DIFFLOG: Beyond Deductive Methods in Program Analysis

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

Sulekha Kulkarni  
University of Pennsylvania  
sulekha@cis.upenn.edu

Richard Zhang  
University of Pennsylvania  
rmzhang@cis.upenn.edu

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

Kihong Heo  
University of Pennsylvania  
kheo@cis.upenn.edu

Woosuk Lee  
University of Pennsylvania  
woosuk@cis.upenn.edu

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

Building effective program analysis tools is a challenging endeavor: analysis designers must balance multiple competing objectives, including scalability, fraction of false alarms, and the possibility of missed bugs. Not all of these design decisions are optimal when the analysis is applied to a new program with different coding idioms, environment assumptions, and quality requirements. Furthermore, the alarms produced are typically accompanied by limited information such as their location and abstract counter-examples. We present a framework DIFFLOG that fundamentally extends the deductive reasoning rules that underlie program analyses with numerical weights. Each alarm is now naturally accompanied by a score, indicating quantities such as the confidence that the alarm is a real bug, the anticipated severity, or expected relevance of the alarm to the programmer. To the analysis user, these techniques offer a lens by which to focus their attention on the most important alarms and a uniform method for the tool to interactively generalize from human feedback. To the analysis designer, these techniques offer novel ways to automatically synthesize analysis rules in a data-driven style. DIFFLOG shows large reductions in false alarm rates and missed bugs in large, complex programs, and it advances the state-of-the-art in synthesizing non-trivial analyses.

1 Introduction

The ideal program analysis tool successfully flags the most serious bugs, produces no false alarms, and gracefully scales to arbitrarily large codebases. The challenges involved in building these tools always force a compromise between these competing requirements. Analysis designers strive to identify highly scalable approximations that still produce results with acceptable accuracy, while analysis users demand greater control over the number of alarms produced, ways to prioritize reports that are most likely to be relevant and represent real bugs, and would like the tool to learn these preferences from past interaction.

Traditional approaches to program reasoning rely on deductive techniques where these limitations manifest either as unsound or as incomplete analysis rules. Applied to a large codebase, these analysis rules produce false alarms in statistically regular ways. Furthermore, because multiple alarms share portions of their derivation trees, it follows that they are correlated in their ground truth, an observation which has also been exploited by previous research in improving analysis accuracy [25, 28, 39]. In this paper, we draw inspiration from the large body of research reconciling logical reasoning with machine learning, which has appeared variously as work on probabilistic databases [9, 12], inductive logic programming [29], statistical relational learning [13], and probabilistic programming (e.g. [11] and [14]).
DIFFLOG: Beyond Deductive Methods in Program Analysis

2 Overview of the Framework

We describe our technique using the example of Andersen’s analysis [2] shown in Figure 2a. We express the analysis using Datalog, a popular formalism to declaratively specify complex program reasoning algorithms [35, 38, 6, 4, 27, 3]. A Datalog program is a collection of rules, each of the form $h := b_1, b_2, \ldots, b_k$, where each component, $h, b_1, b_2, \ldots, b_k$, is called a literal. The free variables, $p, q, \ldots$, are implicitly universally quantified, and $\leftarrow$ is interpreted as implication. For example, the rule $R_3$ may be read as “If the program contains the statement $p := \ast q$, and $q$ may point to $r$, and $r$ may point to $s$, then $p$ may point to $s$.” The meaning of a Datalog program is defined as a fixpoint: to apply the analysis, one iteratively accumulates conclusions until no further tuples can be derived.

Now consider the program of Figure 2b. We show a portion of the reasoning induced by applying Andersen’s analysis in Figure 3. Note that the variable $a$ initially points to the memory location $b_1$, and...
Figure 2: Description of Andersen’s pointer analysis [2]. The tuple pt(p,q) indicates that the memory location p may point to the memory location q. When applied to the program of Figure 2b, it results in the heap graph shown in Figure 2c. The analysis is flow-insensitive, so that it combines the assignment k:=*a with the obsolete conclusion pt(a,b1) to erroneously conclude pt(k,c1) and pt(k,c2).

Figure 3: A portion of the derivation graph leading to each conclusion of the analysis. Each rectangle denotes a tuple, where input tuples are shaded in gray, and output tuples are unshaded. Unboxed nodes indicate rule instances, so for example R1(b1,c1) indicates the instance of the rule R1 with p = b1 and q = c1. The arrows indicate logical dependencies between these entities.

later to the memory location b2. The assignment k := *a can therefore only result in k pointing to c3. However, because the analysis is flow-insensitive, it disregards the order of program statements, and concludes that k may also point to c1 and c2.

The erroneous conclusions arise because the rule R3 is incomplete: even if all of the hypotheses, p := *q, pt(q,r), and pt(r,s), are true, it is possible for the conclusion pt(p,s) to be spurious. We call this situation a misfiring of the rule R3. Observe that since both pt(k,c1) and pt(k,c2) share the intermediate tuple pt(a,b1), they are correlated, in an informal sense, in their ground truth. Suppose the user examines the results of the analysis, and indicates that pt(k,c1) is false. Is it possible for us to generalize from this feedback, and automatically infer that pt(k,c2) is also likely to be false?

Note that it is difficult to characterize this correlation in a purely deductive manner: any of the rule instances leading to the faulty conclusion could have misfired, and ¬pt(k,c1) does not logically entail ¬pt(k,c2). However, on large programs, rules misfire in statistically regular ways. Therefore, our first idea is to associate each rule R with a probability pr of correctly firing; we postulate that each instance of R fires independently and with identical probability pr. We can now associate individual conclusions of the analysis with the probability of being true. For example, if we associate each rule of Andersen’s analysis with the probability pr = 0.9, and treat each input tuple as being known with certainty, then

\[
\Pr(\text{pt}(k,c2)) = \Pr(R3(k,a,b1,c2) \cap R1(b1,c2) \cap R1(a,b1)) = 0.9^3 = 0.729.
\]

The idea is that alarms with higher probability are more likely to be true than alarms with low probability,
and therefore guide the user towards the real bugs in their program. Observe that we have also automatically obtained a way to generalize from user feedback, i.e. by computing conditional probabilities:

\[
Pr( pt(k,c2) \mid \neg pt(k,c1)) = \frac{Pr( pt(k,c2) \cap \neg pt(k,c1))}{Pr(\neg pt(k,c1))} = 0.51 \ll Pr( pt(k,c2)).
\]  

Observe that the unrelated alarm \( pt(k,c3) \) is unaffected: \( Pr( pt(k,c3) \mid \neg pt(k,c1) = Pr( pt(k,c3)) = 0.729. \)

The key challenge behind formalizing this intuition is to succinctly describe how each output tuple came to be derived. We do this by adapting the concept of semiring provenance from databases [15, 8]. Briefly, we first fix a semiring \((K, +, \times, 0_K, 1_K)\), and each instance \( g \) of a rule with a token \( k_g \in K \). For our example of computing probabilities, \( k_g \) is the event that \( g \) has correctly fired, the semiring operations \(+\) and \( \times \) represent union and intersection respectively—\( k + k' = k \cup k' \) and \( k \times k' = k \cap k' \)—and \( 0_K = \emptyset \) and \( 1_K = \Omega \), the set of outcomes of the probability space. The provenance \( k_t \) of a tuple \( t \) is given by:

\[
k_t = \sum_{\tau \in \tau} \prod_{\tau \in \tau} k_g,
\]  

where \( \tau \) ranges over all derivation trees whose conclusion is \( t \), and \( g \in \tau \) ranges over all rule instances occurring in \( \tau \). The probability of a tuple \( t \) is now given by the probability of its associated event: \( Pr(t) = Pr(k_t) \). We have implemented this idea in recent work [33] to obtain an interactive program analysis system. The user repeatedly inspects the alarm with highest confidence, and the system incorporates their feedback and reranks the remaining alarms. We present an excerpt of our experimental results in Table 1.

On average, across two static analyses—a datarace analysis applied to Java programs, and a taint analysis applied to Android apps—and on a suite of 16 real-world benchmark programs, the user has to inspect 44.2% fewer alarms than the baseline to discover all bugs.

Unfortunately, each conclusion of a Datalog program may have many (possibly even infinitely many) derivation trees. Therefore, the main technical difficulty in instantiating our framework is the algorithmic complexity of Equation 3. The system we describe in Table 1 tackles this problem by only performing approximate marginal inference in a Bayesian network along with aggressive constraint pruning. Another approach is to change the underlying semiring, for example to the max-times semiring. As before, each rule \( R \) is associated with a truth value \( p_R \in [0, 1] \), and each instance \( g \) of \( R \) with the same token \( k_g = p_R \). The semiring operations are defined as \( k + k' = \max(k,k') \) and \( k \times k' = kk' \), \( 0_K = 0 \) and \( 1_K = 1 \). Equation 3 can now be efficiently evaluated using previously known algorithms such as seminaive evaluation. Furthermore, the partial derivatives, \( \partial k_t / \partial p_R \) can also be readily computed: we can now adapt popular numerical optimization techniques such as gradient descent and Newton’s method to the task of synthesizing rule weights, and even the analysis itself. In preliminary experiments that we present in Table 2, we show that this technique greatly outperforms the state-of-the-art in learning Datalog programs such as Andersen’s analysis and mod/ref analysis.

<table>
<thead>
<tr>
<th>Analysis</th>
<th>Rules</th>
<th>Program</th>
<th>Size</th>
<th>Alarms</th>
<th>Last True Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>LOC</td>
<td>Tuples</td>
<td>Clauses</td>
</tr>
<tr>
<td>Datarace</td>
<td>102</td>
<td>FTP Server</td>
<td>152K</td>
<td>2067K</td>
<td>2182K</td>
</tr>
<tr>
<td>Taint</td>
<td>62</td>
<td>AndroidTrail</td>
<td>81K</td>
<td>13K</td>
<td>72K</td>
</tr>
</tbody>
</table>

Table 1: Experimental performance of an interactive program analysis system based on DIFFLOG [33]. The column rules measures the number of analysis rules. The columns labelled last true rank indicates the number of alarms that the user needs to inspect before discovering all bugs in the program.
Table 2: Performance of DiffLog-based gradient descent in synthesizing program analyses, compared to two state-of-the-art combinatorial algorithms, ALPS [36], and Zaatar [1]. Each system was given 3 hours to synthesize the analysis.

<table>
<thead>
<tr>
<th>Program</th>
<th>Relations</th>
<th>Rules</th>
<th>Time (in seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Input</td>
<td>Output</td>
<td>Synthesized</td>
</tr>
<tr>
<td>Andersen</td>
<td>4</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Mod/ref</td>
<td>7</td>
<td>5</td>
<td>10</td>
</tr>
</tbody>
</table>

3 Challenges and Opportunities

Interpretability and scalability. The most important challenge in instantiating DiffLog is choosing a semiring so that: (a) the output values come with useful guarantees and are readily interpretable by programmers, and (b) Equation 3 can be evaluated efficiently on real-world codebases. One option we discussed was using the max-times semiring so that efficient Datalog evaluation algorithms can be adapted in a straightforward way. Connecting this to other well-studied problems such as min-cuts is an exciting direction of future research.

Learning. In Section 2, we discussed how the max-times semiring enables fast gradient-descent based learning. In the case of the probabilistic semiring, we may also use the expectation-maximization algorithm to learn rule firing probabilities. The most important problem involving learning is that of invented/hidden predicates. Furthermore, while we have assumed a corpus of labelled training data, human feedback is often inaccurate. Can our learning algorithms operate in unsupervised or weakly supervised settings? On the opposite side, can we build standard candles and large repositories of well-labelled programs?

Rethinking the analysis–user interface. We have discussed how we may associate alarms with the probability that they represent true bugs. Programmers are also interested in the severity and relevance of individual alarms. We are investigating the applicability of DiffLog to produce this information. Furthermore, instead of a passive model where the user chooses which alarm to inspect, there is great value in actively soliciting feedback from the user on alarms and intermediate conclusions of high value [10, 39]. We are investigating the problem of determining tuples whose ground truth would be most effective in reducing uncertainty in remaining alarms.

4 Related Work

There is a large body of research which applies statistical methods to syntactic features of the program to determine which alarms are likely to be true [19, 37, 21]. The z-ranking algorithm [23, 22] is one prominent example, which uses the z-test and ranks alarms according to code locality. By modelling the alarm generation process through Equation 3, our work can be seen as explaining why these techniques tend to work. Statistical methods have also been used to find cost-effective abstractions which are still sufficiently precise to prove the properties of interest [16, 31, 17, 7, 18], predict likely types [34, 20], and mine likely specifications and find anomalies [30, 26, 24]. Human-in-the-loop program analysis systems have largely been based on non-statistical optimization techniques, such as abduction [10], integer linear programming [39], and MaxSMT [28]. They are also often formulated to pinpoint the root cause of errors in the analysis [39, 32], which we encode probabilistically in DiffLog. Finally, Bielik et al [5] consider the problem of automatically learning a static analyzer from data, but focus on a restricted class of analyses which can be expressed using decision trees over program syntax, as opposed to the deeper properties which we can model using fixpoints.
References


