Differential Precondition Checking: A Lightweight, Reusable Analysis for Refactoring Tools

Jeffrey L. Overbey and Ralph E. Johnson
Department of Computer Science
University of Illinois at Urbana-Champaign
{overbey2,johnson}@cs.illinois.edu

***Abstract*—One of the most difficult parts of building automated refactorings is ensuring that they preserve behavior. This paper proposes a new technique to check for behavior preservation; we call this technique *differential precondition checking.* It is simple yet expressive enough to implement the most common refactorings, and the core algorithm runs in linear time. However, the main advantage is that a differential precondition checker can be placed in a library and reused in refactoring tools for many different languages; the core algorithm can be implemented in a way that is completely language independent. We have implemented a differential precondition checker and used it in refactoring tools for Fortran (Photran), PHP, and BC.**

***Keywords*-program representation; refactoring**

I. Introduction

What makes writing a new refactoring tool hard? What are the parts of such a tool? One part is the user interface; refactoring is interactive and requires a good UI. But IDEs like Eclipse provide a good framework for building a UI for a refactoring tool, and most of the UI for a new refactoring tool can be reused from other tools. Another part is the parser and the general language infrastructure. People have tried to reuse the infrastructure from compilers and other tools with mixed results, but our previous work [1] shows that it is possible to generate an infrastructure that is perfectly suited for refactoring, so this is a solved research problem, too. The remaining parts are the refactorings themselves. Automated refactorings have two parts: the transformation—the change made to the user's source code—and a set of *preconditions* which ensure that the transformation will produce a program that compiles and executes with the same behavior as the original program. Authors of refactoring tools agree that precondition checking is much harder than writing the program transformations.

This paper shows how to construct a reusable, generic precondition checker which can be placed in a library and reused in refactoring tools for many different languages. This makes it easier to implement a refactoring tool for a new language.

We call our technique for checking preconditions *differential precondition checking.* A differential precondition checker builds a *semantic model* of the program prior to transformation, simulates the transformation, performs semantic checks on the modified program, computes a semantic model of the modified program, and then looks for differences between the two semantic models. The refactoring indicates what differences are expected; if the actual differences in the semantic models are all expected, then the transformation is considered to be behavior preserving. The changes are applied to the user's code only after the differential precondition checker has determined that the transformation is behavior preserving.

This technique is simple, practical, and minimalistic. It does not guarantee soundness, and it is *not* a general method for testing program equivalence. Rather, it is designed to be straightforward, fast, scalable, and just expressive enough to implement preconditions for the most common refactorings. Most importantly, the core algorithm can be implemented in a way that is completely language independent, so it can be optimized, placed in a library, and reused in refactoring tools for many different languages.

This paper makes five contributions. (Relevant section numbers are noted parenthetically.)

1) It characterizes preconditions as guaranteeing *input validity, compilability,* and *preservation* (§III).
2) It introduces the concept of *differential precondition checking* (§III) and shows how it can simplify precondition checking by eliminating compilability and preservation preconditions (§V).
3) It observes that semantic relationships between the modified and unmodified parts of the program tend to be the most important and, based on this observation, proposes a very concise method for refactorings to specify their preservation requirements (§V).
4) It describes how the main component of a differential precondition checker (called a *preservation analysis)* can be implemented in a way that is both fast and language independent (§VII).
5) It provides an evaluation of the technique (§VIII), considering its successful application to 18 refactorings and its implementation in refactoring tools for Fortran (Photran), PHP, and BC.

II. Precondition Checking

In most tools, each refactoring has its own set of preconditions. These are tested first, and the transformation proceeds only if they pass. Unfortunately, designing a sufficient set of preconditions for a new refactoring is extremely difficult. The author of the refactoring must exhaustively consider every feature in the target language and somehow guarantee that the transformation is incapable of producing an error. Consider Java: Even a "simple" refactoring like Rename must consider naming conflicts, namespaces, qualifiers, shadowing, reserved words, inheritance, overriding, overloading, constructors, visibility, inner classes, reflection, externally-visible names, and "special" names such as `main`.

One promising alternative to traditional precondition checking is to analyze the program *after* it has been transformed, comparing it to the original program to determine whether or not the transformation preserved behavior. This has been used for some dependence-based compiler transformations (e.g., a *fusion preventing dependence* [2, p. 258] is most easily detected after transformation), but researchers have applied it to refactoring tools only recently. Although this technique is not yet used in any commercial tools, research indicates that it tends to make automated refactorings simpler and more robust [3].

So, how can a refactoring tool analyze a program after transformation? Refactorings preserve certain relationships in the source program. The Rename refactoring preserves a name binding relationship: It ensures that every identifier refers to the "same" declaration before and after transformation. Extract Method and Extract Local Variable preserve control flow and def-use chains at the extraction site. As we will see later in this paper, Pull Up Method preserves a name binding relationship, as well as a relationship between classes and methods they override. In our experience, the most common refactorings preserve invariant relationships related to name bindings, inheritance, overriding, control flow, and def-use chains. Analyzing a program after transformation means ensuring that these invariant relationships are preserved across the transformation.

Schäfer et al. have suggested one way to refactor using invariants like these. To implement a Rename refactoring for Java, they stored the original name bindings, changed names, then checked the resulting bindings, adding qualifiers as necessary to guarantee that the name bindings would resolve identically after the transformation was complete [4]. They used a similar approach to implement Extract Method: They stored the original control flow, performed the transformation, then added control flow constructs as necessary to restore the original flow [5]. They have applied this approach to many other refactorings as well [3, 6]. In short, their approach maintains invariants *by construction*—i.e., while performing the transformation, the refactoring checks the invariant and, if possible, adjusts its behavior to preserve it.

The approach taken in this paper is based on some of the same ideas as that of Schäfer et al., but there is a substantial difference in *how* we perform the preservation check. The main difference is that our technique, when implemented appropriately, is language independent; the mechanism for specifying preservation requirements and the algorithm for performing the preservation analysis are the same, regardless of what refactoring is being checked and regardless of what language is being refactored. This means that, unlike the approach of Schäfer et al., our preservation analysis can be implemented in a library and reused verbatim in refactoring tools for many different languages.

III. Differential Precondition Checking

Preconditions determine the conditions under which the program transformation will preserve behavior. Logically, this means that they guarantee three properties:

1) *Input validity.* All input from the user is legal; it is possible to apply the transformation to the given program with the given inputs.
2) *Compilability.* If the transformation is performed, the resulting program will compile; it will meet all the syntactic and semantic requirements of the target language.
3) *Preservation.* If the transformation is performed and the resulting program is compiled and executed, it will exhibit the same runtime behavior as the untransformed program.

Clearly, input validation needs to be performed before the program is transformed, since it may not even be possible to perform a transformation if the user provides invalid input. But compilability is actually easier to determine *after* transformation; essentially, it means running the program through a compiler front end. It turns out that preservation can often be checked *a posteriori* as well.

When *differential precondition checking* is employed, refactorings proceed as follows:

1) Analyze source code and produce a program representation.
2) Construct a *semantic model,* called the *initial model.*
3) Validate user input.
4) Simulate modifying source code, and construct a new program representation. Detect compilability errors, and if appropriate, abandon the refactoring.
5) Construct a semantic model from this new program representation. This is the *derivative model.*
6) Perform a *preservation analysis* by comparing the derivative model with the initial model.
7) If the preservation analysis succeeds, modify the user's source code. Otherwise, abandon the refactoring.

What distinguishes differential precondition checking is how it ensures compilability and preservation. These topics will be discussed in detail in Sections IV and V, respectively. It ensures compilability by performing essentially the same checks that a compiler front end would perform. It ensures behavior preservation by building *semantic models* of the program before and after it is transformed. The refactoring informs the differential precondition checker of what kinds of semantic differences are expected; the checker ensures that the actual differences in the semantic models are all expected differences—hence the name *differential* precondition checking.[1]

Note that a differential precondition checker contrasts the program's semantic model *after* transformation with its semantic model *before* transformation. This is different from program metamorphosis systems [7], which provide an "expected" semantic model and then determine whether the transformed program's semantic model is equivalent to the expected model. As we will see in §§V-D–V-F, the mechanism for specifying expected differences in a differential precondition checker is fairly coarse-grained; it does not uniquely characterize the semantics of a particular transformed program but rather identifies, in general, how a refactoring is expected to affect programs' semantics.

IV. Checking Compilability

Checking for compilability means ensuring that the refactored program does not contain any syntactic or semantic errors, i.e., that it is a legal program in the target language. These errors would usually be detected by the compiler's front end. Typically, these check constraints like "no two local variables in the same scope shall have the same name" and "a class shall not inherit from itself."

When differential precondition checking is employed, these checks are performed in Step 4 (above), and they are used *in lieu of traditional precondition checks.* For example, a refactoring renaming a local variable A to B would not explicitly test for a conflicting local variable named B; instead, it would simply change the declaration of A to B, and, if this resulted in a conflict, it would be detected by the compilability check.

In fact, most refactoring tools already contain most of the infrastructure needed to check for compilability. It is virtually impossible to perform any complicated refactorings without a parser, abstract syntax tree (AST), and name binding information (symbol tables). A type checker is usually needed to resolve name bindings for members of record types, as well as for refactorings like Extract Local Variable. So, refactoring tools generally contain (most of) a compiler front end. Steps 1 and 4 (above) involve running source code through this front end. So checking for compilability in Step 4 is natural.

The literature contains fairly compelling evidence for including a compilability check in a refactoring tool. Compilability checking subsumes some highly nontrivial preconditions—preconditions that developers have "missed" in traditional refactoring implementations. Verbaere et al. [8] identify a bug in several tools' Extract Method refactorings in which the extracted method may return the value of a variable which has not been assigned—a problem which will be identified by a compilability check. Schäfer et al. [4] describe a bug in Eclipse JDT's Rename refactoring which amounts to a failure to preserve name bindings. Daniel et al. [9] reported 21 bugs on Eclipse JDT and 24 on NetBeans. Of the 21 Eclipse bugs, 19 would have been caught by a compilability check. Seven of these identified missing preconditions;[2] the others were actually errors in the transformation that manifested as compilation errors.

Compilability checking also serves as a sanity check. In the presence of a buggy or incomplete transformation, it analyzes what the transformation *actually did,* not what it was *supposed to do.* If the code will not compile after refactoring, the transformation almost certainly did something wrong, and the user should be notified.

V. Checking Preservation

Compilability checking is important but simple. Checking for preservation is more challenging. It involves choosing an appropriate semantic model and finding a preservation analysis algorithm that balances speed, correctness, and generality. In this section, we will use a *program graph* as the semantic model. In Section VII, we will use a slightly different semantic model based on the same ideas.

In the remainder of this section, we will discuss what program graphs are (§V-A) and how they can be used as an analysis representation for a refactoring tool (§V-B). Then, we will discuss what *preservation* means in the context of a program graph (§V-C) and how it can be used instead of traditional precondition checks, using Safe Delete and Pull Up Method as examples (§§V-D–V-F). The discussion here is conceptual in nature; a more detailed, formal treatment will appear in the first author's dissertation [10].

A. Program Graphs

One program representation which has enjoyed success in the refactoring literature [8, 11] is called a program graph. A *program graph* "may be viewed, in broad lines, as an abstract syntax tree augmented by extra edges" [11, p. 253]. These "extra edges"—which we will call *semantic edges*—represent semantic information, such as name bindings, control flow, inheritance relationships, and so forth. Alternatively, one might think of a program graph as an AST with the graph structures of a control flow graph, du-chains, etc. superimposed; the nodes of the AST serve as nodes of the various graph structures.

An example of a Java program and a plausible program graph representation are shown in Figure 1. The underlying abstract syntax tree is shown in outline form; the dotted lines are the extra edges that make the AST a program graph. We have shown three types of edges. *Name binding* edges link the use of an identifier to its corresponding declaration. Within the method body, *control flow* edges form the (intraprocedural) control flow graph; the method declaration node is used as the entry block and null as the exit block. Similarly, there are two du-chains, given by *def-use* edges.

Program graphs are appealing because they summarize the "interesting" aspects of both the syntax and semantics of

[1]Why differential "precondition" checking? A refactoring takes user input I and uses it to determine a program transformation $T(I)$. However, a precondition for the *application* of $T(I)$ to the user's source code is that it satisfies the properties of compilability and preservation.

[2]Bugs 177636, 194996, 194997, 195002, 195004, 194005, and 195006

```
class Test2 {
  int field = 0;
  void fun() {
    int i = 0;
    i++;
    field++;
    System.out.println(i);
  }
}
```

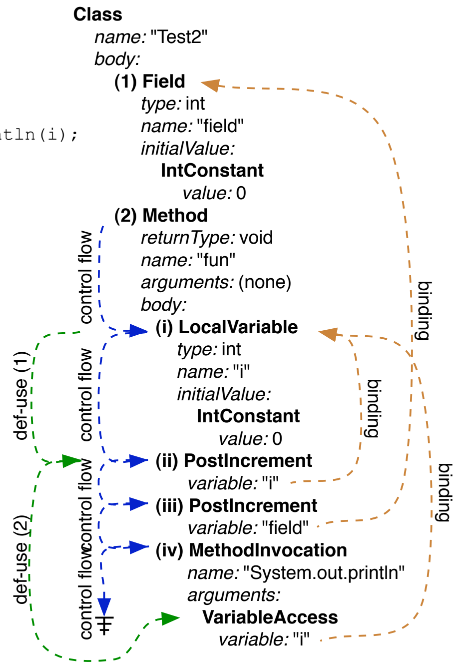


Fig. 1. Example Java program and corresponding program graph

a program in a single representation, obviating the need to maintain a mapping between several distinct representations. Moreover, they are defined abstractly: *the definition of a program graph does not state what types of semantic edges are included.* A person designing a program graph is free to include (or exclude) virtually any type of edge imaginable, depending on the language being refactored and needs of the refactorings that will be implemented. For the 18 refactorings we considered (see §VIII), we found five types of edges to be useful: name binding, control flow, def-use, *override* edges (which link an overriding method to the overridden implementation in a superclass), and *inheritance* edges (which link a class to the concrete methods it inherits from a superclass).

B. Program Graphs and AST Manipulation

In the end, refactoring tools manipulate source code. However, when building a refactoring, it is helpful to think of manipulating the AST instead. Adding a node means inserting source code. Replacing a node means replacing part of the source code. And so on.

This does not change when a program graph is used in a refactoring tool. A program graph is always *derived from* an AST. The content of the AST determines what semantic edges will be superimposed. Semantic edges cannot be manipulated directly; they can only change as a side effect of modifying the AST.

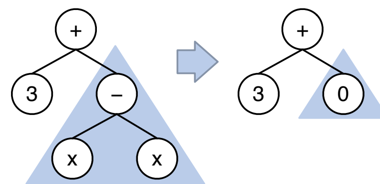
In fact, that observation will serve as the basis of our preservation analysis. When we modify an AST, we will indicate which semantic edges we expect to be preserved and which ones we expect to change. Then, after the source code has been modified, we will determine what semantic edges were actually preserved and compare this with our expectations.

C. Preservation in Program Graphs

This raises a question: What does it mean for a semantic edge to be "preserved" when an AST is modified?

We would like to say: If both the modified and unmodified ASTs contain an edge with the same type and the same endpoints, that edge has been preserved. Unfortunately, it is not clear what the "same" endpoints are, since the AST has been modified, and the endpoints are AST nodes.

Consider a refactoring which replaces the expression $x - x$ with the constant 0. When applied to the expression $3+(x-x)$, this corresponds to the following tree transformation.

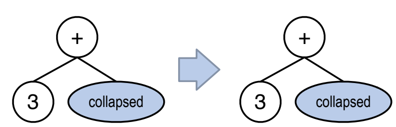


When a subtree is changed (i.e., added, moved, removed, or replaced) in an AST, we will call that the *affected subtree.* A gray triangle surrounds the affected subtrees in the figure above. Using that figure as an example, consider how AST nodes in the unmodified AST correspond with nodes in the modified AST:

- There is an obvious correspondence between AST nodes outside the affected subtrees, since those parts of the AST were unaffected by the transformation.
- As a whole, the affected subtree before the transformation corresponds to the affected subtree after the transformation.
- In general, there is no correspondence between nodes inside the affected subtrees.

Recall that our goal is to determine if a semantic edge has the "same" endpoints before and after an AST transformation. This is easy if an endpoint is outside the affected subtree, or if that endpoint is the affected subtree itself. But if the endpoint is *inside* the affected subtree, we cannot determine exactly which node it should correspond to... except that, if it corresponds to anything, that node would be in the other affected subtree.

Since we cannot determine a correspondence between AST nodes inside the affected subtree, we will *collapse* the affected subtrees into single nodes. This makes the AST before transformation isomorphic to the AST after transformation.



Now, suppose we have superimposed semantic edges to form a program graph. When we collapse the affected subtree to a single node, we will also need to adjust the endpoints of the semantic edges accordingly:

- When an affected subtree is collapsed to a single node, if any semantic edges have an endpoint inside the affected subtree, that endpoint will instead point to the collapsed node.

Note, in particular, that if an edge has *both* endpoints inside the affected subtree, it will become a self-loop on the collapsed node. Also, note that a program graph is not a multigraph: If several edges have the same types and endpoints in the collapsed graph, they will be merged into a single edge.

Collapsing the affected subtree in a program graph actually has a fairly intuitive interpretation: If we replace one subtree with a different subtree that supposedly does the same thing, then the new subtree should interface with its surroundings in (mostly) the same way that the old subtree did. That is, all of the edges that extended into the old subtree should also extend into the new subtree, and all of the edges that emanated from the old subtree should also emanate from the new subtree. There may be some differences within the affected subtree, but the "interface" with the rest of the AST stays the same.

In some cases, we will find it helpful to replace one subtree with *several* subtrees (or, conversely, to replace several subtrees with one). For example, Encapsulate Variable removes a public variable, replacing it with a private variable, an accessor method, and a mutator method. In other words, we are modifying several subtrees at the same time. In these cases, we have an *affected forest* rather than a single affected subtree. However, the preservation rule is essentially the same: All of subtrees in the affected forest are collapsed into a single unit. So if an edge extended into some part of the affected forest before transformation, it should also extend into some part of the affected forest after transformation. In the case of Encapsulate Variable, this correctly models the idea that every name binding that pointed to the original (public) variable should, instead, point to either the new (private) variable, the accessor method, or the mutator method. (We will see an example of an affected forest when we discuss Pull Up Method in §V-F.)

D. *Specifying Preservation Requirements*

Now that we have established how to determine whether a semantic edge has been preserved across a transformation, we turn to a different question: How can we express which semantic edges we expect to be preserved and which ones we expect to change?

1) Edge Classifications: From the above description, we can see that whether we want to preserve an edge depends on its type as well as its relationship to the affected subtree. Therefore, it is helpful to classify every semantic edge as either **internal** (both endpoints of the semantic edge occur within the affected subtree), **external** (neither endpoint occurs within the affected subtree), **incoming** (the head of the semantic edge is outside the affected subtree but the tail is inside it), or **outgoing** (the head is inside the affected subtree and the tail is outside it).

2) Notation: Now, we can establish some notation. To indicate what edges we (do not) expect to preserve, we must indicate three things:

1) *The type(s) of edges to preserve.* We will use the letters N, C, D, O, and I to denote name binding, control flow, def-use, override, and inheritance edges, respectively. (Note, however, that program graphs may contain other types of edges as well, depending on the language being refactored and the requirements of the refactorings being implemented.)
2) *The classification(s) of edges to preserve.* We will use $\leftarrow$, $\rightarrow$, $\circlearrowleft$, and $\times$ to indicate incoming, outgoing, internal, and external edges, respectively. We will use $\leftrightarrow$ as a shorthand for describing both incoming and outgoing edges.
3) *Whether we expect the transformation to introduce additional edges or remove existing edges.* If additional edges may be introduced, we denote this using the symbol $\supseteq$ (i.e., the transformed program will contain a superset of the original edges). If existing edges may be eliminated, we denote this by $\subseteq$. If edges may be both added and removed, then we cannot effectively test for preservation, so those edges will be ignored; we indicate this using the symbol $\gtreqqless$. Otherwise, we expect a 1–1 correspondence between edges, i.e., edges should be preserved exactly. We indicate this by $=$.

E. *Example: Safe Delete (Fortran 95)*

To make these ideas more concrete, let us first consider a Safe Delete refactoring for Fortran which deletes an unreferenced internal subprogram.[3]

The traditional version of this refactoring has only one precondition: There must be no references to the subprogram except for recursive references in its definition.

What would the differential version look like? To determine its preservation requirements, it is often useful to fill out a table like the following (note that Fortran 95 is not object oriented and thus cannot have O- or I-edges):

	N	C	D
$\leftarrow$	$=$	$=$	$=$
$\rightarrow$	$\subseteq$	$=$	$=$
$\circlearrowleft$	$\subseteq$	$\subseteq$	$\subseteq$
$\times$	$=$	$=$	$=$

When a subprogram is deleted, all of the semantic edges inside the deleted subroutine will, of course, disappear, and if the subprogram references any names defined elsewhere (e.g., other subprograms), those edges will disappear. Otherwise, no semantic edges should change.

Notating preservation requirements in tabular form is somewhat space-consuming, since in practice most cells contain $=$. Therefore, we will use a more compact notation. For each edge type, we will use subscripts to indicate which cells are *not* $=$,

[3] A slightly more complete and much more detailed specification for this refactoring is given in the technical report [12] described in the Evaluation section of this paper.

i.e., what edges should *not* be preserved exactly. If all cells are $=$, we will omit the subscript. Using this notation, the preservation requirements in the above table would be notated $N_{\overset{\rightarrow}{\subseteq}} C_{\overset{\circlearrowleft}{\subseteq}} D_{\overset{\circlearrowleft}{\subseteq}}$.

Thus, we can describe the differential version of this refactoring in a single step: *Delete the subprogram definition, ensuring preservation according to the rule* $N_{\overset{\rightarrow}{\subseteq}} C_{\overset{\circlearrowleft}{\subseteq}} D_{\overset{\circlearrowleft}{\subseteq}}$.

F. Example: Pull Up Method (PHP 5)

For a more interesting example, let us consider a Pull Up Method refactoring for PHP 5, which moves a concrete method definition from a class C into its immediate superclass C'.[4] First, consider the traditional version.

Preconditions.

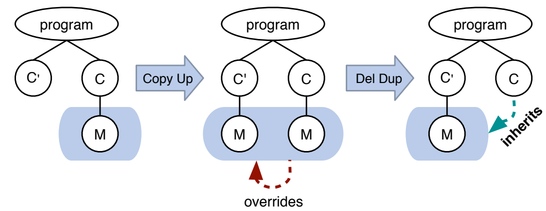
1) *A method with the same name as M must not already exist in C'.* If M were pulled up, there would be two methods with the same name, or M would need to replace the existing method.
2) *If there are any references to M (excluding recursive references inside M itself), then M must not have private visibility.* If it were moved up, its visibility would need to be increased in order for these references to be preserved.
3) *M must not contain any references to the built-in constants* `self` *or* `__CLASS__`. If it were moved up, these would refer to C' instead of C. (Note that PHP contains both `self` and `$this`: The former refers to the enclosing class, while the latter refers to the *this* object.)
4) *M must not contain any references to private members of C (except for M itself, if it is private).* Private members of C would no longer be accessible to M if it were pulled up.
5) *M must not contain any references to members of C for which there is a similarly-named private member of C'.* These references would refer to the private members of C' if the method were pulled up.
6) *If M overrides another concrete method, no subclasses of C' may inherit the overridden method.* Pulling up M would cause these classes to inherit the pulled up method instead.
7) *The user should be warned if M overrides another concrete method.* If M were pulled up into C', then M would replace the method that C' inherited, changing the behavior of that method in objects of type C', although the user might intend this since he explicitly chose to pull up M into C'.

Transformation. Move M from C to C', replacing all occurrences of `parent` in M with `self`.

Now, consider the differential version. The transformation can be expressed as the composition of two smaller refactorings:

1) *Copy Up Method.* Using preservation rule $N O_{\overset{\leftarrow}{\supseteq}\overset{\circlearrowleft}{\supseteq}} I_{\overset{\times}{\subseteq}}$, copy the method definition from C to C', replacing all occurrences of `parent` in M with `self`.
2) *Delete Overriding Duplicate.* Remove the original method definition from C, with rule $N O_{\overset{\circlearrowleft}{\subseteq}} I_{\overset{\leftarrow}{\supseteq}}$.

Pictorially, the process is as follows. The affected forests are highlighted in gray.



When the method is copied from C to C', an internal override edge will be introduced, as may incoming override edges (if another class will override the pulled up method), hence the rule $O_{\overset{\leftarrow}{\supseteq}\overset{\circlearrowleft}{\supseteq}}$. If the method being pulled up overrides a method inherited from the immediate superclass, then an inheritance edge will be lost, hence $I_{\overset{\times}{\subseteq}}$. However, the new method in C' should not be inherited by any subclasses, and all identifiers should bind to the same names they did when the method was contained in C, so no other inheritance or name binding edges are expected to change. Once we have established that no subclasses will accidentally inherit the pulled up method, we can delete the original method from C. This will remove the override edge introduced in the previous step, and C will inherit the pulled up method, so the preservation rule is $N O_{\overset{\circlearrowleft}{\subseteq}} I_{\overset{\leftarrow}{\supseteq}}$.

Now, consider how the differential version of this refactoring satisfies all of the traditional version's preconditions. Precondition 1 would be caught by a compilability check. Preconditions 2–5 are simply preserving name bindings. A program that failed Precondition 6 would introduce an incoming inheritance edge. If a program failed Precondition 7, an outgoing inheritance edge from C' would vanish.

For the differential version, we redefined Pull Up Method as the *composition* of two smaller refactorings. Whenever this is possible, it is generally a good idea: It allows preservation rules to be specified at a finer granularity; the smaller refactorings are often useful in their own right; and, perhaps most importantly, simpler refactorings are easier to implement, easier to test, and therefore more likely to be correct.

VI. The Preservation Analysis Algorithm

If one understands what a program graph is, and what the preservation rules mean, the preservation analysis algorithm is straightforward. A program graph becomes an abstract data type with

Sorts: ProgramGraph, Edge, Type

Operations:

$$\begin{aligned} \text{getAllEdges} &: \text{ProgramGraph} \rightarrow \text{finite set of Edge} \\ \text{classify} &: \text{Edge} \rightarrow \{\leftarrow, \rightarrow, \circlearrowleft, \times\} \\ \text{type} &: \text{Edge} \rightarrow \text{Type} \\ \text{equiv} &: \text{Edge} \times \text{Edge} \rightarrow \{\text{TRUE}, \text{FALSE}\}. \end{aligned}$$

[4] Again, a more complete and detailed specification is available [12].

The *equiv* operation determines whether two edges—one in the original program graph and one in the transformed program graph—are equivalent, i.e., if the edge was preserved. For simplicity, we have left this underspecified, although its intent should be clear from the previous section. Now, preservation is determined by the following algorithm.

Input: P : ProgramGraph *(Original program)*
P' : ProgramGraph *(Transformed program)*
$rule$: Type $\times \{\leftarrow, \rightarrow, \circlearrowleft, \times\} \rightarrow \{=, \subseteq, \supseteq, \supsetneq\}$

Output: PASS or FAIL

let $E :=$ **getAllEdges**(P)
let $E' :=$ **getAllEdges**(P')
for each Edge $e \in E$
  if *rule*(**type**(e), **classify**(e)) is $\supseteq$ or $=$
    but $\nexists\ e' \in E'$ s.t. **equiv**(e, e') = TRUE, then
      FAIL
for each Edge $e' \in E'$
  if **rule**(**type**(e'), **classify**(e')) is $\subseteq$ or $=$
    but $\nexists\ e \in E$ s.t. **equiv**(e, e') = TRUE, then
      FAIL
otherwise, PASS

VII. Analysis with Textual Intervals

The key to an efficient implementation is being able to determine, for a particular edge, whether an equivalent edge exists in the transformed program. If this can be done in $O(1)$ time, then the above algorithm's execution time is linear in the number of edges in the two program graphs. In this section, we will sketch one way to do this (which also makes the implementation language independent).

The ASTs in refactoring tools tend to model source code very closely. This means that they tend to exhibit a very useful property: Every node in an AST corresponds to a particular textual region of the source code, *and this textual region can be mapped back to a unique AST node.* Consider the program graph from Figure 1. The source code is 115 characters long. The *Class* AST node corresponds to the entire source code—the characters at offsets 0 through 114, inclusive, or the interval $[0, 114]$. The field declaration `int field = 0;` corresponds to the interval $[14, 30]$. The post-increment `field++;` becomes $[70, 82]$.

Since AST nodes can be represented as intervals, we can use these intervals to describe the semantic edges of a program graph. For example, the name binding edge from the post-increment to the field declaration becomes $[70, 82] \triangleright_B [14, 30]$. (The interval representation of the program graph in Figure 1 is shown in Figure 2(a).)

During a refactoring transformation, it is possible to track what regions of the original source code are deleted or replaced, as well as where new source code is inserted. These textual regions are contained in the affected forests. Since we know exactly how many characters were added or deleted at what positions, then for any character *outside* these regions, it is possible to determine exactly where that character should occur in the transformed program. Suppose we have a (partial) function $newOffset(n)$ that can determine this value, for a given character offset n in the original program.

Now, suppose we take each edge of the derivative model, and if an endpoint is contained in the affected forest, we replace that interval with $*$. We will call the result the *normalized derivative model.* Then, we can take each edge of the initial program graph and use the *newOffset* function to determine the equivalent edge in the normalized derivative model, likewise replacing endpoints in the affected forest with $*$. We will call this the *normalized initial model.*

If the normalized models are stored as sets (eliminating duplicate edges), then each edge in the initial model corresponds to exactly one edge in the normalized initial model, and each edge in the derivative model corresponds to exactly one edge in the normalized derivative model. Now, an edge in the initial model is equivalent to an edge in the derivative model (in the notation of the previous section, $equiv(e, e')$ if, and only if, their corresponding edges in the initialized models are *equal.* By storing the edges of the normalized models in appropriate data structures (e.g., hash sets), we can determine in $O(1)$ time if a particular edge occurs in either model.

An example is shown in Figure 2. Suppose, in the Java program in Figure 1, we attempt to rename the field declaration from `field` to `i`. The transformation is simple: replace the five characters `field` at offsets 20–24 (the declaration) and 74–78 (the reference) with the one-character string `i`. Since four characters are deleted in each case,

$$newOffset(n) = \begin{cases} n & \text{if } n \leq 19 \\ n - 4 & \text{if } 25 \leq n \leq 73 \\ n - 8 & \text{if } 79 \leq n. \end{cases}$$

The affected forest consists of the field declaration and the second post-increment (initial intervals $[14, 30]$ and $[70, 82]$, derivative intervals $[14, 26]$ and $[66, 74]$). Since `field++` changes to `i++`, the name binding edge for the field reference disappears and becomes a reference to the local variable `i` in the derivative model. Also, a new def-use chain is introduced. Since the renaming transformation would not preserve name bindings (or du-chains, for that matter), it should not be allowed to proceed.

Implementing the preservation analysis using textual intervals, rather than directly on the program graph, has a number of advantages. It allows the preservation analysis to be highly decoupled from the refactoring tool's program representation, which makes it more easily reusable. It is fairly space-efficient, since semantic edges are represented as tuples of integers. Also, there is a fairly natural way to display errors: highlight the affected region(s) of the source code.

VIII. Evaluation

In previous sections, we illustrated differential precondition checking using Safe Delete, Pull Up Method, and Rename as illustrative examples. We also sketched a linear-time algorithm

Initial Model (a)	**Norm. Initial** (b)	**Norm. Deriv.** (c)	**Deriv. Model** (d)
$[74, 78] \rhd_B [14, 30]$	$* \rhd_B *$		
$[65, 65] \rhd_B [46, 60]$	$[61, 61] \rhd_B [42, 56]$	$[61, 61] \rhd_B [42, 56]$	$[61, 61] \rhd_B [42, 56]$
		$* \rhd_B [42, 56]$	$[70, 70] \rhd_B [42, 56]$
$[106, 106] \rhd_B [46, 60]$	$[98, 98] \rhd_B [42, 56]$	$[98, 98] \rhd_B [42, 56]$	$[98, 98] \rhd_B [42, 56]$
$[31, 113] \rhd_C [46, 60]$	$[27, 105] \rhd_C [42, 56]$	$[27, 105] \rhd_C [42, 56]$	$[27, 105] \rhd_C [42, 56]$
$[46, 60] \rhd_C [61, 69]$	$[42, 56] \rhd_C [57, 65]$	$[42, 56] \rhd_C [57, 65]$	$[42, 56] \rhd_C [57, 65]$
$[61, 69] \rhd_C [70, 82]$	$[57, 65] \rhd_C *$	$[57, 65] \rhd_C *$	$[57, 65] \rhd_C [66, 74]$
$[70, 82] \rhd_C [83, 109]$	$* \rhd_C [75, 101]$	$* \rhd_C [75, 101]$	$[66, 74] \rhd_C [75, 101]$
$[83, 109] \rhd_C [-1, -1]$	$[75, 101] \rhd_C [-1, -1]$	$[75, 101] \rhd_C [-1, -1]$	$[75, 101] \rhd_C [-1, -1]$
$[46, 60] \rhd_D [61, 69]$	$[42, 56] \rhd_D [57, 65]$	$[42, 56] \rhd_D [57, 65]$	$[42, 56] \rhd_D [57, 65]$
$[61, 69] \rhd_D [106, 106]$	$[57, 65] \rhd_D [98, 98]$	$[57, 65] \rhd_D [66, 74]$	$[57, 65] \rhd_D [66, 74]$
		$* \rhd_D [98, 98]$	$[66, 74] \rhd_D [98, 98]$

Fig. 2. Textual interval models of the program graph from Figure 1, when `field` is renamed to `i`

for performing the preservation analysis and argued for its language independence. But is this technique effective in practice? We will focus on two questions:

- Q1. *Expressivity.* Are the preservation specifications in §III sufficient to implement the most common automated refactorings?
- Q2. *Performance.* When preconditions are checked differentially, what are the performance bottlenecks? How does the performance compare to a traditional implementation?

For our evaluation, we implemented a differential precondition checker which we reused in three refactoring tools: (1) Photran, a popular Eclipse-based IDE and refactoring tool for Fortran; (2) a prototype refactoring tool for PHP 5; and (3) a similar prototype for BC.

A. Q1: Expressivity

To effectively answer question Q1, we must first identify what the most common automated refactorings are. The best empirical data so far are reported by Murphy-Hill et al. [13]. Table I shows several of the top refactorings; the *Eclipse JDT* column shows the popularity of each refactoring in the Eclipse JDT according to [13, Table 1, "Everyone"]. For comparison, we have also listed the availability of these refactorings in other popular refactoring tools for various languages.

We selected 18 refactorings (see Table II): 7 for Fortran, 9 for BC, and 4 for PHP. Five of these refactorings are Fortran or BC analogs of the five most frequently-used in Eclipse JDT. Nine others are support refactorings, necessitated by decomposition. The remaining refactorings were chosen for other reasons. Add Empty Subprogram and Safe Delete were the first to be implemented; they helped shape and test our implementation. Introduce Implicit None preserves name bindings in an "interesting" way. Pull Up Method required us to model method overriding and other class hierarchy issues in program graphs.

It is worth noting that many popular IDEs provide fewer than 10 refactorings, including Apple Xcode (8 refactorings), Microsoft Visual Studio (6), and Zend Studio (4). So while generality is important and desirable (certainly, a technique that works for 18 refactorings will apply to many others), expediting and improving the implementation of a few common refactorings is equally important, perhaps more so.

TABLE I
AUTOMATED REFACTORINGS IN POPULAR TOOLS.

Refactoring	**Eclipse JDT** (Rank)	**IntelliJ IDEA**[1]	**IntelliJ ReSharper**[2]	**MS Visual Studio**[3]	**Eclipse CDT**	**Visual Assist X**[4]	**Apple Xcode**[5]	**Zend Studio**[6]
Rename	1	●	●	●	●	●	●	●
Extract Variable	2	●	●	○	●	○	○	●
Move	3	●	●	○	○	○	○	●
Extract Method	4	●	●	●	●	●	●	●
Change Signature	5	●	●	●	○	●	○	○
Pull Up Method	11	●	●	○	○	●	●	○

Legend: *● Included* *○ Not Included*

[1] http://www.jetbrains.com/idea/features/refactoring.html
[2] http://www.jetbrains.com/resharper/features/code_refactoring.html
[3] http://msdn.microsoft.com/en-us/library/719exd8s.aspx
[4] http://www.wholetomato.com/products/featureRefactoring.asp
[5] http://developer.apple.com/mac/library/documentation/DeveloperTools/Conceptual/XcodeWorkspace/150-Refactoring/refactoring.html
[6] http://www.zend.com/en/products/studio/features#refactor

TABLE II
REFACTORINGS EVALUATED.

Fortran	1. Rename	**BC**	10. Extract Local Variable
	2. Move		11. *Add Local Variable*
	3. *Introduce USE*		12. *Introduce Block*
	4. Change Function Signature		13. *Insert Assignment*
	5. Introduce IMPLICIT NONE		14. *Move Expression*
	6. Add Empty Subprogram		15. Extract Function
	7. Safe Delete		16. *Add Empty Function*
PHP	8. Pull Up Method		17. *Populate Function*
	9. *Copy Up Method*		18. *Replace Expression*

We wrote detailed specifications of all 18 refactorings in a technical report [12]. Each specification describes both the traditional and the differential version of the refactoring, both at a level of detail sufficient to serve as a basis for implementation. (Several undergraduate interns working on Photran implemented refactorings based on our specifications.) The style of the specifications is similar to the Pull Up Method example from §III but more precise. For example, the Fortran refactoring specifications use the same terminology as the Fortran 95 ISO standard.

We divided refactorings among the three languages as follows. For all of the refactorings that rely primarily on name

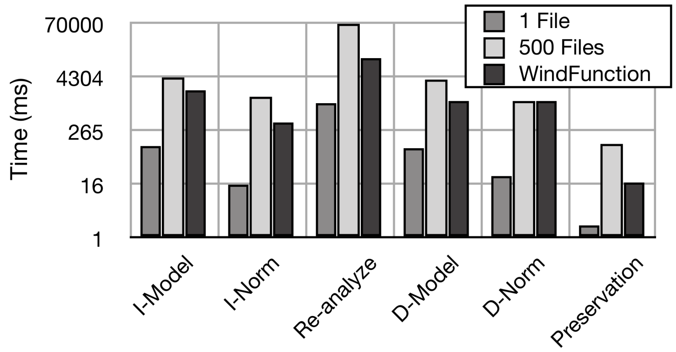


Fig. 3. Rename performance measurements

binding preservation, we targeted Fortran, since it has the most complicated name binding rules. We targeted flow-based refactorings for BC: It contains functions, scalar and array variables, and all of the usual control flow constructs, but it is a much smaller and simpler language than either Fortran or PHP. This kept the specifications of these (usually complex) refactorings to a manageable size without sacrificing any of the essential preconditions. The one object-oriented refactoring targeted PHP 5.

We implemented a differential precondition checker (following §VII) and used it to implement differential refactorings in the three refactoring tools, following our detailed specifications. For BC and PHP, we implemented refactorings as listed in Table II. Since there are no comparable refactoring tools for these languages, we could not perform differential testing. However, we ported several relevant unit tests from the Eclipse CDT and JDT, as well as two informal refactoring benchmarks [14, 15]. For Fortran, we implemented differential versions of Rename, Introduce Implicit None, Add Empty Subprogram, and Safe Delete. Photran included traditional versions of these refactorings, with fairly extensive unit tests, so we were able to reuse the existing test cases to test the differential implementations.

B. Q2: Performance

Since a differential precondition checker's performance depends on the speed of the language-specific front end, as well what refactoring is being performed and what program is being refactored, it is difficult to make any broad claims about performance. In our experience, when a refactoring affects only one or two files in a typical application, the amount of time devoted to precondition checking is negligible. Most of the refactorings we implemented fall into this category. Performance becomes a concern only at scale, e.g., when a refactoring potentially affects every file in a project. We will use Photran's Rename refactoring as an illustrative example. Rename is the most expensive of the refactorings we implemented, since it can potentially change name bindings in every file in the program, it often makes many changes to a single file, and computing name bindings involves accessing a index/cross-reference database.

Figure 3 shows performance measurements[5] for the Rename refactoring on three Fortran programs. Two are examples intended to test scalability: "1 File" is a project with 500 subroutine definitions in a single file, while "500 Files" contains 1 subroutine in each of 500 files. "WindFunction" shows the results of renaming of the wind function in an atmospheric dispersion simulation (a production Fortran program consisting of about 53,000 LOC in 29 files, four of which were ultimately affected by the refactoring). From left to right, the performance measurements represent creation of the initial interval model, normalization of this model, running the front end to reanalyze the modified code, construction of the derivative interval model, normalization of this model, and, finally, the preservation analysis.

Note the logarithmic scale on the y-axis: In all three cases, the performance bottleneck was, by far, the *Re-analyze* measurement—i.e., the amount of time taken for the front end to analyze the modified program and recompute name bindings. This was generally true for other refactorings as well. It is not particularly surprising: When an identifier in one file can refer to an entity in another file, computing name bindings involves populating and accessing a cross-reference database.

In our experience, differential precondition checking is not as fast as traditional precondition checking, but its speed is acceptable. After all, the amount of time it requires is essentially the amount of time the front end takes to analyze the affected files. In the WindFunction example, differential precondition checking took about 9 seconds, while traditional checks took just over 1 second. Photran's name binding analysis is not particularly fast, and its traditional Rename refactoring has been heavily optimized over the course of six years to compensate. In contrast, for the refactorings which made localized changes to only one or two files, the time devoted to precondition checking was unnoticeable.

IX. Limitations

Our preservation analysis has two notable limitations.

First, it *assumes* that, if a replacement subtree interfaces with the rest of the AST in an expected way, it is a valid substitute for the original subtree. It is the refactoring developer's responsibility to ensure that this assumption is appropriate. For example, replacing every instance of the constant 0 with the constant 1 would almost certainly break a program, but our analysis would not detect any problem, since this change would not affect any edges in a typical program graph. However, the refactoring developer should recognize that name bindings, control flow, and du-chains do not model the conditions under which 1 and 0 are interchangeable values.

Second, for our preservation analysis to be effective, the "behavior" to preserve must be modeled by the program graph. There are several cases where this is unlikely to be true, including the following.

[5] The tests were performed on a 2 GHz Intel Core 2 Duo (MacBook), Java 1.6.0_24, with the JVM heap limited to 512 MB.

Interprocedural data flow. One particularly insidious example is illustrated by an Eclipse bug (186253) reported by Daniel et al. [9]. In this bug, Encapsulate Field reorders the fields in a class declaration, causing one field to be initialized incorrectly by accessing the value of an uninitialized field via an accessor method. In theory, this could be detected by a preservation analysis, as it is essentially a failure to preserve du-chains for fields among their initializers. Unfortunately, these would probably not be modeled in a program graph, since doing so would require an interprocedural analysis.

Library replacements, such as replacing primitive `int` values with `AtomicInteger` objects in Java [16], or converting programs to use `ArrayList` instead of `Vector`. Program graphs generally model *language* semantics, not *library* semantics, and therefore are incapable of expressing the invariants that these refactorings maintain.

X. Conclusions & Future Work

In this paper, we classified refactoring preconditions as ensuring input validity, compilability, and behavior preservation, and we proposed a technique for many compilability and preservation preconditions to be checked after transformation in a generic way. We showed that, if essential semantic relationships are treated as edges in a program graph, these edges can be classified based on their relationship to the modified subtree(s). The preservation requirements for common refactorings can be expressed by indicating, for each kind of edge, whether a subset or superset of those edges should be preserved. By exploiting an isomorphism between graph nodes and textual intervals, the preservation checking algorithm can be implemented in a way that is both efficient and language independent. We implemented this technique in a library and applied it to refactorings for Fortran 95, PHP 5, and BC.

Much future work is possible. When differential precondition checking is used, how does it affect the amount of time taken to implement a refactoring? Do refactorings implemented with differential precondition checking tend to have more or fewer bugs than those implemented with traditional precondition checks? Both of these questions will require empirical data from many developers to answer conclusively. What other refactorings can be implemented using the preservation specifications described in this paper? Can a program graph representation be extended to overcome the limitations outlined in the previous section? Can it model C preprocessor directives? Is it useful to extend a differential precondition checker with expensive interprocedural analyses for the purposes of testing but to replace these analyses with cheaper, traditional precondition checks in production? We hope that researchers will address these and other questions about differential precondition checking in the future.

Acknowledgment

This research is part of the Blue Waters sustained-petascale computing project, which is supported by the National Science Foundation (award number OCI 07-25070) and the state of Illinois. Blue Waters is a joint effort of the University of Illinois at Urbana-Champaign, its National Center for Supercomputing Applications, IBM, and the Great Lakes Consortium for Petascale Computation. The authors would like to thank the anonymous reviewers, as well as Rob Bocchino, John Brant, Brett Daniel, Danny Dig, Matthew Fotzler, Milos Gligoric, Vilas Jagannath, Ashley Kasza, Darko Marinov, Stas Negara, and members of the Brett Daniel Software Engineering Seminar for providing invaluable feedback on earlier drafts of this paper.

References

[1] J. L. Overbey and R. E. Johnson, "Generating rewritable abstract syntax trees," in *SLE 2008*, ser. LNCS, vol. 5452, pp. 114–133.

[2] K. Kennedy and J. R. Allen, *Optimizing compilers for modern architectures: a dependence-based approach*. San Francisco: Morgan Kaufmann, 2002.

[3] M. Schäfer and O. de Moor, "Specifying and implementing refactorings," in *SPLASH '10*.

[4] M. Schäfer, T. Ekman, and O. de Moor, "Sound and extensible renaming for Java," in *OOPSLA '08*.

[5] M. Schäfer, M. Verbaere, T. Ekman, and O. de Moor, "Stepping stones over the refactoring rubicon – lightweight language extensions to easily realise refactorings," in *ECOOP '09*.

[6] M. Schäfer, J. Dolby, M. Sridharan, F. Tip, and E. Torlak, "Correct refactoring of concurrent Java code," in *ECOOP '10*.

[7] C. Reichenbach, D. Coughlin, and A. Diwan, "Program metamorphosis," in *ECOOP '09*.

[8] M. Verbaere, R. Ettinger, and O. de Moor, "JunGL: a scripting language for refactoring," in *ICSE'06*.

[9] B. Daniel, D. Dig, K. Garcia, and D. Marinov, "Automated testing of refactoring engines," in *FSE '07*.

[10] J. L. Overbey, "A toolkit for constructing refactoring engines," Ph.D. dissertation, University of Illinois at Urbana-Champaign, 2011.

[11] T. Mens, N. Van Eetvelde, S. Demeyer, and D. Janssens, "Formalizing refactorings with graph transformations," *J. Softw. Maint. Evol.*, vol. 17, no. 4, pp. 247–276, 2005.

[12] J. L. Overbey, M. J. Fotzler, A. J. Kasza, and R. E. Johnson, "A collection of refactoring specifications for Fortran 95, BC, and PHP 5," Tech. Rep. http://jeff.over.bz/papers/2011/tr-refacs.pdf, 2011.

[13] E. Murphy-Hill, C. Parnin, and A. P. Black, "How we refactor, and how we know it," in *ICSE '09*.

[14] "Refactoring benchmarks for extract method," http://c2.com/cgi/wiki?RefactoringBenchmarksFor ExtractMethod.

[15] "Refactoring benchmarks for pull up method," http://c2.com/cgi/wiki?RefactoringBenchmarksFor PullUpMethod.

[16] D. Dig, J. Marrero, and M. D. Ernst, "Refactoring sequential Java code for concurrency via concurrent libraries," in *ICSE '09*, 2009, pp. 397–407.