Learning a Static Bug Finder from Data

YU WANG, Nanjing University
FENGJUAN GAO, Nanjing University
LINZHANG WANG, Nanjing University
KE WANG∗, Visa Research

Static analysis is an effective technique to catch bugs early when they are easy to fix. Recent advances in program reasoning theory have led to increasing adoption of static analyzers in software engineering practice. Despite the significant progress, there is still potential for improvement. In this paper, we present an alternative approach to create static bug finders. Instead of relying on human expertise, we leverage deep neural networks—which have achieved groundbreaking results in a number of problem domains—to train a static analyzer directly from data. In particular, we frame the problem of bug finding as a classification task and train a classifier to differentiate the buggy from non-buggy programs using Gated Graph Neural Network (GGNN). In addition, we propose a novel interval-based propagation mechanism that significantly improves the generalization of GGNN on larger graphs. We have realized our approach into a framework, NeurSA, and extensively evaluated it. In a cross-project prediction task, three neural bug detectors we instantiate from NeurSA are highly precise in catching null pointer dereference, array index out of bound and class cast bugs in unseen code. A close comparison with Facebook Infer in catching null pointer dereference bugs reveals NeurSA to be far more precise in catching the real bugs and suppressing the spurious warnings. We are in active discussion with Visa Inc for possible adoption of NeurSA in their software development cycle. Due to the effectiveness and generality, we expect NeurSA to be helpful in improving the quality of their code base.

CCS Concepts: Software and its engineering → Software notations and tools; General programming languages;

Additional Key Words and Phrases: Static Analysis, Bug Detection, Deep Neural Network

ACM Reference format:
Yu Wang, Fengjuan Gao, Linzhang Wang, and Ke Wang. 2018. Learning a Static Bug Finder from Data. Proc. ACM Program. Lang. 1, CONF, Article 1 (January 2018), 27 pages.
DOI:

1 INTRODUCTION

Static analysis is an important method for finding software defects. It is performed early in the development cycle to catch bugs as quickly as they appear, paving the way for easy fixes. Unlike dynamic analysis, static analysis reasons about every paths in the program, offering formal guarantees on the program’s properties. As an evidence of the increasing maturity and popularity in software engineering practices, many static analyzers have been successfully adopted by major tech companies for improving the quality of their code base (e.g. Microsoft’s SLAM (Ball and Rajamani 2002), Google’s Error Prone (Aftandilian et al. 2012), Facebook’s Infer (Calcagno et al. 2015), Coverity (Bess ey et al. 2010) and Astrée (Blanchet et al. 2003)).

Authors’ addresses: Yu Wang and Fengjuan Gao, Nanjing University, China, {yuwang_cs, figao}@smail.nju.edu.cn; Linzhang Wang, Nanjing University, China, lzwang@nju.edu.cn; Ke Wang, Visa Research, U.S.A, kewang@visa.com.
∗Work done before joining Visa Research.

2018. XXXX-XXXX/2018/1-ART1 $15.00
DOI:
Despite the significant progress, static analyzers suffer from several well-known issues. One, in particular, is the high false positive rate which tends to overshadow the true positives and hurts usability. The reason of this phenomenon is when programs grow larger, static analyzers choose to over approximate the program semantics to alleviate the scalability challenges, which inevitably introduces imprecision (e.g. errors flagged by static analyzers do not occur in reality). On the other hand, problems of false negatives also need to be dealt with. Recently, Habib and Pradel (2018) investigated how effective the state-of-the-art static analyzers are in handling a set of real-world bugs. Habib et al. show more than 90% of the bugs are missed, exposing the severity of false negatives issues.

To tackle the aforementioned weaknesses, in this paper, we explore an alternative approach to create static bug checkers—neural bug detection. The idea is to leverage the power of deep neural networks, which have seen huge success in a variety of problem domains, to train a bug detector directly from data. In particular, we frame the problem of bug finding as a classification task. Namely given a code sample, we predict the presence/absence of a bug. Compared to the classic static analyzers which are manually designed and often require significant fine tuning, our approach removes humans out of the loop, therefore substantially reducing the cost of design. However, to show the plausibility of our approach, we face two important challenges: first how to obtain a large amount of training data which consist of both buggy and non-buggy code snippets; second, how to design a deep learning model that is both accurate and scalable in classifying buggy code. To address the first challenge, we mine code snippets across multiple project corpus to solve the data scarcity problem. In the meanwhile, we hypothesize the cross-project variations would not seriously impact the model precision since bugs of same kind exhibit similar characteristics. To create a balanced data set, we run the state-of-the-art clone detector, DECKARD (Jiang et al. 2007), to pick a non-buggy code example that is syntactically closest to each buggy example we collect. As for the second challenge, we utilize the Gated Graph Neural Network (GGNN) (Li et al. 2015) to learn the semantic patterns of buggy code. Specifically, we use control-flow graph as the program representation. To aid bug detection at the level of lines, we further split each node corresponding to a basic block into a multitude of nodes, each of which represents a single statement. Unfortunately, breaking nodes of basic blocks increases the size of the graph. As a result, information propagation becomes more difficult and especially challenging among nodes that are far apart on a graph, ultimately hindering GGNN’s generalization. To address this scalability issue, we propose a novel propagation mechanism to scale the training of GGNN to large graphs while incurring little to non precision loss. Our insight is using intervals to define how information is propagated on a graph. Specifically, we only allow nodes to communicate with their peers within the same interval to reduce the communication burden. By converting an interval at a lower order graph into a single node on a higher order graph, propagation is transitioned from local to global in an implicit and seamless manner. To recover the embeddings of nodes on the original graph, we move from the high-order graph back to the low-order graph, allowing the local propagation to be restored. This bi-directional transition facilitates the information to be propagated efficiently and thoroughly across the entire graph, ultimately helping GGNN to converge.

We realize our approach into a general, extensible framework, called NEURSA, that performs intra-procedural analysis for different kinds of semantic bugs. The framework first automatically scrapes training data across multiple project corpus, creating a perfectly balanced set of buggy and non-buggy methods; then trains a model to predict the location of a bug; and finally uses the trained model for detecting bugs in previously unseen code. We present three neural bug detectors based on NEURSA that find null pointer dereference, array index out of bound and class cast exceptions. Figure 1 depicts three example bugs (one for each kind) that are caught by our neural bug detectors.
Learning a Static Bug Finder from Data

Extending NEURSA to support a new bug detector only requires a training data generator that extracts buggy code examples from a given code corpus, since the rest of will be automatically performed by NEURSA.

Our approach significantly differs from almost all related work in the literature (Allamanis et al. 2017; Pradel and Sen 2018; Wang et al. 2016). Specifically, we consider deep and semantic bugs that

Proc. ACM Program. Lang., Vol. 1, No. CONF, Article 1. Publication date: January 2018.
are proven to be hard even for state-of-the-art static analyzers instead of shallow and syntactic bugs targeted by other works (Allamanis et al. 2017; Pradel and Sen 2018; Wang et al. 2016). In addition, our neural bug detectors are trained exclusively on the real world programs, which help them to be effective against complicated bugs in unseen code. Finally NeurSA pinpoints a bug in a program to a line instead of predicting an entire file to be buggy or not (Wang et al. 2016).

We evaluate NeurSA and its three instantiations by learning from six Java project corpus containing 28,344 files and searching bugs in another 13 projects of 26,975 files. In total our corpus amounts to 5,642,821 lines. We find that our neural bug detectors are effective in predicting the semantic bugs. In particular, when predicting at the level of methods, the three models yield on average 38.9% precision, 79.6% recall and 52.2% F1 score, even at the level of lines, three models still achieve 73.3% recall. We also find out the neural bug detectors perform equally well in the within- and cross-project prediction. This finding confirms our hypothesis that bugs of the same kind display similar characteristics even if they are created by different developers. To further demonstrate the utility of NeurSA, we compare our neural bug detector with Facebook’s Infer (Calcagno et al. 2015) in catching null pointer dereference bugs\footnote{The only kind of bugs that are handled by both NeurSA and Infer.}, arguably the state-of-the-art static analyzer for Java programs, results show our neural bug detector catches far more bugs (i.e. low false negative) and produces far less spurious warnings (i.e. low false positive).

We make the following contributions:

- We propose a deep neural network based methodology for building static bug checkers. Specifically, we utilize GGNN as the underlying deep neural network to train a classifier for differentiating the buggy code from non-buggy code.
- We propose a novel interval-based propagation model to address the scalability issues GGNN encountered when training on large graphs.
- We design a framework to streamline the learning of a neural bug detector including the automatic data preparation and model training.
- We realize our framework that can be instantiated into different kinds of semantic bugs. The framework is open-sourced at https://github.com/anonymoustool/NeurSA.
- We publish our data set at https://figshare.com/articles/datasets_tar_gz/8796677 for the three neural bug detectors we built based on NeurSA to aid the future research activity.
- We present the evaluation results to show our neural bug detectors are highly precise in detecting the semantic bugs in real-world programs and significantly outperform Facebook Infer, arguably the state-of-the-art static analyzers for Java programs, in catching null pointer dereference bugs.

2 PRELIMINARY

First, we revisit the definition of connected, directed graph. Then we give a brief overview of two previous techniques (Allen 1970; Li et al. 2015), which our work builds on.

2.1 Graph

A graph $G = (V, E)$ consists of a set of nodes $V = \{v_1, ..., v_m\}$, and a list of directed edge sets $E = (E_1, ..., E_K)$ where $K$ is the total number of edge types and $E_k$ is a set of edges with type $k$. $E(v_s, v_d, k), k \in (1, ..., K)$ denotes an edge of type $k$ directed from node $v_s$ to node $v_d$. For graphs with only one edge type, $E$ is represented as $(v_s, v_d)$.

The immediate successors of a node $v_i$ (denoted as imme\_succ($v_i$)) are all of the nodes $v_j$ for which $(v_i, v_j)$ is an edge in $E$. The immediate predecessors of node $v_j$ (denoted as imme\_pred($v_j$)) are all of the nodes $v_i$ for which $(v_i, v_j)$ is an edge in $E$. 
Algorithm 1: Finding intervals

**Input:** Graph \( G \), Node set ‘\( V \)’
**Output:** Interval set \( S \)

1. // \( v_0 \) is the unique entry node for the graph
2. \( H = \{ v_0 \} \);
3. while \( H \neq \emptyset \) do
   4. // remove next \( h \) from \( H \)
   5. \( h = H.\text{pop()} \);
   6. \( I(h) = \{ h \} \);
   7. // only nodes that are neither in the current interval nor any other interval will be considered
   8. while \( \{ v \in V \mid \exists s \in S \land v \in s \land \text{imme\_pred}(v) \subseteq I(h) \} \neq \emptyset \) do
      9. \( I(h) += \{ v \} \);
   10. // find next headers
   11. while \( \{ v \in V \mid \exists s_1 (s_1 \in S \land v \in s_1) \land \exists s_2 \exists m (s_2 \in S \land m \in \text{imme\_pred}(v) \land m \in s_2) \} \neq \emptyset \) do
      12. \( H += \{ v \} \);
   13. \( S += I(h) \);

A path is an ordered sequence of nodes \((v_j, ..., v_k)\) and their connecting edges, in which each \( v_i, i \in (j, ..., k - 1) \) is an immediate predecessor of \( v_{i+1} \). A closed path is a path in which the first and last nodes are the same. The successors of a node \( v_i \) (denoted as \( \text{succ}(v_i) \)) are all of the nodes \( v_j \) for which there exists a path from \( v_i \) to \( v_j \). The predecessors of a node \( v_j \) (denoted as \( \text{pred}(v_j) \)) are all of the nodes \( v_i \) for which there exists a path from \((v_i, ..., v_j)\).

### 2.2 Interval

As described by Allen (1970), an interval \( I(h) \) is the maximal, single entry subgraph in which \( h \) is the only entry node and all closed paths contain \( h \). The unique interval node \( h \) is called the interval head or simply the header node. An interval can be expressed in terms of the nodes in it: \( I(h) = (v_1, v_2, ..., v_m) \).

By selecting the proper set of header nodes, a graph can be partitioned into a unique set of disjoint intervals. An algorithm for such a partition is shown in Algorithm 1. The key is to add into an interval a node only if all of whose immediate predecessors are already in the interval (Line 8 to 9). The intuition is such nodes when added to an interval keep the original header node as the single entry of an interval. To find a header node to establish another interval, we pick a node that is not member of any existing intervals although it must have an (not all) immediate predecessor being member of an interval (Line 11 to 12). We repeat the computation until reaching the fixed-point where all nodes are members of an interval.

The intervals on the original control flow graph are called the first order intervals denoted by \( I^1(h) \), and the graph from which they were derived is called first order graph (also called the set of first order intervals) \( S^1 \) s.t. \( I^1(h) \in S^1 \). By making each first order interval into a node and each interval exit edge into an edge, the second order graph can be derived, from which the second order intervals can also be defined. The procedure can be repeated to derive successively higher order graphs until the n-th order graph consists of a single node\(^2\). Figure 2 illustrates such a sequence of derived graphs.

---

\(^2\)Certain graphs may not be reduced to a single node. Examples are provided in the supplemental material.
Fig. 2. n-th order intervals and graphs.

2.3 Gated Graph Neural Network

We review graph neural networks (GNN) (Gori et al. 2005; Scarselli et al. 2008), which lays the groundwork for GGNN.

We extend the definition of a graph to include $M$ (i.e. $G = (V, E, M)$). $M$ is a set of vectors (or embeddings) $\{\mu_v, ..., \mu_{v_n}\}$, where each $\mu_v \in \mathbb{R}^d$ denotes the embedding of a node $v$ in the graph. GNN updates node embeddings via a propagation model:

$$
\mu_v^{(l+1)} = h(\{\mu_u^{(l)}\}_{u \in N^k(v), k \in \{1, 2, ..., K\}})
$$

Specifically, the new embedding of $v$ is computed by aggregating the current vectors of its neighbouring nodes. $N^k(v)$ is the neighbouring nodes that are connected to $v$ with edge type $k$, i.e., $N^k(v) = \{u|(u, v, k) \in E\} \cup \{u|(v, u, k) \in E\}$. We repeat the propagation for $L$ steps to update $\mu_v$ to $\mu_v^{(L)}$, $\forall v \in V$.

Most GNNs compute a separate node embedding w.r.t. an edge type before merging them into a final embedding. For example (Si et al. 2018),

$$
\mu_v^{(l+1),k} = \sigma_1(\sum_{u \in N^k(v)} W_{2}\mu_u^{(l)}), \forall k \in \{1, 2, ..., K\}
$$

$$
\mu_v^{(l+1)} = \sigma_2(W_3[\mu_v^{(l),1}, \mu_v^{(l),2}, ..., \mu_v^{(l),K}])
$$

$$
\mu_v^{(0)} = W_1\mu_v
$$
Equation 4 denotes the base case where \( l \) is 0, and \( \mu_v \) is the initial embedding vector. The three matrices \( W_1, W_2 \) and \( W_3 \) are variables to be learned, and \( \sigma_1 \) and \( \sigma_2 \) are some nonlinear activation functions.

To further improve the model capacity, Li et al. (2015) proposed Gated Graph Neural Network (GGNN). The major difference Li et al. introduced is Gated Recurrent Units (Cho et al. 2014) as an instantiation of \( h \) in Equation 1. The following equations describe how GGNN works:

\[
\tilde{m}_v^l = \sum_{u \in N(v)} f(\mu_u^l)
\]

\[
\mu_v^{(l+1)} = \text{GRU}(\tilde{m}_v^l, \mu_v^l)
\]

To update the embedding of node \( v \), Equation 5 computes a message \( \tilde{m}_v^l \) using \( f(\cdot) \) (e.g., a linear function) from the embeddings of its neighboring nodes \( N(v) \). Next a GRU takes \( \tilde{m}_v^l \) and \( \mu_v^l \) the current embedding of node \( v \) to compute \( \mu_v^{(l+1)} \) the new embedding.

Similarly, the propagation will be repeated for a fixed number of time steps. In the end, we use the embeddings from the last time step as the final node representations.

3 FRAMEWORK

This section presents NEURSA, a framework for learning neural bug detectors. In particular, we address two challenges: how to obtain sufficient training data and how to train a model that can precisely detect the presence of a bug.

3.1 Overview of NEURSA

Figure 3 depicts the overview of NEURSA. We split NEURSA’s workflow into four parts and describe each one below.

1) Data Collection: We extract methods from the code bases of real world projects. To obtain the label for a bug (i.e., type of the bug), we cross-reference the bug reports and commit history of the same project. For example, given a commit in the format “Fixing Bugzilla#2206…”, we search the record that contains the bug id in the bug reports to determine the type of the bug. Subsequently, we label the method and the lines that are changed as buggy. Whenever a buggy method is added to the dataset, we run DECKARD (Jiang et al. 2007), the state-of-the-art clone detector, to pick a correct method from any code base.
that is syntactically closest to the buggy method. In addition, we regard lines that are not modified in a buggy method to be correct lines.

(2) **Method Representation:** We construct the control flow graph for each method. To facilitate NEURSA to pinpoint a bug in a method, we break each node denoting a basic block into a number of nodes each of which represents a non control statement.

(3) **Training Neural Bug Detectors using GGNN:** We train a neural bug detector using GGNN. In particular, we propose a novel interval-based propagation mechanism to address the generalization issues of GGNN on large graphs. The idea is to only perform propagation among nodes within the same interval. By moving from a lower order interval graph to a higher order interval graph, we implicitly expand the propagation to include more nodes in a graph, and therefore moving the propagation gradually towards the global level. To recover the embeddings of each node in the first order graph, we split an interval of higher order graph back to a multitude of nodes in the lower order graph until arriving at the original control flow graph. The process will be repeated until the model converges. Our intuition is to divide the propagation into two modes: local and global, between which a transition is realized to find the sweet spot.

(4) **Bug Detection:** Given a neural bug detector we trained in the previous step, we use it to detect bugs in unseen code. We provide two detection modes: method and line. The former predicts if a method is buggy and the latter pinpoints where the bug is in a buggy method.

### 3.2 Data Generation

We extract methods from real world project corpus. To collect a buggy method, we look for code commits that contain bug fixes. For instance, if a commit adds `NULL` checks in `foo1`, `foo2` and `foo3` to fix null pointer dereference bugs, then all three methods are considered to be buggy. We acknowledge the location of a bug and its fix may not be precisely the same thing. However, given the programs we target in this paper, which come from high quality and well maintained code bases, it is reasonable to ignore the noise. Choosing non-buggy methods is also an important step. To create a balanced dataset, we run the state-of-the-art clone detector, DECKARD (Jiang et al. 2007), to pick a non-buggy method that is syntactically closest to each buggy method we collect. To identify the buggy lines in a buggy method, we pick those that are modified for a bug fix. Apparently, the rest of the lines in the buggy method are considered to be non buggy.

### 3.3 Method Representation

We represent each method using its control flow graph. To increase the precision of the representation, we split a graph node representing a basic block into a number of nodes, each of which represents a single statement. This variant of control flow graph also simplifies the bug prediction at the level of lines.

In general, we initialize a node based on the Abstract Syntax Tree (AST) or token sequence of the statement it denotes. To enhance the expressiveness of the programs features, we also incorporate variable type information. Given a variable `var`, we consider not only its actual type `τ(var)` but also all the supertypes of `τ(var)`, denoted by `τ*(var)` s.t. `τ*(var) = \bigcup_{i=1}^{n} τ_i(var)`, where `τ_i(var) = \{τ | \exists τ_ω ∈ τ_{i-1}(var) : τ_ω implements τ \}` with a base case `τ_1(var) = \{τ | τ(var) implements type τ \}`. Based on the above-mentioned information, we present three choices for node initialization:

**Characteristic Vectors.** Given a statement denoted by a node in the graph, we first extract its Abstract Syntax Tree (AST). According to the definition of characteristic vectors (Jiang et al. 2007), we then count the number of occurrences for each type of the AST node (e.g. for loop structure, if-else statement, assignment statement) and aggregate them into a vector in any pre-defined order.

Proc. ACM Program. Lang., Vol. 1, No. CONF, Article 1. Publication date: January 2018.
Finally we use the vector as an initial representation of the node. To keep the number of dimensions manageable, we consider all the variable types to be identical.

**RNN-Based Encoding.** As an alternative, we rely on Recurrent Neural Networks (RNNs) to initialize a node. In particular, we treat a statement as a sequence of tokens. After each token is embedded into a numerical vector (similar to word embeddings (Mikolov et al. 2013)), we feed the entire token sequence into a RNN and extract its final hidden state for node initialization. Note that we take some special measures to increase the precision of our encoding. First, whenever a token of a variable type occurs in the sequence, we automatically inject all of its supertypes into the token sequence before the actual type. Second, all variable tokens will receive the same embedding before being sent to the RNN as the inputs. In other words, we represent a variable primarily with its type information.

**Transformer-Based Encoding.** We also utilize Transformer (Vaswani et al. 2017), arguably the state-of-the-art deep model in neural machine translation, to initialize a node. Similar to the RNN-based encoding, we use token sequence to represent a statement. However, instead of using RNN to process the sequence, we compute an attention weight for each token w.r.t. the other tokens in the sequence. In the end we compute the weighted sum of all tokens as the initialization vector. Similar to the RNN-Based encoding, we also take into account the type information to represent a variable.

### 3.4 Training Neural Bug Detectors

![Diagram](image.png)

(a) Transition from low-order to high-order graph.  
(b) Transition from high-order to low-order graph.

**Fig. 4.** Example of interval graph propagation.

Given the method representations we derived, training a classifier with GGNN is a straight-forward task. However, we notice as the size of a graph increases, GGNN drops its accuracy, indicating its inadequacy in addressing the scalability challenge. Fundamentally, the cause of decrease in GGNN’s accuracy lies in its propagation model. Specifically when a graph has large diameter, information has to be propagated over long distance, therefore, message exchange between nodes that are far apart in a graph becomes difficult. To overcome the scalability issues, we propose a novel interval-based propagation model that scales the generalization of GGNN to large graphs.

Proc. ACM Program. Lang., Vol. 1, No. CONF, Article 1. Publication date: January 2018.
insight is to use intervals to regulate how information is propagated on a graph. In particular, nodes are only allowed to communicate with their peers within the same interval. By transitioning the propagation on lower-order graphs to higher-order graphs (and vice versa), we enable a sufficient message exchange among all nodes in a graph. Below we use the graph in Figure 2 to describe in details how the propagation works.

Starting with first order graph \( S^1 \) (i.e. initial control flow graph), since nodes are only allowed to exchange with their peers within the same interval, propagation will only take place in \( I^1(3) \) (node 3, 4, 5 and 6) and \( I^1(7) \) (node 7 and 8). The message exchange is conducted the same way as before (i.e. Equation 5 and 6). After repeating the propagation for a few steps, we move the propagation to the second order graph \( S^2 \). Since we create two new nodes (i.e. node 9 and 10) on \( S^2 \) denoting \( I^1(3) \) and \( I^1(7) \) on \( S^1 \), we sum the embeddings of nodes within \( I^1(3) \) and \( I^1(7) \) to be the initial representation for node 9 and 10 on \( S^2 \). The following equation defines the initialization for nodes that are created when transitioning to higher-order graphs.

\[
\mu^{(l)}_{I^{i+1}(h)} = \sum_{\nu \in I^{i+1}(h)} \mu^{(l)}_{I^{i+1}(h)}
\]

Similar to the propagation on \( S^1 \), propagation on \( S^2 \) takes place in \( I^2(2) \) (node 2, 9 and 10) while node 1 is still isolated. Note that as propagation occurs within \( I^2(2) \) on \( S^2 \), all nodes except node 1 on \( S^1 \) are communicating, with node 9 and 10 (on \( S^2 \)) being the proxy of node 3-6 and node 7 and 8 (on \( S^1 \)) respectively. This is where our new propagation model is advantageous over the existing one. As the propagation moves towards the global mode, the amount of data traffic is still manageable because many nodes only communicate through their proxies without being present in the graph to overload the propagation. When arriving at \( S^3 \), we enable the propagation among all nodes in the graph directly or indirectly. Figure 4a illustrates the process.

Now to recover the node embeddings on \( S^1 \), we move the propagation back from \( S^3 \) to \( S^1 \) (Figure 4b). The idea is to reemphasize local propagation among nodes within an interval after their exposure to the global view of the graph. To initialize nodes within an interval on a lower order graph that are split from a single node on a higher order graph, we perform the following:

\[
\forall m \in I^{i+1}(h), I^i(m) = \frac{\mu^{(l)}_{I^{i+1}(h)}}{|I^{i+1}(h)|}
\]

The process of transitioning between lower order graph and higher order graph is repeated until the model converges.

There are also many alternative designs (Hamilton et al. 2017; Kipf and Welling 2016; Liao et al. 2018) relying on graph partitioning to scale graph neural networks. Compared with those works, our interval based propagation enjoys several conceptual advantages. First, since partition problems in graph theory are typically NP-hard, those works look for heuristic to approximate in practice. Second, given the graph partitions, they need to manually design how to alternate between the two propagation modes (i.e. local and global). In contrast, by transitioning from lower order graph to higher order graph (and vice versa), our propagation model mixed the two modes naturally and seamlessly. Third, our propagation model makes use of the special constructs in programs, which none of the related works considered. Specifically, intervals can be regarded as a representation of loop constructs, especially those that consist of many nodes, therefore by attending to a loop construct in a propagation model, GGNN can extract deeper and more precise semantic program features that other works can not.

By repeating the interval-based propagation model for \( L \) steps, we sum the final embeddings of all nodes in the graph to represent a method.
3.5 Bug Detection

Given the embedding vector of a method, we use a Feed Forward Neural Network (FFNN) (Svozil et al. 1997) to predict if the method is buggy. When a method is predicted to be buggy, we continue to predict the lines on which a bug resides. Given a node embedding \( \mu^L_i \), which represents a single line in the method, we use another FFNN to predict if a line is buggy.

4 METHODOLOGY

This section presents three neural bug detectors we created based on NEURSA framework. The bug detectors address a diverse set of programming mistakes: null pointer dereference bugs, array index out of bound bugs, and class casting bugs.

4.1 Null Pointer Exception

The first neural bug detector addresses null pointer exception (NPE for short), which is caused by dereferencing null pointer. The main challenge for static analyzers to catch them is to precisely analyze the points-to relations, which also can scale to large programs (Shi et al. 2018). We made the following adjustments to our graph encoding to deal with the null pointer dereference bugs.

First, given a method call, we explicitly inject its return type and the types of its arguments. Second, we add an entry of NULL to the vocabulary. Finally, we perform value flow analysis (Shi et al. 2018; Sui et al. 2012) to extract the data dependency among variables, in particular, we introduce a unique type of edge, which describes the value flow for pointers exclusively. Since the backbone of our graph is a variant of control flow graph, all the dependency edges are added between statement nodes (containing the dependent variables) rather than the variable itself.

4.2 Array Index Out of Bound Exception

Array index out of bound exception (AIOE for short) occurs when the index of an array falls out of the range \([0, n-1]\) (\(n\) is the length of the array). The main challenge of statically analyzing this bug is to precisely determine the array bound and the index value at compile time (Gao et al. 2016a,b). To address this challenge, we attempted the following.

Given an array declaration, we inject the type and the length of the array into our graph encoding. Whenever an array is accessed, we also add the type of the index variable to the mix. Finally we connect the value flow edges between statements that contain array declarations and array access operations.

4.3 Class Cast Exception

Class cast exception (CCE for short) is thrown when the object is cast to a subclass of which it is not an instance. The challenge lies in analyzing the type of a variable, determining whether there is an inherent relation between the variable that is being cast and the target type the variable is cast to. To deal with the challenge, we take the following actions.

Given a cast operation, we explicitly encode the type of the variable to be cast, providing an opportunity for GGNN to check the compatibility between its actual type and target type to be cast to. In addition, we also add the value flow edges connecting the cast operation to all statements that contain other variables the variable depends on.

5 IMPLEMENTATION

The code extraction, construction of control flow graph and intervals are implemented based on Spoon (Pawlak et al. 2015), which is an open-source library for Java source code transformation and analysis.
All neural bug detectors are implemented in Tensorflow. All RNNs built in the model have 1 recurrent layer with 100 hidden units. We adopt random initialization for weight initialization. Each token in the vocabulary is embedded into a 100-dimensional vector. We train the neural bug detectors using the Adam optimizer (Kingma and Ba 2014). All experiments are performed on a 3.7GHz i7-8700K machine with 32GB RAM and NVIDIA GTX 1080 GPU.

6 EVALUATION
This section presents our extensive evaluations of the three neural bug detectors we instantiate from NEURSA. We also compare our interval-based propagation model to the existing propagation mechanism. Finally, we show how our neural bug detector fares against Facebook Infer in catching null pointer dereference bugs.

6.1 Metrics
Since we deal with largely unbalanced testing set (i.e. the amount of correct code is significantly larger than that of the buggy code), we use three metrics—Precision, Recall, and F1—which are also widely adopted in defect prediction techniques (Wang et al. 2016). The metrics are computed by the following formulas:

$$
\text{Precision} = \frac{TP}{TP + FP}
$$

(9)

$$
\text{Recall} = \frac{TP}{TP + FN}
$$

(10)

$$
F1 = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}
$$

(11)

TP, FP, FN, TN denote true positive, false positive, false negative and true negative respectively. True positive is the number of predicted defective methods that are truly defective, while false positive is the number of predicted defective methods that are not defective. False negative records the number of defective methods that are predicted as non-defective. A higher precision suggests relatively low number of false alarms while high recall indicates relatively low number of missed bugs. F1 takes both precision and recall into consideration.

$$
\text{Top-N Recall} = \frac{TP_N}{TP_N + FN_N}
$$

(12)

We introduce another metric, top-N recall, dedicated to the prediction at the level of lines. Top-N refers to considering the top N lines to be buggy ranked by the predicted probabilities in a buggy method. Given the top-N predictions, we compute the recall as the only metric of line-level prediction. Our intuition is to favour predictions that capture all bugs in a method. Even it emits a high rate of false warnings, the issue should not be considered as serious since N is a small number. On the contrary, low recall would seriously hurts the usability of a bug finder. As a method is already predicted to be buggy, low recall provides little extra information for developer to pinpoint a bug.

6.2 Datasets
We made significant effort to collect real-world, publicly accessible datasets for our evaluation. In the end we use defect4j (Just et al. 2014), bugs.jar (Saha et al. 2018) and the other by Ye et al. (2014). We also contacted the authors of BugSwarm and MoreBugs who did not respond to our request. As mentioned previously, we obtain the labels for each buggy method and their lines by
Table 1. Projects used in the evaluation.

| Dataset | Projects | Description                                      | #Methods |
|---------|----------|--------------------------------------------------|----------|
|         |          |                                                  | NPE      | AIOE   | CCE   |
| Test    | Lang     | Java lang library                                | 115      | 46     | 75    |
|         | Closure  | A JavaScript checker and optimizer.              | 11       | 0      | 0     |
|         | Chart    | Java chart library                               | 120      | 5      | 0     |
|         | Mockito  | Mocking framework for unit tests                 | 49       | 6      | 42    |
|         | Math     | Mathematics and statistics components            | 44       | 59     | 14    |
|         | Accumulo | Key/value store                                  | 16       | 0      | 0     |
|         | Camel    | Enterprise integration framework                 | 155      | 20     | 6     |
|         | Flink    | System for data analytics in clusters            | 33       | 0      | 0     |
|         | Jackrabbit-oak | hierarchical content repository            | 68       | 7      | 12    |
|         | Log4j2   | Logging library for Java                         | 44       | 2      | 1     |
|         | Maven    | Project management and comprehension tool        | 12       | 0      | 0     |
|         | Wicket   | Web application framework                        | 23       | 8      | 16    |
|         |          | Total                                            | 690 (173) | 153 (38) | 166 (40) |
| Training| Birt     | Data visualizations platform                      | 1356     | 258    | 308   |
|         | JDT UI   | User interface for the Java IDE                  | 1794     | 126    | 312   |
|         | SWT      | Eclipse Platform project repository               | 552      | 272    | 52    |
|         | Platform UI | User interface and help components of Eclipse | 1840     | 144    | 388   |
|         | AspectJ  | An aspect-oriented programming extension          | 302      | 28     | 38    |
|         | Tomcat   | Web server and servlet container                 | 222      | 36     | 56    |
|         |          | Total                                            | 6066 (3033) | 864 (432) | 1154(577) |

cross-referencing the commit history and bug reports. Specifically, we search for commits that are considered to be bug fixes, and infer the type of the bug by referencing the bug reports. Methods and lines that are modified by commits of bug fixes are labeled buggy. Finally, we pick a correct method that is syntactically similar to pair with the buggy method.

Table 1 depicts the projects our datasets are composed of. We briefly describe the functionality of each project. The first column shows if a project is used in the training or test set. The last three columns are the number of total methods for each of the three bug types. Numbers in parenthesis are the number of buggy methods. For the actual number of bugs and buggy methods in each project, we invite readers to refer to the supplemental material for the details. Our evaluation focuses on the cross-project defect prediction, which resembles the real usage scenarios of NeURSA better than within-project defect prediction.

6.3 Baselines

We compare NeURSA against two other methodologies. The first one uses the traditional AST-based program encoding proposed in (Allamanis et al. 2017) while the second one uses a control flow graph-based program encoding. In both methodologies, we feed the program graphs to a standard GGNN built with the existing propagation model. Note the only difference between NeURSA and control flow graph-based program encoding is the propagation model GGNN is equipped with, which clarifies the contribution of our interval-based propagation mechanism.

To give more details, we re-implemented the graph encoding scheme proposed in (Allamanis et al. 2017), which uses AST as the backbone of the graph and additional edges to denote the variable type and data flow information. We also add the edges between the terminal nodes in AST. For convenience, we refer the first baseline as AST method and the second as CFG method.

Developers may fix multiple methods for a single bug so the number of buggy methods and bugs may not be identical.
6.4 Compare Node Initializations

We compare the three encoding schemes for node initialization: characteristic vectors, RNN-based encoding and transformer-based encoding. We show the performance of each encoding at both method-level and line-level predictions.

Table 2 presents the method-level prediction results of the three encoding schemes in precision, recall and F1. Figure 5a shows the average of all three metrics across all bug types for each encoding. We find that GGNN exhibits a decent performance in all node initialization schemes. In particular, RNN-based encoding has the highest recall and F1 score in all three bug types (i.e. on average higher than characteristic vectors and transformer-based encoding by 12.9% and 12.0% respectively), indicating it’s the most precise encoding scheme for node initialization.

As for the line-level predictions, we depict the average top-N recall across all bug types for each encoding scheme in Figure 5b. The characteristic vectors based encoding again falls behind whereas the RNN-based encoding shows a slight advantage over transformer-based encoding. The reason is that characteristic vectors do not capture as precise a representation of a statement as the other two. As for the transformer, we find their capabilities do not transfer to the programming field. We suspect this is caused by the fundamental difference between program language and natural language.

Based on the comparison among the three encoding schemes for node initialization, we choose the RNN-based encoding as NeURSA’s default configuration, in which we compare NeURSA against the two baselines in the remaining experiments.

6.5 Evaluate Method-Level Predictions

To evaluate the performance of method-level predictions, we build three sets of neural bug detectors based on NeURSA and the two baselines. Each set includes three models, each of which deals with null pointer dereference, array index out of bound and class casting bugs respectively.

Table 3 shows the precision, recall, and F1 for all models in the method-level prediction. The highest precision, recall and F1 for each bug type is highlighted in bold. In general, NeURSA is better than AST method and CFG method in most metrics, particularly, NeURSA is far more accurate in dealing with null pointer dereference and array index out of bound bugs (i.e. by more than 10% in F1 score). Furthermore, we find out NeURSA beats the two baselines by even bigger margin in
Table 2. Compare the different encoding for node initialization.

| Node Representations | NPE   | AIOE  | CCE   |
|----------------------|-------|-------|-------|
|                      | Precision | Recall | F1    | Precision | Recall | F1    | Precision | Recall | F1    |
| Characteristic vectors | 26.6  | 64.0  | 37.6  | 40.1     | 82.1   | 53.9  | 27.9     | 52.4   | 36.4  |
| RNN-based encoding   | 30.3  | 72.1  | 42.6  | 44.7     | 85.7   | 58.7  | 41.9     | 81.0   | 55.3  |
| Transformer-based encoding | 29.0  | 68.5  | 40.8  | 44.6     | 82.1   | 57.8  | 38.7     | 66.7   | 49.0  |

Table 3. Method-level prediction results.

| Methods | NPE   | AIOE  | CCE   |
|---------|-------|-------|-------|
|          | Precision | Recall | F1    | Precision | Recall | F1    | Precision | Recall | F1    |
| AST      | 24.0   | 52.3  | 32.3  | 34.8     | 57.1   | 43.2  | 38.3     | 71.4   | 49.8  |
| CFG      | 24.2   | 55.9  | 33.8  | 28.5     | 64.3   | 39.5  | 38.7     | 66.7   | 49.0  |
| NeurSA   | 30.3   | 72.1  | 42.6  | 44.7     | 85.7   | 58.7  | 41.9     | 81.0   | 55.3  |

Fig. 6. Average precision, recall and F1 for method-level prediction.

Fig. 7. F1 score of each methodology in top N% largest graphs.

F1 score on the top 10% largest graphs (i.e. 73.5% by NeurSA vs. 29.3% by CFG vs. 38.9% by AST), indicating the interval-based propagation model indeed improves the scalability of GGNN for generalizing on larger graphs. Figure 7 shows how the F1 score changes for each methodology across the graph size.

Figure 6 shows a bar graph charting the average performance across all bug types among the three methodologies. On average, NeurSA achieves 52.2% in F1 score, while the AST and CFG method achieve 42.0% and 40.8% respectively. In terms of the average recall, NeurSA achieves 79.6% while AST and CFG achieve 60.2% and 62.3% respectively. Our results demonstrate at the method-level prediction, NeurSA outperforms the baselines in both recall and F1 significantly.

6.6 Evaluate Line-level Prediction

To completely separate the line-level prediction with the method-level prediction, we train all neural bug detectors from buggy methods only. In other words, the job of line-level predictors is to locate the bugs in a known buggy method. Table 4 presents the top-N recall of the line-level
Table 4. Top-N recall for line-level prediction.

| Methods | Top-N | NPE | AIOE | CCE | Avg. |
|---------|-------|-----|------|-----|------|
| AST     | Top-1 | 37.8| 28.6 | 66.7| 44.4 |
|         | Top-3 | 55.0| 35.7 | 66.7| 52.5 |
|         | Top-5 | 64.0| 39.3 | 81.0| 61.4 |
|         | Top-7 | 72.1| 42.9 | 85.7| 66.9 |
|         | Top-10| 80.2| 64.3 | 95.2| 79.9 |
| CFG     | Top-1 | 47.7| 32.1 | 52.4| 44.1 |
|         | Top-3 | 55.9| 46.4 | 66.7| 56.3 |
|         | Top-5 | 61.3| 46.4 | 76.2| 61.3 |
|         | Top-7 | 67.6| 57.1 | 76.2| 67.0 |
|         | Top-10| 79.3| 64.3 | 95.2| 79.6 |
| NeurSA  | Top-1 | 44.1| 35.7 | 47.6| 42.5 |
|         | Top-3 | 57.7| 50.0 | 71.4| 59.7 |
|         | Top-5 | 67.6| 71.4 | 81.0| 73.3 |
|         | Top-7 | 73.0| 75.0 | 81.0| 76.3 |
|         | Top-10| 82.0| 75.0 | 95.2| 84.1 |

prediction results. We choose N to be 1, 3, 5, 7, and 10 for multiple prediction configurations. As before, we highlight the highest top-N recall for each methodology across all bug types. Overall, NeurSA outperforms the baselines in most metrics. Specifically, for array index out of bound bugs, NeurSA yields significantly better models than AST and CFG methods in each top-N configuration. However, the improvement NeurSA made over the baselines is not as significant as that in method-level prediction, especially in dealing with class cast bugs where AST method outperforms NeurSA in certain configurations. The last column shows average top-N recall performance among all three bug types. NeurSA achieves almost 60% in top-3 and more than 70% in top-5 recall, which is still notably better than the two other methodologies. Figure 8 depicts the top-3 recall across the graph size. Similar to the method-level prediction, NeurSA shows bigger improvement over the baselines on the top 10% largest graphs.

Through our extensive evaluations of NeurSA in both method- and line-level predictions, we conclude that NeurSA’s neural bug detectors are more precise in capturing the semantic buggy patterns than the two other methodologies. Compared to the CFG method, the superior performance NeurSA displays is entirely due to the interval-based propagation model, which demonstrates a better generalization of GGNN. As for AST methods, NeurSA uses a more semantic and principle graph representation to facilitate GGNN for learning deeper and more complicated semantic features.

### 6.7 Compare against Static Analysis Tools

This section compares NeurSA against traditional static analyzers. As a conceptual advantage, we re-emphasize that creating neural bug finders based on NeurSA does not require the substantial amount of human-expertise that is needed to build classical static analyzers. Sufficient amount of training data is all NeurSA needs. Besides, NeurSA also allows an easier extension to support new types of bugs compared to static analyzers.

To compare the actual performance between NeurSA and static analyzers in catching real world, complex and semantic bugs, we pick Facebook Infer (Calcagno et al. 2015), arguably the state-of-the-art static analyzer supporting Java program language. We compare NeurSA and Infer in...
catching null pointer dereference bugs, which happen to be the only type of bugs both NEURSA and Infer support.

We collected all null pointer dereference bugs in all of our testing projects. Since Infer was not able to compile all testing projects, we collected 58 null pointer dereference bugs from Lang, Math, Flink, Closure, WICKET and Mockito. On those projects, Infer reports 1008 null pointer dereference bugs in total. After manually verifying the reports according to the ground truth, we confirm that Infer detects only one of them. In comparison, NEURSA is able to detect 42 buggy methods with 138 warnings. With the top-3 prediction mode at the line-level, NEURSA achieves 71.4% recall, in other words, by scanning three lines in each buggy method, developers are able to precisely locate 30 out of the 58 bugs.

Worth noting we only validate Infer’s report according to the existing bugs, it is possible that Infer detects potentially unknown bugs. In other words, there might have been true bugs contained in the 1008 warnings reported by Infer. However, since NEURSA and Infer use the same ground truth, it is equally possible that other bugs reported by NEURSA may also be true positives.

Overall, we demonstrate the neural bug detector instantiated from NEURSA is significantly more precise than Infer in catching the null pointer dereference bugs.

7 DISCUSSION

This section discusses matters pertaining to the design of NEURSA and performances of the three neural bug detectors built on NEURSA.

7.1 Dealing with Noise

Recent studies (Kim et al. 2011) have discovered that the datasets used for training bug detectors can be noisy. We discuss two potential sources that could introduce noise in our datasets.

First, bugs types can be mislabeled (e.g. null pointer dereference can be labeled as an array index out of bound). As explained in Section 3.1, we determine the type of a bug by matching key words in the bug report. Even though the correctness can not be guaranteed, it is fair to disregard mislabeling as a serious issue. Because the nature of the three types of bugs we deal with is very different. Unless developer made a mistake in describing the bug in the report, the way we determine a bug type should be reliable.

Second, identifying a buggy method based upon the code patches is unsound. It is entirely possible for developers to commit quick hack around instead of fixes that address the root cause of the bug. However, since our datasets are well-studied in the literature (e.g. defects4j and bugs.jar), noise caused by imprecise fixes should be minimal. To confirm our hypothesis, we randomly pick 100 bugs in our datasets for manual inspection, and we find that all of them have not only the correct labels of bug types but also the correct locations in the method.

Finally, even though the noise is inevitable, the superior performance our neural bug detectors displayed over the baselines still counts. Because all models operate from the exact same dataset.

7.2 Data Sufficiency

In this experiment, we examine the sufficiency of our training data. Specifically, starting from 10% of the original training data, we gradually increase the percentage to investigate the performance trend for the three sets of neural bug detectors built by NEURSA and two other baselines. The testing data is kept intact for this experiment. Figure 9 shows how the F1 scores change as the percentage of the original training data increases. Figure 9a shows the three competing models in catching null pointer dereference bugs. Three models show similar convergence. That is when

---

4Some projects require build tools such as those provided by defects4j that Infer does not have access to.
reaching 80% all three models show little improvements onward. Even at 50%, their performances do not change by a big margin. Compared to the two baselines, the model built based on NeURSA requires less training data to converge. Overall, we conclude our data set is sufficient for training detectors of null pointer dereference bugs.

Figure 9b and 9c shows the performance trend of the other two classes of bug detectors. Compared to the null pointer dereference bug detectors, all array index out of bound bug detectors display a smoother convergence, indicating the lower complexity in learning the semantic patterns of array index out of bound bugs. Similarly, class casting bugs detectors also seem to require less amount of training data to generalize compared to the null pointer dereference bugs. According to our manual inspection, the reason is that the patterns of null pointer dereference bugs are significantly more diverse than those of the other two bug types. To some degree, it also explains null pointer dereference bugs are harder to prevent, which tend to occur more frequently than other types of bugs in software development. We list several examples of null pointer dereference bugs in Figure 10 we encountered in our dataset.

Overall, we demonstrate in this experiment, the training data for all three sets of bug detectors are sufficient. Bug detectors instantiated from NeURSA tend to converge early with higher precision.

7.3 Project Selection

We pick projects that are widely studied in the literature (Just et al. 2014; Saha et al. 2018; Ye et al. 2014). Even though they are considered to be general and representative to many software projects, NeURSA’s performance is not guaranteed to transfer to any other project.

7.4 Bug Selection

We have analyzed all kinds of Java runtime exceptions in our dataset, and show their distributions in Figure 11. We chose null pointer dereference, array index out of bound and class casting bugs to create neural bug detectors due to their high frequency. We did not use illegal argument exceptions despite having enough data. The reason is vast majority of the bugs can be caught by a simple type checker on the argument of the caller and the parameter of the callee. Other bugs like out of assertion error does not have enough data for building a bug detector by NeURSA despite its importance role in ensuring software quality.

8 RELATED WORK

Language Models for Programs. The recent success in machine learning has lead to a strong interest in applying machine learning techniques to learn program representations. Hindle et al. (2012) leverage an n-gram language model to show that source code is highly repetitive. other
Learning a Static Bug Finder from Data

(a) NPE caused by missing check.

(b) NPE caused by comparing two NULLs.

(c) NPE caused by splitting empty data of Byte class.

(d) NPE caused by insufficient check that misses the object.

(e) NPE caused by insufficient check that misses the return value of a method.

Fig. 10. Illustrative examples of a variety of the NPE bugs.
works (Alon et al. 2018, 2019; Bielik et al. 2016; Maddison and Tarlow 2014) model the code structure based on ASTs. Henkel et al. (2018) use abstractions of traces obtained from symbolic execution of a program as a representation for learning program embeddings. Wang et al. proposed another line of works in learning program semantics from executions (Wang 2019; Wang et al. 2017); of late they show combining symbolic and concrete executions could be an even more promising approach in learning precise and efficient program embeddings (Wang and Su 2019).

**Machine Learning for Defect Prediction.** Utilizing machine learning techniques for software defect prediction is another rapidly growing research field. So far the literature has been focusing on detecting simpler bugs of more syntactic nature. Wang et al. leverage deep belief network to learn program representations for defect prediction (Wang et al. 2016). Their model performs file-level defect prediction, in other words, predicts an entire file to be buggy or non-buggy. On the contrary, NEURSA pinpoints bugs in a method. Finally, Pradel and Sen (2018) present Deepbugs, a framework to detect name-based bugs. Compared to the bugs of swapped function arguments, wrong binary operator and wrong operand in binary operation DeepBugs target, NEURSA deals with semantic bugs that are far more complex and even challenging for latest static analyzers. As a more specialized effort, some prior works also attempted to detect vulnerabilities in programs. Choi et al. train a memory network model for predicting buffer overruns (Choi et al. 2017). Li et al. proposed a deep learning-based vulnerability detector VulDeePecker (Li et al. 2018). A drawback is their model relies on examples that are manually created. Instead, NEURSA only considers real-world programs and is equipped with the infrastructure to collect data automatically.

**Static Bug Finding.** Static analysis is a classical technique of find bugs without running programs. Recent works focus on the paradox - a highly precise analysis limits its scalability and an imprecise one seriously hurts its precision or recall. Pinpoint (Shi et al. 2018) and SMOKE (Fan et al. 2019) present two kinds of techniques to resolve the paradox. Shi et al. (2018) propose function-level summary to decompose the cost of high-precision points-to analysis by precisely discovering local data dependency. Then it leverages the function summary when conducting the expensive inter-procedural analysis. SMOKE adopts a staged approach to resolve the paradox. In the first stage, instead of using a uniform precise analysis for all paths, it uses a scalable but imprecise analysis. In the second stage, it leverages a more precise analysis to verify the feasibility of those candidates.

Facebook Infer (Berdine et al. 2006; Calcagno et al. 2015, 2009) is the static analyzer we used as the baseline in our comparison. It combines techniques like separation logic (Berdine et al. 2006;
Learning a Static Bug Finder from Data

2006) and bi-abduction (Calcagno et al. 2009). Separation logic is a kind of mathematical logic which facilitates reasoning about mutations to computer memory. It enables scalability by breaking reasoning into chunks corresponding to local operations on memory, and then composing the reasoning chunks together. Bi-abduction is a form of logical inference for separation logic which automates the key ideas about local reasoning.

9 CONCLUSION

Although static analysis in bug finding has been an active research area for decades, static analyzers still face important challenges (e.g. precision, scalability and user-friendliness) to be widely adopted in practice. In this paper, we present an alternative methodology of creating static bug finders. Specifically, we leverage the power of deep neural networks to train a model for classifying the buggy code from non-buggy code. In addition, we also propose an interval-based propagation model to improve the generalization of GGNN. We have realized our approach in a framework, NEURSA, which in principle can create any neural bug detector given a sufficient amount of training data. Three neural bug detectors we instantiate from NEURSA are highly effective in catching null pointer dereferencing, array index out of bound and class casting bugs. Compared to Facebook Infer, arguably the state-of-the-art static analyzer in catching null pointer dereference bugs, our neural bug detector displayed a far more superior performance. For future work, we will further evaluate the effectiveness of NEURSA after Visa Inc.’s adoption to their software development cycle. In addition, we will enhance NEURSA’s capability to support inter-procedural analysis for catching more complicated semantic bugs with high scalability.

REFERENCES

Edward Aftandilian, Raluca Sauciuc, Siddharth Priya, and Sundaresan Krishnan. 2012. Building Useful Program Analysis Tools Using an Extensible Java Compiler. In Proceedings of the 2012 IEEE 12th International Working Conference on Source Code Analysis and Manipulation (SCAM ’12). IEEE Computer Society, Washington, DC, USA, 14–23. https://doi.org/10.1109/SCAM.2012.28

Miltiadis Allamanis, Marc Brockschmidt, and Mahmoud Khademi. 2017. Learning to represent programs with graphs. arXiv preprint arXiv:1711.00740 (2017).

Frances E. Allen. 1970. Control Flow Analysis. In Proceedings of a Symposium on Compiler Optimization. ACM, New York, NY, USA, 1–19. https://doi.org/10.1145/800028.808479

Uri Alon, Meital Zilberstein, Omer Levy, and Eran Yahav. 2018. A General Path-based Representation for Predicting Program Properties. In Proceedings of the 39th ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI 2018). ACM, New York, NY, USA, 404–419. https://doi.org/10.1145/3192366.3192412

Uri Alon, Meital Zilberstein, Omer Levy, and Eran Yahav. 2019. Code2Vec: Learning Distributed Representations of Code. Proc. ACM Program. Lang. 3, POPL, Article 40 (Jan. 2019), 29 pages. https://doi.org/10.1145/3290353

Thomas Ball and Sriram K. Rajamani. 2002. The SLAM Project: Debugging System Software via Static Analysis. SIGPLAN Not. 37, 1 (Jan. 2002), 1–3. https://doi.org/10.1145/565816.503274

Josh Berdine, Cristiano Calcagno, and Peter W. O’Hearn. 2006. Smallfoot: Modular Automatic Assertion Checking with Separation Logic. In Proceedings of the 4th International Conference on Formal Methods for Components and Objects (FMCO’05). Springer-Verlag, Berlin, Heidelberg, 115–137. https://doi.org/10.1007/11804192_6

Al Bessey, Ken Block, Ben Chelf, Andy Chou, Bryan Fulton, Seth Hallem, Charles Henri-Gros, Asya Kamsky, Scott McPeak, and Dawson Engler. 2010. A Few Billion Lines of Code Later: Using Static Analysis to Find Bugs in the Real World. Commun. ACM 53, 2 (Feb. 2010), 66–75. https://doi.org/10.1145/1646535.1646574

Pavol Bielik, Veselin Raychev, and Martin Vechev. 2016. PHOG: Probabilistic Model for Code. In Proceedings of the 33rd International Conference on International Conference on Machine Learning - Volume 48 (ICML'16). JMLR.org, 2933–2942. http://dl.acm.org/citation.cfm?id=3045390.3045699

Bruno Blanchet, Patrick Cousot, Radhia Cousot, Jérôme Feret, Laurent Mauborgne, Antoine Miné, David Monniaux, and Xavier Rival. 2003. A Static Analyzer for Large Safety-critical Software. In Proceedings of the ACM SIGPLAN 2003 Conference on Programming Language Design and Implementation (PLDI ’03). ACM, New York, NY, USA, 196–207. https://doi.org/10.1145/781131.781153
Cristiano Calcagno, Dino Distefano, Jeremy Dubreil, Dominik Gabi, Pieter Hooimeijer, Martino Luca, Peter O’Hearn, Irene Papakonstantinou, Jim Purbrick, and Dulma Rodriguez. 2015. Moving Fast with Software Verification. In NASA Formal Methods, Klaus Havelund, Gerard Holzmann, and Rajeev Joshi (Eds.). Springer International Publishing, Cham, 3–11.

Cristiano Calcagno, Dino Distefano, Peter O’Hearn, and Hongseok Yang. 2009. Compositional Shape Analysis by Means of Bi-abduction. In Proceedings of the 36th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL ’09). ACM, New York, NY, USA, 289–300. https://doi.org/10.1145/1480881.1480917

Kyunghyun Cho, Bart Van Merriënboer, Dzmitry Bahdanau, and Yoshua Bengio. 2014. On the properties of neural machine translation: Encoder-decoder approaches. arXiv preprint arXiv:1409.1259 (2014).

Min-Je Choi, Sehun Jeong, Hakjoo Oh, and Jaegul Choo. 2017. End-to-end Prediction of Buffer Overruns from Raw Source Code via Neural Memory Networks. In Proceedings of the 26th International Joint Conference on Artificial Intelligence (IJCAI’17). AAAI Press, 1546–1553. http://dl.acm.org/citation.cfm?id=3172077.3172102

Gang Fan, Rongxin Wu, Qingkai Shi, Xiao Xiao, Jinguo Zhou, and Charles Zhang. 2019. Smoke: scalable path-sensitive memory leak detection for millions of lines of code. In Proceedings of the 41st International Conference on Software Engineering. IEEE Press, 72–82.

Fengjuan Gao, Tianjiao Chen, Yu Wang, Lingyun Situ, Linzhang Wang, and Xuandong Li. 2016a. Carrybound: static array bounds checking in C programs based on taint analysis. In Proceedings of the 8th Asia-Pacific Symposium on Internetware. ACM, 81–90.

Fengjuan Gao, Linzhang Wang, and Xuandong Li. 2016b. BovInspector: Automatic Inspection and Repair of Buffer Overflow Vulnerabilities. In Proceedings of the 31st IEEE/ACM International Conference on Automated Software Engineering (ASE 2016). ACM, New York, NY, USA, 786–791. https://doi.org/10.1145/2970276.2970282

Marco Gori, Gabriele Monfardini, and Franco Scarselli. 2005. A new model for learning in graph domains. In Proceedings. 2005 IEEE International Joint Conference on Neural Networks, 2005, Vol. 2. IEEE, 729–734.

Andrew Habib and Michael Pradel. 2018. How Many of All Bugs Do We Find? A Study of Static Bug Detectors. In Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering (ASE 2018). ACM, New York, NY, USA, 317–328. https://doi.org/10.1145/3238147.3238213

Will Hamilton, Zhitao Ying, and Jure Leskovec. 2017. Inductive representation learning on large graphs. In Advances in Neural Information Processing Systems. 1024–1034.

Jordan Henkel, Shuvendu K Lahiri, Ben Liblit, and Thomas Reps. 2018. Code vectors: understanding programs through embedded abstracted symbolic traces. In Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering. ACM, 163–174.

Afram Hindle, Earl T Barr, Zhendong Su, Mark Gabel, and Premkumar Devanbu. 2012. On the naturalness of software. In 2012 34th International Conference on Software Engineering (ICSE). IEEE, 837–847.

L. Jiang, G. Misherghi, Z. Su, and S. Glondu. 2007. DECKARD: Scalable and Accurate Tree-Based Detection of Code Clones. In 29th International Conference on Software Engineering (ICSE’07). 96–105. https://doi.org/10.1109/ICSE.2007.30

René Just, Darioush Jalali, and Michael D Ernst. 2014. Defects4J: A database of existing faults to enable controlled testing studies for Java programs. In Proceedings of the 2014 International Symposium on Software Testing and Analysis. ACM, 437–440.

Sunghun Kim, Hongyu Zhang, Rongxin Wu, and Liang Gong. 2011. Dealing with Noise in Defect Prediction. In Proceedings of the 33rd International Conference on Software Engineering (ICSE ’11). ACM, New York, NY, USA, 481–490. https://doi.org/10.1145/1985793.1985859

Diederik P Kingma and Jimmy Ba. 2014. Adam: A method for stochastic optimization. arXiv preprint arXiv:1412.6980 (2014).

Thomas N Kipf and Max Welling. 2016. Semi-supervised classification with graph convolutional networks. arXiv preprint arXiv:1609.02907 (2016).

Yujia Li, Daniel Tarlow, Marc Brockschmidt, and Richard Zemel. 2015. Gated graph sequence neural networks. arXiv preprint arXiv:1511.05493 (2015).

Zhen Li, Deqing Zou, Shouhuai Xu, Xinyu Ou, Hai Jin, Sujuan Wang, Zhijun Deng, and Yuyi Zhong. 2018. VulDeePecker: A Deep Learning-Based System for Vulnerability Detection. In 25th Annual Network and Distributed System Security Symposium, NDSS. http://wp.internetsociety.org/nds/wp-content/uploads/sites/25/2018/02/ndss2018_03A-2_Li_paper.pdf

Renjie Liao, Marc Brockschmidt, Daniel Tarlow, Alexander L Gaunt, Raquel Urtasun, and Richard Zemel. 2018. Graph partition neural networks for semi-supervised classification. arXiv preprint arXiv:1803.06272 (2018).

Chris Maddison and Daniel Tarlow. 2014. Structured generative models of natural source code. In International Conference on Machine Learning. 649–657.

Tomas Mikolov, Kai Chen, Greg Corrado, and Jeffrey Dean. 2013. Efficient estimation of word representations in vector space. arXiv preprint arXiv:1301.3781 (2013).

Renaud Pawlak, Martin Monperrus, Nicolas Petitprez, Carlos Noguera, and Lionel Seinturier. 2015. Spoon: A Library for Implementing Analyses and Transformations of Java Source Code. Software: Practice and Experience 46 (2015), 1155–1179.

Proc. ACM Program. Lang., Vol. 1, No. CONF, Article 1. Publication date: January 2018.
https://doi.org/10.1002/spe.2346

Michael Pradel and Koushik Sen. 2018. Deepbugs: a learning approach to name-based bug detection. *Proceedings of the ACM on Programming Languages* 2, OOPSLA (2018), 147.

Ripon Saha, Yingjun Lyu, Wing Lam, Hiroaki Yoshida, and Mukul Prasad. 2018. Bugs. jar: a large-scale, diverse dataset of real-world java bugs. In *2018 IEEE/ACM 15th International Conference on Mining Software Repositories (MSR)*. IEEE, 10–13.

Franco Scarselli, Marco Gori, Ah Chung Tsoi, Markus Hagenbuchner, and Gabriele Monfardini. 2008. The graph neural network model. *IEEE Transactions on Neural Networks* 20, 1 (2008), 61–80.

Qingkai Shi, Xiao Xiao, Rongxin Wu, Jinguo Zhou, Gang Fan, and Charles Zhang. 2018. Pinpoint: fast and precise sparse value flow analysis for million lines of code. In *Proceedings of the 39th ACM SIGPLAN Conference on Programming Language Design and Implementation*. ACM, 693–706.

Xujie Si, Hanjun Dai, Mukund Raghothaman, Mayur Naik, and Le Song. 2018. Learning loop invariants for program verification. In *Advances in Neural Information Processing Systems*. 7751–7762.

Yulei Sui, Ding Ye, and Jingling Xue. 2012. Static memory leak detection using full-sparse value-flow analysis. In *Proceedings of the 2012 International Symposium on Software Testing and Analysis*. ACM, 254–264.

Daniel Svozil, Vladimir Kvasnicka, and Jiri Pospichal. 1997. Introduction to multi-layer feed-forward neural networks. *Chemometrics and intelligent laboratory systems* 39, 1 (1997), 43–62.

Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N Gomez, Lukasz Kaiser, and Illia Polosukhin. 2017. Attention is all you need. In *Advances in neural information processing systems*. 5998–6008.

Ke Wang. 2019. Learning Scalable and Precise Representation of Program Semantics. *arXiv preprint arXiv:1905.05251* (2019).

Ke Wang, Rishabh Singh, and Zhendong Su. 2017. Dynamic Neural Program Embedding for Program Repair. *arXiv preprint arXiv:1711.07163* (2017).

Ke Wang and Zhendong Su. 2019. A Hybrid Approach for Learning Program Representations. *arXiv preprint arXiv:1907.02136* (2019).

Song Wang, Taiyue Liu, and Lin Tan. 2016. Automatically learning semantic features for defect prediction. In *2016 IEEE/ACM 38th International Conference on Software Engineering (ICSE)*. IEEE, 297–308.

Xin Ye, Razvan Bunescu, and Chang Liu. 2014. Learning to rank relevant files for bug reports using domain knowledge. In *Proceedings of the 22nd ACM SIGSOFT International Symposium on Foundations of Software Engineering*. ACM, 689–699.
A APPENDIX

A.1 Irreducible Graph

Figure 12 shows examples of graphs that can not be reduced to a single node.

Fig. 12. Examples of irreducible graph.
A.2 Examples of Array Index Out of Bound bugs and Class Cast Exceptions

Figure 13 and 14 show examples of the array index out of bound and class casting bugs. Note that even though there are lots of these kinds of bugs, the pattern of them are less than null pointer dereference bugs.

```
// Casting PC to ChildClass raises CCE.
public void manipulate(ParentClass PC) {
    ChildClass CC = (ChildClass) PC;
}

public void foo() {
    ParentClass PC = new ParentClass();
    manipulate(PC);
}
```

(a) A typical pattern of CCE.

```
// Extracted from bugs-dot-jar_LOG4J2-104
static {
    ...
    // url.returnLines() returns objects not in XML format
    props.loadFromXML(url.returnLines());
    ...
}
```

(b) CCE caused by different class.

```
// Extracted from bugs-dot-jar_CAMEL-9672
public Object getManagedObjectForProcessor(CamelContext context, Processor processor, ProcessorDefinition<? extends Processor> definition, Route route) {
    ...
    else if (target instanceof FilterProcessor) {
        // FilterDefinition is so precise that it results in CCE
        // The repair patch changes it to its parent class ExpressionNode.
        answer = new ManagedFilter(context, (FilterProcessor) target, (FilterDefinition) definition);
        ...
    }
}
```

(c) CCE caused by class inherent.

```
// Extracted from eclipse.jdt.ui-096ab8f
private ITypeBinding getDestinationBinding() throws JavaModelException {
    ...
    // None of the two class cast operations are safe.
    return (ITypeBinding)((SimpleName)node).resolveBinding();
    // Fixed codes
    if (!(node instanceof SimpleName)) return null;
    IBinding binding = ((SimpleName)node).resolveBinding();
    if (!(binding instanceof ITypeBinding)) return null;
    return (ITypeBinding)binding;
}
```

(d) CCE caused by multiple class cast operations.

Fig. 13. Illustrative examples of the CCE bugs.
1:26 Yu Wang, Fengjuan Gao, Linzhang Wang, and Ke Wang

(a) A typical pattern of AIOE.

```java
public void restoreState(IDialogSettings dialogSettings) {
...
  priorities[i] = Integer.parseInt(priority);
...
}
```

(b) AIOE caused by zero length array.

```java
public void logMessage(final String fqcn, final Level level,
  final Marker marker, final Message msg,
  final Throwable throwable) {
...
  if (... && params != null && params[params.length - 1] instanceof Throwable) {
    t = (Throwable) params[params.length - 1];
  }
...
}
```

(c) AIOE caused by miscalculate starting position in destination array.

```java
public void addFilterMapBefore(FilterMap filterMap) {
...
  // The 4-th argument should be filterMaps.length - (filterMapInsertPoint + 1)
  System.arraycopy(filterMaps, filterMapInsertPoint, results,
  filterMaps.length - filterMapInsertPoint + 1,
  ...
}
```

Fig. 14. Illustrative examples of AIOE.
A.3 Other Pertinent Information of Evaluated Projects

Table 5 shows the number of bugs and buggy methods in our evaluated projects. The number outside (inside) of the parenthesis is the number of bugs (buggy methods). Note that developer may fix multiple methods for a single bug so the number of buggy method and bugs may differ.

Table 5. Number of bugs of evaluated projects

| Projects           | Number of bugs (buggy methods) |
|--------------------|---------------------------------|
|                    | NPE    | AIOE   | CCE    |
| Lang               | 5 (7)  | 3 (5)  | 1 (2)  |
| Closure            | 2 (18) | 0 (0)  | 0 (0)  |
| Chart              | 4 (17) | 1 (7)  | 0 (0)  |
| Mockito            | 7 (14) | 2 (5)  | 5 (23) |
| Math               | 10 (16)| 8 (17) | 2 (3)  |
| Accumulo           | 5 (6)  | 0 (0)  | 0 (0)  |
| Camel              | 8 (17) | 1 (1)  | 1 (1)  |
| Flink              | 6 (13) | 0 (0)  | 0 (0)  |
| Jackrabbit-oak     | 7 (23) | 1 (1)  | 1 (1)  |
| Log4j2             | 16 (29)| 1 (1)  | 1 (2)  |
| Maven              | 3 (6)  | 0 (0)  | 0 (0)  |
| Wicket             | 6 (7)  | 1 (1)  | 3 (8)  |
| Birt               | 165 (678)| 19 (129)| 39 (154)|
| JDT UI             | 332 (897)| 39 (63)| 47 (156)|
| SWT                | 105 (276)| 40 (136)| 7 (26) |
| Platform UI        | 389 (920)| 27 (72)| 60 (194)|
| AspectJ            | 72 (151)| 9 (14) | 9 (19) |
| Tomcat             | 44 (111)| 6 (18) | 12 (28)|
| Total              | 1186 (3206)| 143 (470)| 188 (617)|