving this recurrence, e.g., using the well-known Master Theorem [10], gives the asymptotic complexity \( O(n \log n) \). Thus, we can obtain difficult program complexity bounds by inferring and solving relatively simple recurrence relations, e.g., we obtain mergesort’s complexity involving log from a recurrence that does not directly involve log.

Example. For the mergesort program in Figure 2, we instrument the program with the new variables i d and t to keep track of recursive calls. We also record execution traces at the program entrance to capture the length of the input and the unique id of each recursive call.

The tree in Figure 2 shows the program execution traces when applying mergesort to a list of 7 elements. The root node (7, [1]) is the first mergesort call with id [1] on the list of 7 elements. The children nodes (3, [1, 1]) and (4, [1, 2]) respectively represent the first and second recursive calls on the first 3 and the remaining 4 elements of the original list.

We first analyze the recursive parts of merge. From the execution traces, we form tuples of the form \((i_0, t_0)\), where \(i_0\) represents the input length of the original call and \(t_1\) the input length of the first recursive call. We then use a learning technique such as linear regression to find a relation \(t_1 \approx c_0\), which represents the relation between the sizes of the original problem and the subproblems. For example, from the data (7, 3), (3, 1), (2, 1), (4, 2) in the execution tree in Figure 2, we obtain the relation \(t_1 \approx \frac{1}{2}t_0\). Similarly, we obtain \(t_2 \approx \frac{1}{2}t_0\) as the relation between mergesort and its second recursive call. The combination \(t_0 = \frac{1}{2} + \frac{n}{2}\) gives the recurrence \(T(n) = T\left(\frac{n}{2}\right) + T\left(\frac{n}{2}\right)\), indicating that mergesort makes two recursive calls over inputs that are approximately half of the original input.

For the non-recursive merge function, we find a general polynomial relation to capture its complexity. First, we instrument the program using the counter variable I t and increment it in each loop to count the number of executed blocks. Next, from traces recorded at the program exit (using the trace function), we compute the relation \(t \approx 2n + 2\), indicating merge runs in linear time.
There are many static analyses for program complexity, e.g., the transition system to derive upper runtime bounds. Several techniques Hansel et al. [24] use symbolic execution to obtain an integer termination property and non-polynomial worst-case upper bounds. We propose new dynamic analysis techniques to learn numerical and recurrence relations to capture precise program runtime complexity bounds. Using evaluation trees and can derive the complexity bound for mergesort. These works use static or symbolic analyses while we dynamically learn complexity invariants.

The combination of the recursive and non-recursive results gives the recurrence $T(n) = 2T(\frac{n}{2}) + O(n)$ (merge takes linear time). We can now apply the Master Theorem [10] to solve this recurrence to obtain the complexity $O(n \log n)$.

**Evaluation.** We applied the described approach to compute recurrence relations for several recursive programs in OCaml. We manually instrumented each program, ran it on randomly generated inputs to obtain execution traces (e.g., for mergesort we randomly generated input lists of various sizes), and finally computed the recurrences.

Table 1 shows the results. We were able to obtain the correct recurrences for all considered programs. We used the Master Theorem, which supports recurrences of the form $T(n) = aT(\frac{n}{b}) + f(n)$, to compute the complexities of binary search and merge sort. For the other programs, we manually convert their recurrences to program complexities.

### 5 Conclusion and Future Work

We propose new dynamic analysis techniques to learn numerical and recurrence relations to capture precise program runtime complexity bounds. In addition to developing tools implementing these ideas, we are extending the work with other learning techniques such as linear regression [18] and neural networks [42] to compute more general relations to represent inexact, e.g., lower and upper, complexity bounds. We are also exploring existing WCET techniques to generate worst-case complexity inputs and check candidate invariants (e.g., using the guess-and-check approach proposed in [33] to remove spurious results and generate counterexamples to help dynamic inference).

### ACKNOWLEDGMENTS

We thank the anonymous reviewers for helpful comments. This work is supported by the National Science Foundation under Grant CCF-1948536 and the Army Research Office under Grant W911NF-19-1-0054.
REFERENCES


