Path-Based Function Embedding and Its Application to Error-Handling Specification Mining

Daniel DeFreez  
University of California, Davis  
dcdefreez@ucdavis.edu

Aditya V. Thakur  
University of California, Davis  
avthakur@ucdavis.edu

Cindy Rubio-González  
University of California, Davis  
crubio@ucdavis.edu

ABSTRACT

Identifying relationships among program elements is useful for program understanding, debugging, and analysis. One such kind of relationship is synonymy. Function synonyms are functions that play a similar role in code; examples include functions that perform initialization for different device drivers, and functions that implement different symmetric-key encryption schemes. Function synonyms are not necessarily semantically equivalent and can be syntactically dissimilar; consequently, approaches for identifying code clones or functional equivalence cannot be used to identify them. This paper presents Func2vec, a technique that learns an embedding mapping each function to a vector in a continuous vector space such that vectors for function synonyms are in close proximity. We compute the function embedding by training a neural network on sentences generated using random walks over the interprocedural control-flow graph. We show the effectiveness of Func2vec for identifying function synonyms in the Linux kernel. Finally, we apply Func2vec to the problem of mining error-handling specifications in Linux file systems and drivers. We show that the function synonyms identified by Func2vec result in error-handling specifications with high support.

CCS CONCEPTS

- Computing methodologies → Unsupervised learning;  
- Software and its engineering → Automated static analysis; Error handling and recovery;

KEYWORDS

program analysis, program embeddings, error handling, program comprehension, specification mining

1 INTRODUCTION

Apart from writing new code, a software engineer spends a substantial amount of time understanding, evolving, and verifying existing software. Program comprehension [16] entails inferring a mental model of the relationships among various program elements [15]. When available, documentation can aid program comprehension [10]. For instance, documentation about high-level API functions often contains a “See Also” section enabling the reader to navigate to relevant functions. However, such documentation is either unavailable for low-level code, or it is difficult to maintain as the code evolves [14]. Furthermore, languages such as C lack features such as polymorphism and encapsulation that make explicit the relationships between functions.

This paper deals with the problem of identifying function synonyms: functions that serve the same purpose or play a similar role in code. Identifying function synonyms is especially challenging in low-level code written in C, such as the Linux kernel, because (i) function synonyms are often semantically different and syntactically dissimilar; e.g., snd_atiixp_free and snd_intel8x0_free in the Linux PCI sound drivers atiixp and intel8x0, respectively; (ii) function synonyms need not always have similar names; e.g., acpi_video_get_brightness and intel_panel_get_backlight each return the brightness level of the backlight; and (iii) functions with similar names are not necessarily synonyms; e.g., rcu_seq_start adjusts the current sequence number, while kprobe_seq_start returns the current sequence number. Thus, techniques that identify syntactic and semantic code clones, check semantic equivalence, or rely on naming conventions [7, 11, 31] cannot be used to identify function synonyms.

This paper presents Func2vec, a technique that learns an embedding mapping each function to a vector in a continuous vector space such that vectors for function synonyms are in close proximity. Figure 1 illustrates the output of Func2vec for the PCI sound drivers; in particular, Func2vec maps each function to a vector in $\mathbb{R}^{300}$, which is then projected onto 2-dimensions using t-SNE [17]. Functions are grouped based on functionality (probe, open, free, etc.); e.g., snd_atiixp_free and snd_intel8x0_free both belong to the group labeled free. Functions within each group are synonymous, and are clustered together in the Func2vec embedding.

Func2vec is based on the insight that two functions are synonyms if the contexts in which they are called along program paths are similar. Specifically, Func2vec encodes the program as a labeled pushdown system ($\ell$-PDS), where labels represent program elements such as function calls, instructions, types, and error codes. Random walks generated over the $\ell$-PDS are used to learn a vector
embedding using a neural network [19]. **Func2vec** is the first technique to use static interprocedural program traces to learn a function embedding that captures the hierarchical structure of programs.

Using two data sets, we show that **Func2vec** is capable of accurately identifying function synonyms for a runnable Linux kernel (2 million LOC). **Func2vec** is the first to learn a function embedding for large-scale low-level code such as the Linux kernel.

As a case study, we apply **Func2vec** to the problem of mining error-handling specifications in the Linux kernel. An error-handling specification lists the functions that should be executed when an error occurs based on the previous functions called. Specification mining is a popular technique with many applications [1, 8, 30, 32]. The number of times a specification occurs in the code is called its support. To avoid reporting false specifications, only specifications above a large support threshold are reported. However, even for a code base as large as Linux, many true specifications have a low support [30]. Furthermore, error-handling specifications have an even lower support because error-handling code is less common.

The key insight behind mining high-support error-handling specifications is that several low-support specifications can be merged if they involve function synonyms. Our specification miner leverages **Func2vec** as well as multiple implementations of Linux file systems and drivers to obtain merged error-handling specifications that have high support; Section 2 presents an example.

The contributions of this paper are as follows:

- **Func2vec**, a technique for learning a function embedding that captures the hierarchical structure of programs (§3).
- An evaluation of the effectiveness of **Func2vec** for finding function synonyms in the Linux kernel (§4).
- A formulation of mining error-handling specifications for low-level systems code that uses a function embedding (§5).
- An evaluation of the usefulness of **Func2vec** for mining merged error-handling specifications across 10 Linux file systems, and 48 Linux device drivers (§6).

We describe related work in §7, and conclude in §8.

## 2 Motivating Example

This section illustrates how identifying function synonyms can be used to mine error-handling specifications in Linux PCI sound drivers. Figure 2 shows excerpts from the function **snd_atiixp_create** in driver atiixp, and **snd_intel8x0_create** in driver intel8x0. Note that the functions look almost identical only because we have not shown dissimilar code (36 LOC in **snd_atiixp_create** and 193 LOC in **snd_intel8x0_create**).

An error handler is code that is executed if an error occurs; in Linux, it corresponds to a conditional statement that checks for an error. Figure 2 shows error handlers for **snd_atiixp_create** and **snd_intel8x0_create** (marked H1 through H5).

An error-handling specification imposes requirements on an error handler based on the set of functions that have been previously called. An error-handling specification is defined as \( C \Rightarrow R \), where \( C \) is the context and \( R \) is the response. This specification states that if the set of functions in the context are successfully called and an error occurs, then the functions in the response must be called (usually to release resources acquired by functions in the context).

The specification for error handler H2 in **snd_atiixp_create** (Figure 2a) is \( \{\text{pci_enable_device}, \text{kzalloc}, \text{pci_request_regions}\} \Rightarrow \{\text{snd_atiixp_free}\} \). The support of the specification is only 4. The specification for the error handler H4 in **snd_intel8x0_create** is \( \{\text{pci_enable_device}, \text{kzalloc}, \text{pci_request_regions}\} \Rightarrow \{\text{snd_intel8x0_free}\} \), which has the same context as the specification found in atiixp but has a different response. This specification has a support of 7. However, assuming a support threshold of 10, these two (true) specifications would not be reported by the specification miner due to their low support.

**Func2vec** reports that **snd_atiixp_free** and **snd_intel8x0_free** are function synonyms. Thus, the above specifications can be combined to form a merged error-handling specification. An error handler that supports any one of the specifications in the merge supports all of the specifications because the functions involved are synonyms. Consequently, merged specifications have support higher than those of the corresponding individual specifications. For example, when considering 48 device drivers, **Func2vec** finds 16 function synonyms for **snd_atiixp_free** and **snd_intel8x0_free**. Using this information, we find a merged specification with a support of 80. In Linux, merged specifications often result from combining multiple, similar implementations such as multiple device drivers or multiple file systems. As can be seen, function synonyms are crucial for finding merged specifications with high support.

## 3 Func2Vec: Path-Based Function Embedding

**Func2vec** maps a discrete set of functions to a continuous vector space; that is, given a vocabulary \( L \) of program functions, each program function \( \ell \in L \) is mapped to a \( d \)-dimensional vector in \( \mathbb{R}^d \). To accomplish this, **Func2vec** generates a linearized representation of programs, viz. “sentences” over a given vocabulary. **Func2vec** is the first to use static interprocedural program paths for this purpose. Intuitively, if many program paths have a call to function \( f_2 \) after a call to function \( f_1 \), and a call to \( f_3 \) after a call to \( f_1 \), then \( f_2 \) and \( f_3 \) should be embedded close to each other.
(a) Function snd_atiixp_create in driver atiixp

(b) Function snd_intel8x0_create in driver intel8x0

Figure 2: (a) An excerpt from the function snd_atiixp_create in the driver atiixp (sound/pci/atiixp.c). The function contains three error-handling specifications. Each specification consists of a context set (function calls highlighted in gray) and a response set (function calls in a box). The first specification is associated with error handler H2 and has a 1-element context (highlighted in gray) and a 1-element response (in a box). The second specification is associated with error handler H3 and has a 2-element context (highlighted in gray) and a 2-element response (in a box). The third specification is associated with handlers H4 and H5. It has a 3-element context (highlighted in gray) and a 1-element context (in a box); (b) an excerpt from the function snd_intel8x0_create in the driver intel8x0 (sound/pci/intel8x0.c) in which three error-handling specifications are also found. The specifications for the two functions differ only in the response for the third specification.

A naive approach for linearizing a program is to generate a sentence using the instructions along every valid interprocedural path in the program. Such an approach has the following disadvantages: using the entire instruction set would generate sentences with a very large vocabulary; there are too many program paths for this approach to be practical; and it does not capture the hierarchical structure of programs.

The design of Func2vec addresses each of these disadvantages. Func2vec abstracts each program instruction to reduce the vocabulary. To address the path explosion problem, Func2vec performs a random walk of the program restricted to generate \( \gamma \) paths of length at most \( k \) starting at a call to each function. Lastly, on encountering a function call, the random walk either outputs the function name itself, or decides to step into the function definition. This strategy of the random walk is able to capture the hierarchical structure of programs: the context preceding the function call can be linked to either the function call itself or to the context in the body of the function being called. Figure 3 shows the three main components of Func2vec.

### 3.1 Program Encoder

A pushdown system (PDS) is used to model the set of valid interprocedural paths in the program [26]. A PDS is defined as follows:

Definition 3.1. A pushdown system is a triple \( \mathcal{P} = (P, \Gamma, \Delta) \) where \( P \) and \( \Gamma \) are finite sets, control locations and stack alphabet, respectively. A configuration of \( \mathcal{P} \) is a pair \( (p, w) \), where \( p \in P \) and \( w \in \Gamma^* \). \( \Delta \) contains a finite number of rules \( (p, \gamma) \rightarrow (p', w) \), where \( p, p' \in P \) and \( \gamma, w \in \Gamma^* \), which define a transition relation \( \Rightarrow \) between configurations of \( \mathcal{P} \) such that if \( r = (p, \gamma) \rightarrow (p', w) \), then \( (p, \gamma w') \Rightarrow (p', w'') \) for all \( w'' \in \Gamma^* \).

\( c \xrightarrow{r} c' \) denotes that the rule \( r \in \Delta \) was used to transition from configuration \( c \) to \( c' \) of \( \mathcal{P} \). To model control flow of a program a
void pci_disable_device(struct pci_dev *dev)
{
    struct pci_devres *dr = ...
    if (dr == NULL) {
        dev->enabled = 0;
    }
    do_pci_disable_device(dev);
}

int snd_atiixp_create(...)
{
    struct atiixp *chip = ...
    if (chip == NULL) {
        pci_disable_device(dev);
        return -ENOMEM;
    }
    err = ...
    if (err < 0)
    {
        pci_disable_device(dev);
        kfree(chip);
        return err;
    }
    chip->addr = ...
    ...
}

Rules for snd_atiixp_create:
(1) (p, n1) → (p, n2): atiixp
(2) (p, n3) → (p, n4): EQ
(3) (p, n5) → (p, n6): pci_disable_device
(4) (p, n7) → (p, n8): ENOMEM
(5) (p, n9) → (p, e)
(6) (p, n10) → (p, n11): STORE
(7) (p, n11) → (p, n12): LT
(8) (p, n12) → (p, e)
(9) (p, n13) → (p, n14): atiixp
(10) (p, n14) → (p, n15): pci_disable_device
(11) (p, n15) → (p, n16): pci_devres
(12) (p, n16) → (p, e)
(13) (p, n17) → (p, n18): pci_disable_device
(14) (p, n18) → (p, n19): pci_devres
(15) (p, n19) → (p, n20): EQ
(16) (p, n20) → (p, n21): kfree
(17) (p, n21) → (p, e)
(18) (p, n22) → (p, e)
(19) (p, n23) → (p, n24): pci_devres
(20) (p, n24) → (p, e)
(21) (p, n25) → (p, e)

Rules for pci_disable_device:
(22) (p, n2) → (p, n3): pci_devres
(23) (p, n3) → (p, n4): EQ
(24) (p, n4) → (p, n5)
(25) (p, n5) → (p, n6)
(26) (p, n6) → (p, n7): pci_devres
(27) (p, n7) → (p, n8)
(28) (p, n8) → (p, n9)
(29) (p, n9) → (p, n10)
(30) (p, n10) → (p, n11): kfree
do_pci_disable_device
(31) (p, n11) → (p, n12)
(32) (p, n12) → (p, e)

(a) Simplified code from Figure 2a
(b) Graphical representation of ℓ-PDS
(c) ℓ-PDS rules

Figure 4: Example of ℓ-PDS Encoding

A labeled PDS (ℓ-PDS) is a PDS in which each rule is associated with a sequence of labels, and these labels are concatenated as the ℓ-PDS makes its transitions. More formally:

Definition 3.2. A labeled pushdown system (ℓ-PDS) is a triple \( \mathcal{L} = (\mathcal{P}, \mathcal{L}, f) \), where \( \mathcal{P} = (\mathcal{P}, \Gamma, \Lambda) \) is a PDS, \( \mathcal{L} \) is a finite set of labels, and \( f : \Lambda \rightarrow \mathcal{L} \) is a map that assigns a sequence of labels to each rule of \( \mathcal{P} \). A configuration \( \mathcal{C} \) is a pair \( (c, l) \), where \( c \) is a configuration of the PDS \( \mathcal{P} \) and \( l \in \mathcal{L} \). \( \mathcal{C} \) and \( \mathcal{L} \) define the transition relation \( \Rightarrow \) between configurations of \( \mathcal{C} \) such that if \( c \Rightarrow c' \) and \( c \in \Lambda \), then \( c \Rightarrow (c', l') \), where \( f(l) = l' \).

\( c \Rightarrow c' \) denotes that the rule \( r \in \Lambda \) was used to transition from configuration \( c \) to \( c' \) of \( \mathcal{L} \). In practice, labels are only attached to internal rules of the ℓ-PDS. A unique label is assigned to each instruction category, error code, struct type, and function. Each function is abstracted to a list of such labels as follows:

- Instructions are classified into categories such as LOAD, STORE, EQ, etc. The internal rule associated with a particular instruction is labeled with the corresponding instruction category.
- Systems code defines specific constants that are used as error codes; see §5. If such an error is used in the instruction, then we add the error-code label to the corresponding internal rule.
- If the instruction loads or stores to a struct variable, then we add the struct-type label to the corresponding internal rule.
- If the instruction is a function call, then the function label to the corresponding internal rule is added.

Example 3.3. Figure 4a shows simplified functions pci_disable_device and snd_atiixp_create (from §2). Figure 4b shows a graphical representation of the corresponding ℓ-PDS. Figure 4c lists the ℓ-PDS rules; we use the notation \( r : l \) to mean that \( f(r) = l \) in the ℓ-PDS. The instruction-category labels used in this example are [EQ, STORE, LT] (for simplicity, we do not include labels LOAD and RET); the struct-type labels are [atiixp, pci_devres], the error-code labels are [ENOMEM], and the function labels are [pci_disable_device, kfree, do_pci_disable_device].

We describe the first 7 rules for the function snd_atiixp_create in Figure 4c. The internal rule (1) corresponds to line 14 in Figure 4a, where the variable chip of type struct atiixp is assigned. Thus, the rule is labeled with struct-type label atiixp. The internal rule (2) corresponds to the equality expression on line 15, and is attached the instruction label EQ. Unlabeled rules (3)
Given an ℓ-PDS \( L = (P, L, f) \), a window size \( w \), embedding size \( d \), walks per label \( y \), and walk length \( k \), \textsc{Func2vec} (Algorithm 2) generates \( y \) walks for each label in \( L \), and uses them to train the model. The result is a vector representation for labels \( \Phi: L \rightarrow \mathbb{R}^d \).

**Algorithm 2: \textsc{Func2vec} \((L, w, d, y, k)\)**

**Input:** \( \ell \)-PDS \( L = (P, L, f) \), window size \( w \), embedding size \( d \), walks per label \( y \), walk length \( k \)

**Output:** Vector representation for labels \( \Phi: L \rightarrow \mathbb{R}^d \)

1. \( W \leftarrow \emptyset \)
2. for \( i \leftarrow 0 \) to \( y \) do
3. \( \text{foreach } \ell \in L \) do
4. \( V \leftarrow W \cup \text{RandomWalk}(L, \ell, k) \)
5. \( \Phi \leftarrow \text{TrainModel}(W, d, w) \)

and (4) correspond to the true and false branches of the conditional on line 15. Call rule (5) and internal rule (6) are associated with the function call \texttt{pci\_disable\_device} on line 16. Note that the call rule is not labeled; the internal rule has a function label \texttt{pci\_disable\_device}. Finally, rule (7) is given the error-code label \texttt{ENOMEM}, and corresponds to the return statement on line 17. ■

### 3.2 Random Walker

Algorithm 1 shows how to generate a random walk of an ℓ-PDS. Given a set \( S \), \text{Random}(S) returns an element \( s \in S \) that is chosen uniformly at random. \text{Labels}(s) returns the sequence of labels associated with an ℓ-PDS configuration. Given an ℓ-PDS \( L \), a start label \( \ell \), and a walk length \( k \), a random walk is generated as follows. A rule associated with label \( \ell \) is chosen at random (line 1), and the configuration \( c \) is initialized (line 2). Then, in the loop at line 4 the current configuration \( c \) is updated by choosing uniformly at random a next configuration in the ℓ-PDS. Note that in Definition 3.2, labels are concatenated when the configuration is updated.

**Example 3.4.** Consider label \( \ell = \texttt{attixp} \), and walk length \( k = 10 \).

There are two rules associated with \texttt{attixp}: rules (1) and (19) from Figure 4c. Assume rule (1) was chosen and the random walk starts at rule (1) with label \texttt{attixp}. Two possible random walks would be:

- \( W_1 \leftarrow \text{attixp} \texttt{EQ} \texttt{pci\_disable\_device} \texttt{ENOMEM} \)
- \( W_2 \leftarrow \text{attixp} \texttt{EQ} \texttt{pci\_deves} \texttt{EQ} \texttt{pci\_deves do pci\_disable\_device} \)

During walk \( W_1 \) internal rule (6) was chosen, while walk \( W_2 \) stepped into the function call by choosing the call rule (5). ■

### 3.3 Model Trainer

Given an ℓ-PDS \( L \), a window \( w \), a dimension \( d \), a number of walks per label \( y \), and a walk length \( k \), \textsc{Func2vec} (Algorithm 2) generates \( y \) walks for each label in \( L \), and uses them to train the model. The result is a vector representation for labels \( \Phi: L \rightarrow \mathbb{R}^d \).

TrainModel on line 5 uses a neural network to learn \( \Phi \). Traditional language models try to estimate the probability of seeing a label \( \ell \) given the context of the previous labels in the random walk; viz. \( \Pr(\ell_1|\ell_1, \ell_2, \ldots, \ell_{i-1}) \). Apart from learning the probability distribution of label co-occurrences, we also want to learn the embedding: \( \Phi: L \rightarrow \mathbb{R}^d \). Thus, our problem is to estimate the likelihood: \( \Pr(\ell_i|\Phi(\ell_1), \Phi(\ell_2), \ldots, \Phi(\ell_{i-1})) \). Mikolov et al. [19] introduce a technique that uses a single-layer fully-connected neural network to approximate this likelihood. It uses a context of size \( w \) both before and after the given word, and considers the context as a set ignoring the ordering constraint. This results in the following optimization problem for computing \( \Phi \): maximize \( \log \Pr(\ell_i|\Phi(\ell_{i-w}), \ldots, \Phi(\ell_{i-1}), \Phi(\ell_{i+1}), \ldots, \Phi(\ell_{i+w})) \).

The implementation of \textsc{Func2vec} uses the implementation of Mikolov et al. [19] provided in Gensim [25].

### 4 \textsc{Func2vec} Evaluation

The experiments in this section are designed to answer the following research questions:

- **RQ1.** How effective is \textsc{Func2vec} at identifying function synonyms?
- **RQ2.** What impact do path-based sentences have?

\textsc{Func2vec} is evaluated against a runnable Linux kernel with all file systems and PCI sound drivers included, roughly 2 million LOC. The resulting ℓ-PDS consists of 5,407,483 stack locations (nodes), 6,083,632 PDS rules, and 77,194 labels. For this experiment the number of walks generated per label \( y \) was 100, the walk length \( k \) was 100, the vector dimension \( d \) was 300, and the window size \( w \) was 10. Setting the window size \( w \) to 10 indicates a window of 10+10, where 10 labels in either the forward or backward direction are within the sliding window. These parameters were chosen via grid search over a small training set that is disjoint from the gold standard below. To process the Linux kernel, \textsc{Func2vec} requires approximately 24G of memory and two hours of compute time on Amazon EC2 R4 instances. These instances use Intel Xeon E5-2686 v4 (Broadwell) Processors and DDR4 Memory.

**Gold Standard.** We constructed two gold standard data sets to evaluate \textsc{Func2vec}. The first data set, GS1, consists of 2,652 unique functions that were identified by hand and reviewed with the help of a Linux kernel developer. These functions form 265 equivalence classes of function synonyms, ranging in size from two to 94. Note that the functions in GS1 cross components, can violate naming conventions, and are generally the hardest class of synonyms to find. Specifically, GS1 includes 6,079 function pairs that are synonyms, but do not follow any known naming scheme, e.g., \texttt{nlmsg\_trim} and \texttt{gen\_msg\_cancel}, and 2,279 functions pairs that are not synonyms, but do follow a naming scheme, e.g., \texttt{sr\_release} and \texttt{sd\_release}.

We constructed a second data set GS2 by relying on a single strong naming convention. In Linux it is often the case that two different functions are created that perform essentially the same task, and one of the functions has underscores prepended to the name. GS2 consists of the 2,017 pairs of functions of this form. As a sanity check, a random sample of 50 pairs was selected and all 50 were judged to be function synonyms.

**Evaluation Metrics.** Two different metrics are used to evaluate \textsc{Func2vec}. The first metric is the area under the Receiver Operating
Figure 5: Receiver Operating Characteristic (ROC) Curves

(a) Gold Standard GS1

(b) Gold Standard GS2

Table 1: Func2vec Metrics

<table>
<thead>
<tr>
<th>Gold Standard Test</th>
<th>Metric</th>
<th>Path-based</th>
<th>Flat</th>
</tr>
</thead>
<tbody>
<tr>
<td>GS1: Manually reviewed</td>
<td>AUROC</td>
<td>0.72</td>
<td>0.56</td>
</tr>
<tr>
<td>GS2: Underscore names</td>
<td>AUROC</td>
<td>0.81</td>
<td>0.67</td>
</tr>
<tr>
<td>GS1: Manually reviewed</td>
<td>Cluster F1</td>
<td>0.73</td>
<td>0.56</td>
</tr>
<tr>
<td>GS2: Underscore names</td>
<td>Cluster F1</td>
<td>0.59</td>
<td>0.52</td>
</tr>
</tbody>
</table>
Threats to Validity. Identifying function synonyms is an inherently subjective task. We tried to mitigate this as much as possible by enlisting the assistance of a Linux kernel developer when constructing our gold standard. Multiple people performed overlapping classification independently, and any conflicting classifications were flagged and discussed. Nonetheless, it is not feasible to construct exhaustive ground truth for the Linux kernel, and therefore it is possible that Func2vec will perform differently for classes of function synonyms we are unaware of.

5 ERROR-HANDLING SPECIFICATIONS

To show the practical utility of identifying synonymous functions with Func2vec, we present a detailed case study exploring their effect on mining error-handling specifications. The major phases of the mining process are locating error handlers, extracting error handler contexts and responses, and frequent itemset mining. These phases are shown in Figure 6 and described in this section.

5.1 Defining Error-Handling Specifications

Error-handling specifications are mined based on the observation that the actions performed after an error occurs (the error-handler response) frequently depend on the actions carried out before the error occurred (the error-handler context). Such a context and response pair define an error-handling specification.

Error Handlers. An error handler is a piece of code that is executed upon detection of an error. Our evaluation targets the Linux kernel, which is written in C. Without explicit error-handling language constructs such as try/catch, locating error handlers in C code must rely on some amount of domain knowledge. We know that Linux defines a specific set of integer error constants, referred to as error codes. When returned from a function, these error codes denote an error that has occurred. This is known as the return-code idiom.

The context and response of an error handler consist of the functions called before and after an error is detected, respectively. In many cases, the order in which these functions are called does not matter. Once the predicate associated with the error handler is identified, the context and response are computed via traversing the code paths in the backward and forward directions, respectively.

Example 5.1. The function snd_atiixp_create in Figure 2a contains the five error handlers H1–H5; which are listed in Table 2 along with their corresponding contexts and responses.

---

```
static struct inode *btrfs_new_inode(...) {
  // Most of the function is omitted
  path = btrfs_alloc_path();
  ...
  btrfs_free_path(path);
  ret = ...
  if (ret) {
    // btrfs_free_path not required
  }
}
```

---

Figure 7: Code snippet from the btrfs file system. The path is freed prior to the error handler on line 7 is reached.

Error-Handling Specifications. An error-handling specification is defined as an association rule whose antecedent is the specification context and consequent is the specification response. This rule simply means that the set of function calls in the context implies that the set of function calls in the response are required to happen once an error is detected.

Definition 5.2. An error-handling specification $S$ is defined as $C_S \Rightarrow R_S$, where $C_S = \{c_1, c_2, \ldots, c_m\}$ is the context set of function calls for the specification $S$, and $R_S = \{r_1, r_2, \ldots, r_m\}$ is the response set of function calls for the specification $S$.

Example 5.3. The following error-handling specifications can be inferred for the atiixp sound driver:

$S_1 \equiv \{pci_enable_device\} \Rightarrow \{pci_disable_device\}$

$S_2 \equiv \{pci_enable_device, kalloc\} \Rightarrow \{pci_disable_device, kfree\}$

$S_3 \equiv \{pci_enable_device, kalloc, pci_request_regions\} \Rightarrow \{snd_atiixp_free\}$

Definition 5.4. An error-handling specification $S \equiv C_S \Rightarrow R_S$ is applicable to an error-handler $H$, denoted by $S \triangleright H$, iff $C_S \subseteq C_H$ and $C_S \cup R_S \subseteq C_H$, where $C_H$ and $R_H$ are the context and response of the error handler $H$, respectively.

Example 5.5. Consider the error-handlers H1–H5 in Ex. 5.1 and the specifications in Ex. 5.3; then $S_1 \triangleright H_2$, $S_2 \triangleright H_3$, $S_3 \triangleright H_4$, and $S_3 \triangleright H_5$.

The first term $C_S \subseteq C_H$ in Definition 5.4 says that the entire specification context must apply to the handler context. The second term $C_S \cup R_S \subseteq C_H$ is added for cases where the required response actions have already happened prior to a particular error handler being reached, as illustrated by the following example.

Example 5.6. Consider the specification $S \equiv \{btrfs_alloc_path\} \Rightarrow \{btrfs_free_path\}$, and the code snippet from the btrfs file system, shown in Figure 7. The context $C_H$ for the error handler $H$ at line 7 is $\{btrfs_alloc_path, btrfs_free_path\}$. If Definition 5.4 is restricted to only contain the term $C_S \subseteq C_H$, then specification $S$ is applicable to the error handler $H$. Clearly this is incorrect, as the path has been allocated and then freed prior to the error handler being reached. Consequently, without the second term in Definition 5.4, the error handler $H$ would be flagged as a violation, even though the path has already been freed.

Definition 5.7. An error-handling specification $S \equiv C_S \Rightarrow R_S$ is satisfied by an error-handler $H$, denoted by $S \triangleright H$, iff $S \triangleright H$ and $R_S \subseteq R_H$, where $R_H$ is the response of $H$.

---

Figure 6: Specification Mining Architecture

---

Figure 7: Code snippet from the btrfs file system. The path is freed prior to the error handler on line 7 is reached.
Error Handling Specifications

<table>
<thead>
<tr>
<th>Error Handler</th>
<th>Lines</th>
<th>Function Generating Error</th>
<th>Context</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1</td>
<td>1596</td>
<td>pci_enable_device</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>H2</td>
<td>1600-1601</td>
<td>kcalloc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H3</td>
<td>1610-1612</td>
<td>pci_request_regions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H4</td>
<td>1623-1625</td>
<td>request_irq</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H5</td>
<td>1633-1634</td>
<td>snd_device_new</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 2: Error Handlers in snd_atiixp_create

Let $\mathcal{T}$ be a set of transactions, where each transaction $T \in \mathcal{T}$ is a set of items. A frequent itemset mining algorithm returns the sets of items that frequently co-occur in the same transaction in $\mathcal{T}$.

**Example 5.8.** Consider the error-handlers in Ex. 5.1 and the specifications in Ex. 5.3, then $S_{1} \triangleright H_{2}, S_{2} \triangleright H_{3}, S_{3} \triangleright H_{4}$, and $S_{4} \triangleright H_{5}$. If the call to function snd_atiixp_free on line 1633 in Figure 2a was missing, then $S_{3} \triangleright H_{5}$; i.e., $S_{3}$ would not be satisfied by $H_{5}$. □

The above definitions of error-handling specifications and satisfiability can be extended to handle synonymous functions. Let $F$ be the set of functions in the program that is being mined. $\Pi : F \to F$ is said to be a partition function iff $\Pi(f_{1}) = \Pi(f_{2})$ for all functions $f_{1}$ and $f_{2}$ that are identical or synonyms. We abuse notation slightly by extending the partition function that applies to a single function to a set of functions: $\Pi((f_{1}, f_{2}, \ldots, f_{n})) = (\Pi(f_{1}), \Pi(f_{2}), \ldots, \Pi(f_{n}))$. Similarly, given an error-handling specification $S \supseteq C_{S} \supseteq R_{S}$, we use $\Pi(S)$ to mean $\Pi(C_{S}) \supseteq \Pi(R_{S})$.

**Definition 5.9.** Given a partition function $\Pi$, a set $X$ of error-handling specifications is said to be a merged error-handling specification with respect to $\Pi$ iff $\Pi(S) = \Pi(S')$ for all $S, S' \in X$. □

**Example 5.10.** Let the partition function $\Pi$ be such that $\Pi(snd_atiixp_free) = \Pi(snd_int18x8_free)$. Then $\{\{pci_enable_device, kcalloc, pci_request_regions\}, \{pci_enable_device, kcalloc, pci_request_regions\}, \{snd_int18x8_free\}\} = \{\{pci_enable_device, kcalloc, pci_request_regions\}, \{pci_enable_device, kcalloc, pci_request_regions\}, \{snd_int18x8_free\}\}$ is a merged error-handling specification with respect to $\Pi$.

Using this notation, Definitions 5.4 and 5.7 can be naturally extended to merged error-handling specifications.

**Definition 5.11.** A merged error-handling specification $X$ is applicable to an error-handler $H$, denoted by $X \triangleright H$, iff there exists $S \in X$ such that $S \triangleright H$. □

**Definition 5.12.** A merged error-handling specification $X$ is satisfied by an error-handler $H$, denoted by $X \triangleright H$, iff there exists $S \in X$ such that $S \triangleright H$. □

### 5.2 Mining Error-Handling Specifications

Given a set of error handlers with their respective contexts and responses, frequent itemset mining is used to infer likely error-handling specifications. Frequent itemset mining algorithms take the minimum support threshold as a parameter, and return all sets of items that have a support greater than or equal to this threshold.

**6 SPECIFICATION MINING EVALUATION**

This section is designed to answer the following question: what impact do function synonyms have on the quality of mined error-handling specifications?

We mine error-handling specifications in 48 drivers and 10 Linux file systems (btrfs, cryptfs, ext2, ext4, GFS2, HFS, HFS+, nilfs2, OCFS2, and UFS). We chose Linux file systems and drivers because of the dire consequences of error handling defects, but the mining approach is general and can be applied to other parts of Linux, or to any C program that uses the return-code idiom for error handling. Frequent itemset mining is used to infer specifications in this evaluation, but function synonyms could be used to enhance other mining techniques.

**Implementation Details.** As shown in Figure 6, our miner takes as input (1) error handler context and response sets, and (2) synonymous function information. Our implementation relies extensively on the LLVM compiler infrastructure [12]. To locate error handlers, we use an existing LLVM-based error-propagation analysis [27–29], augmented with an LLVM pass that identifies handlers based on a list of functions that are known to be called only on error paths. Table 3 shows the total number of error handlers found. Function synonyms are identified by Func2vec. Eclat/LCM [4] is used to compute frequent itemsets.
Table 4: Specification support improvement when using synonyms. The “Un.” column lists the support for each specification without merging, and the “Mrg.” column lists the support for each specification after merging.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>[pci_enable_device, kzalloc, pci_request_regions]</td>
<td>7 80</td>
<td>124 124</td>
</tr>
<tr>
<td>[pci_enable_device, kzalloc, pci_request_regions]</td>
<td>6 80</td>
<td>124 124</td>
</tr>
<tr>
<td>[pci_enable_device, kzalloc, pci_request_regions]</td>
<td>4 80</td>
<td>124 124</td>
</tr>
<tr>
<td>[pci_enable_device, kzalloc, pci_request_regions]</td>
<td>4 80</td>
<td>124 124</td>
</tr>
<tr>
<td>[pci_enable_device, kzalloc, pci_request_regions]</td>
<td>6 80</td>
<td>124 124</td>
</tr>
<tr>
<td>[pci_enable_device, kzalloc, pci_request_regions]</td>
<td>3 124</td>
<td>124 124</td>
</tr>
<tr>
<td>[pci_enable_device, kzalloc, pci_request_regions]</td>
<td>2 124</td>
<td>124 124</td>
</tr>
<tr>
<td>[pci_enable_device, kzalloc, pci_request_regions]</td>
<td>2 124</td>
<td>124 124</td>
</tr>
<tr>
<td>[pci_enable_device, kzalloc, pci_request_regions]</td>
<td>3 124</td>
<td>124 124</td>
</tr>
<tr>
<td>[pci_enable_device, kzalloc, pci_request_regions]</td>
<td>6 124</td>
<td>124 124</td>
</tr>
<tr>
<td>[btrfs_alloc_path]</td>
<td>487 541</td>
<td>124 124</td>
</tr>
<tr>
<td>[btrfs_alloc_path]</td>
<td>54 541</td>
<td>124 124</td>
</tr>
<tr>
<td>[gfs2_holder_init]</td>
<td>33 74</td>
<td>124 124</td>
</tr>
<tr>
<td>[gfs2_glock_nq]</td>
<td>23 74</td>
<td>124 124</td>
</tr>
<tr>
<td>[gfs2_glock_nq]</td>
<td>28 74</td>
<td>124 124</td>
</tr>
<tr>
<td>[hfs_find_init]</td>
<td>17 49</td>
<td>124 124</td>
</tr>
<tr>
<td>[hfsplus_find_init]</td>
<td>32 49</td>
<td>124 124</td>
</tr>
<tr>
<td>[__kmalloc]</td>
<td>187 353</td>
<td>124 124</td>
</tr>
<tr>
<td>[kzalloc]</td>
<td>166 353</td>
<td>124 124</td>
</tr>
</tbody>
</table>

Examples of Specifications. To further illustrate the impact on specification quality, Table 4 shows six examples of merged error-handling specifications. The first example shows a specification found across device drivers (see §3). All 18 functions found in the response sets (e.g., snd_intel8x0_free, snd_via8x0m_free, etc.) are function synonyms reported by Func2vec for brevity, we only list 5 individual specifications. This results in a merged specification with a support of 80. Without synonyms, these individual specifications would not be reported at all because they fall below the support threshold of 10.

Not all of the sound driver specifications in Table 4 have the same form. The five specifications in the second row, starting with snd_nm256_free, are taken from a group of 8 merged specifications. Unlike the first example, these do not include pci_request_regions in the context, even though all of these free functions are synonyms and close together in the Func2vec embedding. The free functions in the second row do not call pci_release_regions, and therefore pci_request_regions does not appear in any of the contexts. Here, specification mining and Func2vec have worked in concert to arrive at the correct specifications.

The btrfs example in Table 4 illustrates merging specifications within a single implementation. btrfs_free_path is a synonym of the function btrfs_release_path, as the primary purpose of each is to drop references to a path in the file system. The difference is that btrfs_free_path also frees the memory, while callers of btrfs_release_path handle the memory operation separately. Merging these related specifications brings up the btrfs_release_path version so that they appear together in the mining report.

The specifications shown in the fourth row of Table 4 led to the discovery of two previously unknown bugs in the GFS2 file system. The patch we submitted to fix these bugs was accepted by Red Hat and merged into Linux version 4.7. Figure 8 shows one of the two bugs. The function first calls gfs2_holder_init, which acquires a reference to a glock. The function then attempts to enqueue this holder structure. On the normal path where gfs2_glock_nq succeeds, there is no problem. If gfs2_glock_nq fails on line 4, however, gfs2_holder_uninit is never called even though gfs2_holder_init completed successfully. As is common with error handling bugs, only in rare circumstances will this problem be encountered because it requires gfs2_glock_nq to fail. But when the bug is triggered the consequences are severe, resulting in an inaccurate reference count for the glock.

Figure 8: Bug found in GFS2. The function should not exit on line 7 without calling gfs2_holder_uninit.
The fifth row in Table 4 shows a specification that crosses two related file systems, HFS and HFS+. The HFS and HFS+ file systems are implemented by Linux to interoperate with Mac OS. Other related file systems such as ext2 and UFS also contain specifications that can be improved by merging with function synonyms.

Finally, the sixth row illustrates how function synonyms can be useful even for specifications that already have high support. The function kalloc is similar to kmalloc because they both allocate memory, but kalloc zeroes the memory first. From an error-handling perspective they are equivalent.

7 RELATED WORK

Distributed Representations. Distributed representations have been extensively studied in natural language processing and cognition [9]. Recent advances have resulted in scalable approaches to computing such distributed representations (or vector embeddings) given a corpus of sentences; for instance, word2vec [19], and Glove [22]. DeepWalk [23] computes vector embeddings of nodes in a graph. DeepWalk is similar to Func2vec in that they both use random walks to generate a corpus of sentences. However, DeepWalk generates walks consisting of nodes, while Func2vec generates walks consisting of labels along edges. Func2vec also abstracts the program code into an ℓ-PDS. Ye et al. [36] apply vector representations to information retrieval in software engineering by using word2vec on documentation associated with code.

Nguyen et al. [21] computes distributed representations of API functions using word2vec. They generated sentences using the program AST, as opposed to interprocedural paths, and used their technique to migrate API usages from Java to C#. Similarly, Alon et al. [2] presents an approach for learning program representations using paths in the AST, which is then used to predict names for variables and methods in JavaScript, Java, Python, and C# programs. Wang et al. [33] learns program embeddings from program execution traces, and use the embeddings to classify errors in student programming assignments written in C#. DeepBugs [24] learns a word2vec-based embedding for each identifier in a JavaScript program using the sequence of tokens around the identifier. This embedding is used for name-based bug detection. In contrast to these approaches, we propose a technique to learn a function embedding from interprocedural static paths in the program, and use the embedding in mining error-handling specifications in Linux, which is written in C.

Error-Handling Specification Mining. One of the key developments in the error-handling specification mining literature has been the use of normal paths to mine specifications for error-handling paths. This line of thought was first mentioned in [35], and was subsequently used in several other papers [1, 8, 30, 32, 35].

Weimer and Necula [35] find association rules of the form FCa ⇒ FCe, where function call FCa should be followed by call FCe, and FCe is found at least once in exception-handling code. Improving on [35], Thummalapenta and Xie [32] mine conditional association rules of the form (FC1,...FCn) ∧ FCa ⇒ FC1′...FCn′, which denotes a sequence of function calls prior to the target function FCa that throws an exception, and then a sequence of recovery function calls. Acharya and Xie [1] mine error-handling specifications from interprocedural traces. Cleanup functions are identified from error traces, which are then used along with normal traces to find specifications. Goues and Weimer [8] broaden this notion of trace reliability to include a number of other features (e.g., execution frequency, cloning, code age, density, etc.), and significantly improve the false positive rate reported in [35]. Collectively, these approaches have been successful at finding defects in error-handling code that shares function calls with normal paths. But there exist functions that are only called on error paths, and that are only meaningful to Linux. Thus the correct use of these functions cannot be deduced from normal paths or outside programs, and they would be missed by the above approaches.

Much of the work on error-handling specifications has focused on languages with exception-handling support, such as Java or C++. Several approaches [5, 32, 34, 35] find error-handling specifications in Java programs using static analysis. Buse and Weimer [5] infer and characterize exception-causing conditions, which are then used as documentation. Weimer and Necula [34] use dataflow analysis to locate resource management mistakes in error-handling code and propose a language extension to improve reliability. A common mistake found might be the failure to release resources or to clean up properly along all paths. Identifying blocks of error-handling code in these languages is comparatively easy; but as we have shown, it is more challenging to distinguish between normal and error-handling paths in Linux.

Implementation Inconsistencies. Engler et al. [6] use the notion of internal consistency to find programming errors. One of their techniques for finding related pieces of code relied on the idiomatic use of function pointers to define multiple implementations of a single interface. Min et al. [20] compare multiple file systems by leveraging the VFS interface to identify implementations of the same functionality. These are complementary to our work.

8 CONCLUSION

We introduced the notion of function synonyms, which are functions that play a similar role in code. Synonymous functions might be syntactically dissimilar and might not be semantically equivalent. We presented Func2vec, a technique that learns an embedding mapping each function to a vector in a continuous vector space such that vectors for function synonyms are in close proximity. Specifically, Func2vec computes a function embedding by training a neural network on sentences generated using random walks of the interprocedural control-flow graph of the program. We showed the effectiveness and scalability of Func2vec by evaluating it against two gold standards of function synonyms in the Linux kernel.

We showed how Func2vec can improve the quality of error-handling specifications for 10 Linux file systems and 48 Linux device drivers. A challenge in mining error-handling specifications is that their support is often too low. To overcome this challenge, Func2vec was used to identify function synonyms across multiple implementations of file systems and device drivers. These function synonyms were then used to merge individual error-handling specifications, resulting in merged specifications with high support.

ACKNOWLEDGMENTS

This work was supported by NSF grant CCF-1464439, and AWS Cloud Credits for Research.