

# Roles Are Really Great!

Viktor Kuncak, Patrick Lam, and Martin Rinard  
 Laboratory for Computer Science  
 Massachusetts Institute of Technology  
 Cambridge, MA 02139  
 {vkuncak, plam, rinard}@lcs.mit.edu

## ABSTRACT

We present a new role system for specifying changing referencing relationships of heap objects. The role of an object depends, in large part, on its aliasing relationships with other objects, with the role of each object changing as its aliasing relationships change. Roles therefore capture important object and data structure properties and provide useful information about how the actions of the program interact with these properties. Our role system enables the programmer to specify the legal aliasing relationships that define the set of roles that objects may play, the roles of procedure parameters and object fields, and the role changes that procedures perform while manipulating objects. We present an interprocedural, compositional, and context-sensitive role analysis algorithm that verifies that a program respects the role constraints.

## Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Example</b>	<b>2</b>
2.1	Role Definitions . . . . .	2
2.2	Roles and Procedure Interfaces . . . . .	3
<b>3</b>	<b>Abstract Syntax and Semantics of Roles</b>	<b>3</b>
3.1	Heap Representation . . . . .	3
3.2	Role Representation . . . . .	3
3.3	Role Semantics . . . . .	4
<b>4</b>	<b>Role Properties</b>	<b>4</b>
4.1	Formal Properties of Roles . . . . .	5
<b>5</b>	<b>A Programming Model</b>	<b>7</b>
5.1	A Simple Imperative Language . . . . .	7
5.2	Operational Semantics . . . . .	7
5.3	Onstage and Offstage Objects . . . . .	7

5.4	Role Consistency . . . . .	9
5.4.1	Offstage Consistency . . . . .	9
5.4.2	Reference Removal Consistency . . . . .	9
5.4.3	Procedure Call Consistency . . . . .	9
5.4.4	Explicit Role Check . . . . .	9
5.5	Instrumented Semantics . . . . .	10
<b>6</b>	<b>Intraprocedural Role Analysis</b>	<b>10</b>
6.1	Abstraction Relation . . . . .	11
6.2	Transfer Functions . . . . .	12
6.2.1	Expansion . . . . .	13
6.2.2	Contraction . . . . .	15
6.2.3	Symbolic Execution . . . . .	16
6.2.4	Node Check . . . . .	16
<b>7</b>	<b>Interprocedural Role Analysis</b>	<b>17</b>
7.1	Procedure Transfer Relations . . . . .	17
7.1.1	Initial Context . . . . .	17
7.1.2	Procedure Effects . . . . .	19
7.1.3	Semantics of Procedure Effects . . . . .	19
7.2	Verifying Procedure Transfer Relations . . . . .	20
7.2.1	Role Graphs at Procedure Entry . . . . .	20
7.2.2	Verifying Basic Statements . . . . .	20
7.2.3	Verifying Procedure Postconditions . . . . .	21
7.3	Analyzing Call Sites . . . . .	21
7.3.1	Context Matching . . . . .	21
7.3.2	Effect Instantiation . . . . .	22
7.3.3	Role Reconstruction . . . . .	23
<b>8</b>	<b>Extensions</b>	<b>23</b>
8.1	Multislots . . . . .	23
8.2	Cascading Role Changes . . . . .	23
<b>9</b>	<b>Related Work</b>	<b>24</b>
<b>10</b>	<b>Conclusion</b>	<b>25</b>

## 1 Introduction

Types capture important properties of the objects that programs manipulate, increasing both the safety and readability of the program. Traditional type systems capture properties (such as the format of data items stored in the fields of the object) that are invariant over the lifetime of the object. But in many cases, properties that do change are as important

\*This research was supported in part by DARPA Contract F33615-00-C-1692, NSF Grant CCR00-86154, NSF Grant CCR00-63513, and an NSERC graduate scholarship.

as properties that do not. Recognizing the benefit of capturing these changes, researchers have developed systems in which the type of the object changes as the values stored in its fields change or as the program invokes operations on the object [44, 43, 10, 47, 48, 4, 20, 13]. These systems integrate the concept of changing object states into the type system.

The fundamental idea in this paper is that the state of each object also depends on the data structures in which it participates. Our type system therefore captures the referencing relationships that determine this data structure participation. As objects move between data structures, their types change to reflect their changing relationships with other objects. Our system uses *roles* to formalize the concept of a type that depends on the referencing relationships. Each role declaration provides complete aliasing information for each object that plays that role—in addition to specifying roles for the fields of the object, the role declaration also identifies the complete set of references in the heap that refer to the object. In this way roles generalize linear type systems [45, 2, 30] by allowing multiple aliases to be statically tracked, and extend alias types [42, 46] with the ability to specify roles of objects that are the source of aliases.

This approach attacks a key difficulty associated with state-based type systems: the need to ensure that any state change performed using one alias is correctly reflected in the declared types of the other aliases. Because each object's role identifies all of its heap aliases, the analysis can verify the correctness of the role information at all remaining or new heap aliases after an operation changes the referencing relationships.

Roles capture important object and data structure properties, improving both the safety and transparency of the program. For example, roles allow the programmer to express data structure consistency properties (with the properties verified by the role analysis), to improve the precision of procedure interface specifications (by allowing the programmer to specify the role of each parameter), to express precise referencing and interaction behaviors between objects (by specifying verified roles for object fields and aliases), and to express constraints on the coordinated movements of objects between data structures (by using the aliasing information in role definitions to identify legal data structure membership combinations). Roles may also aid program optimization by providing precise aliasing information.

This paper makes the following contributions:

- **Role Concept:** The concept that the state of an object depends on its referencing relationships; specifically, that objects with different heap aliases should be regarded as having different states.
- **Role Definition Language:** It presents a language for defining roles. The programmer can use this language to express data structure invariants and properties such as data structure participation.
- **Programming Model:** It presents a set of role consistency rules. These rules give a programming model for changing the role of an object and the circumstances under which roles can be temporarily violated.
- **Procedure Interface Specification Language:** It presents a language for specifying the initial context and effects of each procedure. The effects summarize

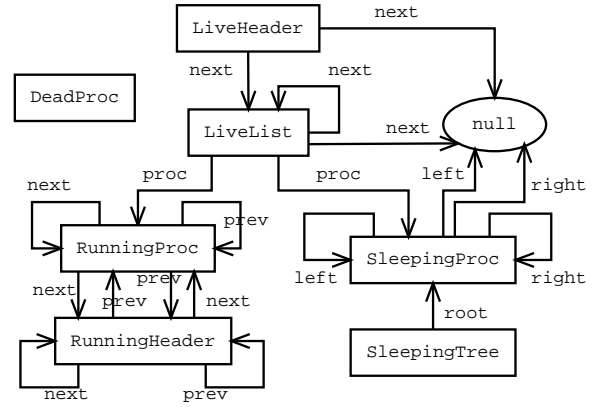


Figure 1: Role Reference Diagram for Scheduler

the actions of the procedure in terms of the references it changes and the regions of the heap that it affects.

- **Role Analysis Algorithm:** It presents an algorithm for verifying that the program respects the constraints given by a set of role definitions and procedure specifications. The algorithm uses a data-flow analysis to infer intermediate referencing relationships between objects, allowing the programmer to focus on role changes and procedure interfaces.

## 2 Example

Figure 1 presents a *role reference diagram* for a process scheduler. Each box in the diagram denotes a disjoint set of objects of a given role. The labelled arrows between boxes indicate possible references between the objects in each set. As the diagram indicates, the scheduler maintains a list of live processes. A live process can be either running or sleeping. The running processes form a doubly-linked list, while sleeping processes form a binary tree. Both kinds of processes have `proc` references from the live list nodes `LiveList`. Header objects `RunningHeader` and `SleepingTree` simplify operations on the data structures that store the process objects.

As Figure 1 shows, data structure participation determines the conceptual state of each object. In our example, processes that participate in the sleeping process tree data structure are classified as sleeping processes, while processes that participate in the running process list data structure are classified as running processes. Moreover, movements between data structures correspond to conceptual state changes—when a process stops sleeping and starts running, it moves from the sleeping process tree to the running process list.

### 2.1 Role Definitions

Figure 2 presents the role definitions for the objects in our example.<sup>1</sup> Each role definition specifies the constraints that an object must satisfy to play the role. Field constraints

<sup>1</sup>In general, each role definition would specify the static class of objects that can play that role. To simplify the

specify the roles of the objects to which the fields refer, while slot constraints identify the number and kind of aliases of the object.

```

role LiveHeader {
  fields next : LiveList | null;
}
role LiveList {
  fields next : LiveList | null,
        proc : RunningProc | SleepingProc;
  slots LiveList.next | LiveHeader.next;
  acyclic next;
}
role RunningHeader {
  fields next : RunningProc | RunningHeader,
        prev : RunningProc | RunningHeader;
  slots RunningHeader.next | RunningProc.next,
        RunningHeader.prev | RunningProc.prev;
  identities next.prev, prev.next;
}
role RunningProc {
  fields next : RunningProc | RunningHeader,
        prev : RunningProc | RunningHeader;
  slots RunningHeader.next | RunningProc.next,
        RunningHeader.prev | RunningProc.prev,
        LiveList.proc;
  identities next.prev, prev.next;
}
role SleepingTree {
  fields root : SleepingProc | null,
  acyclic left, right;
}
role SleepingProc {
  fields left : SleepingProc | null,
        right : SleepingProc | null;
  slots SleepingProc.left | SleepingProc.right |
        SleepingTree.root;
  LiveList.proc;
  acyclic left, right;
}
role DeadProc { }

```

Figure 2: Role Definitions for a Scheduler

Role definitions may also contain two additional kinds of constraints: identity constraints, which specify paths that lead back to the object, and acyclicity constraints, which specify paths with no cycles. In our example, the identity constraint `next.prev` in the `RunningProc` role specifies the cyclic doubly-linked list constraint that following the `next`, then `prev` fields always leads back to the initial object. The acyclic constraint `left, right` in the `SleepingProc` role specifies that there are no cycles in the heap involving only `left` and `right` edges. On the other hand, the list of running processes must be cyclic because its nodes can never point to `null`.

The slot constraints specify the complete set of heap aliases for the object. In our example, this implies that no process can be simultaneously running and sleeping.

presentation, we assume that all objects are instances of a single class with a set of fields  $F$ .

In general, roles can capture data structure consistency properties such as disjointness and can prevent representation exposure [8]. As a data structure description language, roles can naturally specify trees with additional pointers. Roles can also approximate non-tree data structures like sparse matrices. Because most role constraints are local, it is possible to inductively infer them from data structure instances.

## 2.2 Roles and Procedure Interfaces

Procedures specify the initial and final roles of their parameters. The `suspend` procedure in Figure 3, for example, takes two parameters: an object with role `RunningProc`  $p$ , and the `SleepingTree`  $s$ . The procedure changes the role of the object referenced by  $p$  to `SleepingProc` whereas the object referenced by  $s$  retains its original role. To perform the role change, the procedure removes  $p$  from its `RunningList` data structure and inserts it into the `SleepingTree` data structure  $s$ . If the procedure fails to perform the insertions or deletions correctly, for instance by leaving an object in both structures, the role analysis will report an error.

```

procedure suspend(p : RunningProc ->> SleepingProc,
                 s : SleepingTree)
local pp, pn, r;
{
  pp = p.prev;  pn = p.next;
  r = s.root;
  p.prev = null; p.next = null;
  pp.next = pn;  pn.prev = pp;
  s.root = p;    p.left = r;
  setRole(p : SleepingProc);
}

```

Figure 3: Suspend Procedure

## 3 Abstract Syntax and Semantics of Roles

In this section, we precisely define what it means for a given heap to satisfy a set of role definitions. In subsequent sections we will use this definition as a starting point for a programming model and role analysis.

### 3.1 Heap Representation

We represent a concrete program heap as a finite directed graph  $H_c$  with  $\text{nodes}(H_c)$  representing objects of the heap and labelled edges representing heap references. A graph edge  $\langle o_1, f, o_2 \rangle \in H_c$  denotes a reference with field name  $f$  from object  $o_1$  to object  $o_2$ . To simplify the presentation, we fix a global set of fields  $F$  and assume that all objects have all fields in  $F$ . We do not consider subtyping or dynamic dispatch in this paper.

### 3.2 Role Representation

Let  $R$  denote the set of roles used in role definitions,  $\text{null}_R$  be a special symbol always denoting a null object  $\text{null}_c$ , and let

$R_0 = R \cup \{\text{null}_R\}$ . We represent each role as the conjunction of the following four kinds of constraints:

- **Fields:** For every field name  $f \in F$  we introduce a function  $\text{field}_f : R \rightarrow 2^{R_0}$  denoting the set of roles that objects of role  $r \in R$  can reference through field  $f$ . A field  $f$  of role  $r$  can be null if and only if  $\text{null}_R \in \text{field}_f(r)$ . The explicit use of  $\text{null}_R$  and the possibility to specify a set of alternative roles for every field allows roles to express both may and must referencing relationships.
- **Slots:** Every role  $r$  has  $\text{slotno}(r)$  slots. A slot  $\text{slot}_k(r)$  of role  $r \in R$  is a subset of  $R \times F$ . Let  $o$  be an object of role  $r$  and  $o'$  an object of role  $r'$ . A reference  $\langle o', f, o \rangle \in H_c$  can fill a slot  $k$  of object  $o$  if and only if  $\langle r', f \rangle \in \text{slot}_k(r)$ . An object with role  $r$  must have each of its slots filled by exactly one reference.
- **Identities:** Every role  $r \in R$  has a set of identities  $(r) \subseteq F \times F$ . Identities are pairs of fields  $\langle f, g \rangle$  such that following reference  $f$  on object  $o$  and then returning on reference  $g$  leads back to  $o$ .
- **Acyclicities:** Every role  $r \in R$  has a set  $\text{acyclic}(r) \subseteq F$  of fields along which cycles are forbidden.

### 3.3 Role Semantics

We define the semantics of roles as a conjunction of invariants associated with role definitions. A *concrete role assignment* is a map  $\rho_c : \text{nodes}(H_c) \rightarrow R_0$  such that  $\rho_c(\text{null}_c) = \text{null}_R$ .

**Definition 1** *Given a set of role definitions, we say that heap  $H_c$  is role consistent iff there exists a role assignment  $\rho_c : \text{nodes}(H_c) \rightarrow R_0$  such that for every  $o \in \text{nodes}(H_c)$  the predicate  $\text{locallyConsistent}(o, H_c, \rho_c)$  is satisfied. We call any such role assignment  $\rho_c$  a valid role assignment.*

The predicate  $\text{locallyConsistent}(o, H_c, \rho_c)$  formalizes the constraints associated with role definitions.

**Definition 2**  $\text{locallyConsistent}(o, H_c, \rho_c)$  iff all of the following conditions are met. Let  $r = \rho_c(o)$ .

- 1) For every field  $f \in F$  and  $\langle o, f, o' \rangle \in H_c$ ,  $\rho_c(o') \in \text{field}_f(r)$ .
- 2) Let  $\{\langle o_1, f_1 \rangle, \dots, \langle o_k, f_k \rangle\} = \{\langle o', f \rangle \mid \langle o', f, o \rangle \in H_c\}$  be the set of all aliases of node  $o$ . Then  $k = \text{slotno}(r)$  and there exists some permutation  $p$  of the set  $\{1, \dots, k\}$  such that  $\langle \rho_c(o_i), f_i \rangle \in \text{slot}_{p_i}(r)$  for all  $i$ .
- 3) If  $\langle o, f, o' \rangle \in H_c$ ,  $\langle o', g, o'' \rangle \in H_c$ , and  $\langle f, g \rangle \in \text{identities}(r)$ , then  $o = o''$ .
- 4) It is not the case that graph  $H_c$  contains a cycle  $o_1, f_1, \dots, o_s, f_s, o_1$  where  $o_1 = o$  and  $f_1, \dots, f_s \in \text{acyclic}(r)$

Note that a role consistent heap may have multiple valid role assignments  $\rho_c$ . However, in each of these role assignments, every object  $o$  is assigned exactly one role  $\rho_c(o)$ . The existence of a role assignment  $\rho_c$  with the property  $\rho_c(o_1) \neq \rho_c(o_2)$  thus implies  $o_1 \neq o_2$ . This is just one of the ways in which roles make aliasing more predictable.

## 4 Role Properties

Roles capture important properties of the objects and provide useful information about how the actions of the program affect those properties.

- **Consistency Properties:** Roles can ensure that the program respects application-level data structure consistency properties. The roles in our process scheduler, for example, ensure that a process cannot be simultaneously sleeping and running.
- **Interface Changes:** In many cases, the interface of an object changes as its referencing relationships change. In our process scheduler, for example, only running processes can be suspended. Because procedures declare the roles of their parameters, the role system can ensure that the program uses objects correctly even as the object's interface changes.
- **Multiple Uses:** Code factoring minimizes code duplication by producing general-purpose classes (such as the Java Vector and Hashtable classes) that can be used in a variety of contexts. But this practice obscures the different purposes that different instances of these classes serve in the computation. Because each instance's purpose is usually reflected in its relationships with other objects, roles can often recapture these distinctions.
- **Correlated Relationships:** In many cases, groups of objects cooperate to implement a piece of functionality. Standard type declarations provide some information about these collaborations by identifying the points-to relationships between related objects at the granularity of classes. But roles can capture a much more precise notion of cooperation, because they track correlated state changes of related objects.

Programmers can use roles for specifying the membership of objects in data structures and the structural invariants of data structures. In both cases, the slot constraints are essential.

When used to describe membership of an object in a data structure, slots specify the source of the alias from a data structure node that stores the object. By assigning different sets of roles to data structures used at different program points, it is possible to distinguish nodes stored in different data structure instances. As an object moves between data structures, the role of the object changes appropriately to reflect the new source of the alias.

When describing nodes of data structures, slot constraints specify the aliasing constraints of nodes; this is enough to precisely describe a variety of data structures and approximate many others. Property 16 below shows how to identify trees in role definitions even if tree nodes have additional aliases from other sets of nodes. It is also possible to define nodes which make up a compound data structure linked via disjoint sets of fields, such as threaded trees, sparse matrices and skip lists.

**Example 3** The following role definitions specify a sparse matrix of width and height at least 3. These definitions can be easily constructed from a sketch of a sparse matrix, as in Figure 4.

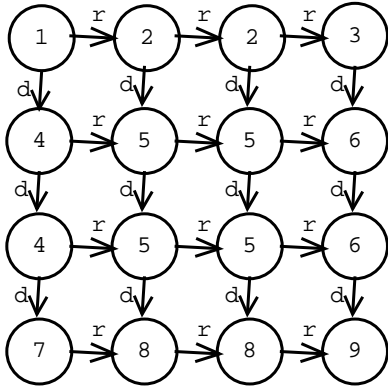


Figure 4: Roles of Nodes of a Sparse Matrix

```

role A1 {
  fields right : A2, down : A4;
  acyclic right, down;
}
role A2 {
  fields right : A2 | A3, down : A5;
  slots A1.right | A2.right;
  acyclic right, down;
}
role A3 {
  fields down : A6;
  slots A2.right;
  acyclic right, down;
}
role A4 {
  fields right : A5, down : A4 | A7;
  slots A1.down | A4.down;
  acyclic right, down;
}
role A5 {
  fields right : A5 | A6, down : A5 | A8;
  slots A4.right | A5.right, A2.down | A5.down;
  acyclic right, down;
}
role A6 {
  fields down : A6 | A9;
  slots A5.right, A3.down | A6.down;
  acyclic right, down;
}
role A7 {
  fields right : A8;
  slots A4.down;
  acyclic right, down;
}
role A8 {
  fields right : A8 | A9;
  slots A7.right | A8.right, A5.down;
  acyclic right, down;
}
role A9 {
  slots A8.right, A6.down;
  acyclic right, down;
}

```

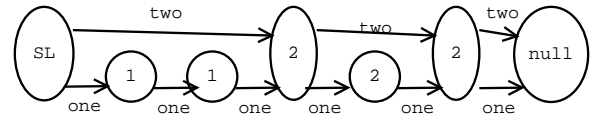


Figure 5: Sketch of a Two-Level Skip List

}

**Example 4** We next give role definitions for a two-level skip list [36] sketched in Figure 5.

```

role SkipList {
  fields one : OneNode | TwoNode | null;
  two : TwoNode | null;
}
role OneNode {
  fields one : OneNode | TwoNode | null;
  two : null;
  slots OneNode.one | TwoNode.one | SkipList.one;
  acyclic one, two;
}
role TwoNode {
  fields one : OneNode | TwoNode | null;
  two : TwoNode | null;
  slots OneNode.one | TwoNode.one | SkipList.one,
  TwoNode.two | SkipList.two;
  acyclic one, two;
}

```

#### 4.1 Formal Properties of Roles

In this section we identify some of the invariants expressible using sets of mutually recursive role definitions. A further study of role properties can be found in [31].

The following properties show some of the ways role specifications make object aliasing more predictable. They are an immediate consequence of the semantics of roles.

##### Property 5 (Role Disjointness)

If there exists a valid role assignment  $\rho_c$  for  $H_c$  such that  $\rho_c(o_1) \neq \rho_c(o_2)$ , then  $o_1 \neq o_2$ .

The previous property gives a simple criterion for showing that objects  $o_1$  and  $o_2$  are unaliased: find a valid role assignment which assigns different roles to  $o_1$  and  $o_2$ . This use of roles generalizes the use of static types for pointer analysis [12]. Since roles create a finer partition of objects than a typical static type system, their potential for proving absence of aliasing is even larger.

##### Property 6 (Disjointness Propagation)

If  $\langle o_1, f, o_2 \rangle, \langle o_3, g, o_4 \rangle \in H_c$ ,  $o_1 \neq o_3$ , and there exists a valid role assignment  $\rho_c$  for  $H_c$  such that  $\rho_c(o_2) = \rho_c(o_4) = r$  but  $\text{field}_f(r) \cap \text{field}_g(r) = \emptyset$ , then  $o_2 \neq o_4$ .

##### Property 7 (Generalized Uniqueness)

If  $\langle o_1, f, o_2 \rangle, \langle o_3, g, o_4 \rangle \in H_c$ ,  $o_1 \neq o_3$ , and there exists a role assignment  $\rho_c$  such that  $\rho_c(o_2) = \rho_c(o_4) = r$ , but there are no indices  $i \neq j$  such that  $\langle \rho_c(o_1), f \rangle \in \text{slot}_i(r)$  and  $\langle \rho_c(o_2), g \rangle \in \text{slot}_j(r)$  then  $o_2 \neq o_4$ .

A special case of Property 7 occurs when  $\text{slotno}(r) = 1$ ; this constrains all references to objects of role  $r$  to be unique.

Role definitions induce a role reference diagram RRD which captures some, but not all, role constraints.

**Definition 8 (Role Reference Diagram)**

Given a set of definitions of roles  $R$ , a role reference diagram RRD is a directed graph with nodes  $R_0$  and labelled edges defined by

$$\text{RRD} = \{ \langle r, f, r' \rangle \mid r' \in \text{field}_f(r) \text{ and } \exists i \langle r, f \rangle \in \text{slot}_i(r') \} \\ \cup \{ \langle r, f, \text{null}_R \rangle \mid \text{null}_R \in \text{field}_f(r) \}$$

Each role reference diagram is a refinement of the corresponding class diagram in a statically typed language, because it partitions classes into multiple roles according to their referencing relationships. The sets  $\rho_c^{-1}(r)$  of objects with role  $r$  change during program execution, reflecting the changing referencing relationships of objects.

Role definitions give more information than a role reference diagram. Slot constraints specify not only that objects of role  $r_1$  can reference objects of role  $r_2$  along field  $f$ , but also give cardinalities on the number of references from other objects. In addition, role definitions include identity and acyclicity constraints, which are not present in role reference diagrams.

**Property 9** Let  $\rho_c$  be any valid role assignment. Define

$$G = \{ \langle \rho_c(o_1), f, \rho_c(o_2) \rangle \mid \langle o_1, f, o_2 \rangle \in H_c \}$$

Then  $G$  is a subgraph of RRD.

It follows from Property 9 that roles give an approximation of may-reachability among heap objects.

**Property 10 (May Reachability)**

If there is a valid role assignment  $\rho_c : \text{nodes}(H_c) \rightarrow R_0$  such that  $\rho_c(o_1) \neq \rho_c(o_2)$  where  $o_1, o_2 \in \text{nodes}(H_c)$  and there is no path from  $\rho_c(o_1)$  to  $\rho_c(o_2)$  in the role reference diagram RRD, then there is no path from  $o_1$  to  $o_2$  in  $H_c$ .

The next property shows the advantage of explicitly specifying null references in role definitions. While the ability to specify acyclicity is provided by the `acyclic` constraint, it is also possible to indirectly specify must-cyclicity.

**Property 11 (Must Cyclicity)**

Let  $F_0 \subseteq F$  and  $R_{\text{CYC}} \subseteq R$  be a set of nodes in the role reference diagram RRD such that for every node  $r \in R_{\text{CYC}}$ , if  $\langle r, f, r' \rangle \in \text{RRD}$  then  $r' \in R_{\text{CYC}}$ . If  $\rho_c$  is a valid role assignment for  $H_c$ , then every object  $o_1 \in H_c$  with  $\rho_c(o_1) \in R_{\text{CYC}}$  is a member of a cycle in  $H_c$  with edges from  $F_0$ .

The following property shows that roles can specify a form of must-reachability among the sets of objects with the same role.

**Property 12 (Downstream Path Termination)**

Assume that for some set of fields  $F_0 \subseteq F$  there are sets of nodes  $R_{\text{INTER}} \subseteq R$ ,  $R_{\text{FINAL}} \subseteq R_0$  of the role reference diagram RRD such that for every node  $r \in R_{\text{INTER}}$ :

1.  $F_0 \subseteq \text{acyclic}(r)$
2. if  $\langle r, f, r' \rangle \in \text{RRD}$  for  $f \in F_0$ , then  $r' \in R_{\text{INTER}} \cup R_{\text{FINAL}}$

Let  $\rho_c$  be a valid role assignment for  $H_c$ . Then every path in  $H_c$  starting from an object  $o_1$  with role  $\rho_c(o_1) \in R_{\text{INTER}}$  and containing only edges labelled with  $F_0$  is a prefix of a path that terminates at some object  $o_2$  with  $\rho_c(o_2) \in R_{\text{FINAL}}$ .

**Property 13 (Upstream Path Termination)**

Assume that for some set of fields  $F_0 \subseteq F$  there are sets of nodes  $R_{\text{INTER}} \subseteq R$ ,  $R_{\text{INIT}} \subseteq R_0$  of the role reference diagram RRD such that for every node  $r \in R_{\text{INTER}}$ :

1.  $F_0 \subseteq \text{acyclic}(r)$
2. if  $\langle r', f, r \rangle \in \text{RRD}$  for  $f \in F_0$ , then  $r' \in R_{\text{INTER}} \cup R_{\text{INIT}}$

Let  $\rho_c$  be a valid role assignment for  $H_c$ . Then every path in  $H_c$  terminating at an object  $o_2$  with  $\rho_c(o_2) \in R_{\text{INTER}}$  and containing only edges labelled with  $F_0$  is a suffix of a path which started at some object  $o_1$ , where  $\rho_c(o_1) \in R_{\text{INIT}}$ .

The next two properties guarantee reachability properties by which there must exist at least one path in the heap, rather than stating properties of all paths as in Properties 12 and 13.

**Property 14 (Downstream Must Reachability)**

Assume that for some set of fields  $F_0 \subseteq F$  there are sets of roles  $R_{\text{INTER}} \subseteq R$ ,  $R_{\text{FINAL}} \subseteq R_0$  of the role reference diagram RRD such that for every node  $r \in R_{\text{INTER}}$ :

1.  $F_0 \subseteq \text{acyclic}(r)$
2. there exists  $f \in F_0$  such that  $\text{field}_f(r) \subseteq R_{\text{INTER}} \cup R_{\text{FINAL}}$

Let  $\rho_c$  be a valid role assignment for  $H_c$ . Then for every object  $o_1$  with  $\rho_c(o_1) \in R_{\text{INTER}}$  there is a path in  $H_c$  with edges from  $F_0$  from  $o_1$  to some object  $o_2$  where  $\rho_c(o_2) \in R_{\text{FINAL}}$ .

**Property 15 (Upstream Must Reachability)**

Assume that for some set of fields  $F_0 \subseteq F$  there are sets of nodes  $R_{\text{INTER}} \subseteq R$ ,  $R_{\text{INIT}} \subseteq R$  of the role reference diagram RRD such that for every node  $r \in R_{\text{INTER}}$ :

1.  $F_0 \subseteq \text{acyclic}(r)$
2. there exists  $k$  such that  $\text{slot}_k(r) \subseteq (R_{\text{INTER}} \cup R_{\text{INIT}}) \times F$

Let  $\rho_c$  be a valid role assignment for  $H_c$ . Then for every object  $o_2$  with  $\rho_c(o_2) \in R_{\text{INTER}}$  there is a path in  $H_c$  from some object  $o_1$  with  $\rho_c(o_1) \in R_{\text{INIT}}$  to the object  $o_2$ .

Trees are a class of data structures especially suited for static analysis. Roles can express graphs that are not trees, but it is useful to identify trees as certain sets of mutually recursive role definitions.

**Property 16 (Treeness)**

Let  $R_{\text{TREE}} \subseteq R$  be a set of roles and  $F_0 \subseteq F$  set of fields such that for every  $r \in R_{\text{TREE}}$

1.  $F_0 \subseteq \text{acyclic}(r)$
2.  $|\{i \mid \text{slot}_i(r) \cap (R_{\text{TREE}} \times F_0) \neq \emptyset\}| \leq 1$

Let  $\rho_c$  be a valid role assignment for  $H_c$  and  $S \subseteq \{ \langle n_1, f, n_2 \rangle \mid \langle n_1, f, n_2 \rangle \in H_c, \rho(n_1), \rho(n_2) \in R_{\text{TREE}}, f \in F_0 \}$ . Then  $S$  is a set of trees.

## 5 A Programming Model

In this section we define what it means for an execution of a program to respect the role constraints. This definition is complicated by the need to allow the program to temporarily violate the role constraints during data structure manipulations. Our approach is to let the program violate the constraints for objects referenced by local variables or parameters, but require all other objects to satisfy the constraints.

We first present a simple imperative language with dynamic object allocation and give its operational semantics. We then specify additional statement preconditions that enforce the role consistency requirements.

### 5.1 A Simple Imperative Language

Our core language contains, as basic statements, Load ( $x=y.f$ ), Store ( $x.f=y$ ), Copy ( $x=y$ ), and New ( $x=new$ ). All variables are references to objects in the global heap and all assignments are reference assignments. We use an elementary `test` statement combined with nondeterministic choice and iteration to express `if` and `while` statement, using the usual translation [22, 1]. We represent the control flow of programs using control-flow graphs.

A program is a collection of procedures  $\text{proc} \in \text{Proc}$ . Procedures change the global heap but do not return values. Every procedure  $\text{proc}$  has a list of parameters  $\text{param}(\text{proc}) = \{\text{param}_i(\text{proc})\}_i$  and a list of local variables  $\text{local}(\text{proc})$ . We use  $\text{var}(\text{proc})$  to denote  $\text{param}(\text{proc}) \cup \text{local}(\text{proc})$ . A procedure definition specifies the initial role  $\text{preR}_k(\text{proc})$  and the final role  $\text{postR}_k(\text{proc})$  for every parameter  $\text{param}_k(\text{proc})$ . We use  $\text{proc}_j$  for indices  $j \in \mathcal{N}$  to denote activation records of procedure  $\text{proc}$ . We further assume that there are no modifications of parameter variables so every parameter references the same object throughout the lifetime of procedure activation.

**Example 17** The following `kill` procedure removes a process from both the doubly linked list of running processes and the list of all active processes. This is indicated by the transition from `RunningProc` to `DeadProc`.

```

procedure kill(p : RunningProc ->> DeadProc,
             l : LiveHeader)
local prev, current, cp, nxt, lp, ln;
{
  // find 'p' in 'l'
  prev = l; current = l.next;
  cp = current.proc;
  while (cp != p) {
    prev = current;
    current = current.next;
    cp = current.proc;
  }
  // remove 'current' and 'p' from active list
  nxt = current.next;
  prev.next = nxt; current.
  current.proc = null;
  setRole(current : IsolatedCell);
  // remove 'p' from running list
  lp = p.prev; ln = p.next;

```

```

  p.prev = null; p.next = null;
  lp.next = ln; ln.prev = lp;
  setRole(p : DeadProc);
}

```

### 5.2 Operational Semantics

In this section we give the operational semantics for our language. We focus on the first three columns in Figures 6 and 7; the safety conditions in the fourth column are detailed in Section 5.4.

Figure 6 gives the small-step operational semantics for the basic statements. We use  $A \uplus B$  to denote the union  $A \cup B$  where the sets  $A$  and  $B$  are disjoint. The program state consists of the stack  $s$  and the concrete heap  $H_c$ . The stack  $s$  is a sequence of pairs  $p@proc_i \in \times(\text{Proc} \times \mathcal{N})$ , where  $p \in N_{\text{CFG}}(\text{proc})$  is a program point, and  $\text{proc}_i \in \text{Proc} \times \mathcal{N}$  is an activation record of procedure  $\text{proc}$ . Program points  $p \in N_{\text{CFG}}(\text{proc})$  are nodes of the control-flow graphs. There is one control-flow graph for every procedure  $\text{proc}$ . An edge of the control-flow graph  $\langle p, p' \rangle \in E_{\text{CFG}}(\text{proc})$  indicates that control may transfer from point  $p$  to point  $p'$ . We write  $p : \text{stat}$  to state that program point  $p$  contains a statement  $\text{stat}$ . The control flow graph of each procedure contains special program points `entry` and `exit` indicating procedure entry and exit, with no statements associated with them. We assume that all conditions are of the form  $x==y$  or  $!(x==y)$  where  $x$  and  $y$  are either variables or a special constant `null` which always points to the `nullc` object.

The concrete heap is either an error heap  $\text{error}_c$  or a non-error heap. A non-error heap  $H_c \subseteq N \times F \times N \cup ((\text{Proc} \times \mathcal{N}) \times V \times N)$  is a directed graph with labelled edges, where nodes represent objects and procedure activation records, whereas edges represent heap references and local variables. An edge  $\langle o_1, f, o_2 \rangle \in N \times F \times N$  denotes a reference from object  $o_1$  to object  $o_2$  via field  $f \in F$ . An edge  $\langle \text{proc}_i, x, o \rangle \in H_c$  means that local variable  $x$  in activation record  $\text{proc}_i$  points to object  $o$ .

A load statement  $x=y.f$  makes the variable  $x$  point to node  $o_f$ , which is referenced by the  $f$  field of object  $o_y$ , which is in turn referenced by variable  $y$ . A store statement  $x.f=y$  replaces the reference along field  $f$  in object  $o_x$  by a reference to object  $o_y$  that is referenced by  $y$ . The copy statement  $x=y$  copies a reference to object  $o_y$  into variable  $x$ . The statement  $x=new$  creates a new object  $o_n$  with all fields initially referencing `nullc`, and makes  $x$  point to  $o_n$ . The statement `test(c)` allows execution to proceed only if condition  $c$  is satisfied.

Figure 7 describes the semantics of procedure calls. Procedure call pushes new activation record onto stack, inserts it into the heap, and initializes the parameters. Procedure entry initializes local variables. Procedure exit removes the activation record from the heap and the stack.

### 5.3 Onstage and Offstage Objects

At every program point the set of all objects of heap  $H_c$  can be partitioned into:

Statement	Transition	Constraints	Role Consistency
$p : x=y.f$	$\langle p@proc_i; s, H_c \uplus \{\langle proc_i, x, o_x \rangle\} \rangle \longrightarrow \langle p'@proc_i; s, H'_c \rangle$	$x, y \in local(proc),$ $\langle proc_i, y, o_y \rangle, \langle o_y, f, o_f \rangle \in H_c,$ $\langle p, p' \rangle \in E_{CFG}(proc),$ $H'_c = H_c \uplus \{proc_i, x, o_f\}$	$accessible(o_f, proc_i, H_c),$ $con(H'_c, offstage(H'_c))$
$p : x.f=y$	$\langle p@proc_i; s, H_c \uplus \{\langle o_x, f, o_f \rangle\} \rangle \longrightarrow \langle p'@proc_i; s, H'_c \rangle$	$x, y \in local(proc),$ $\langle proc_i, x, o_x \rangle, \langle proc_i, y, o_y \rangle \in H_c,$ $\langle p, p' \rangle \in E_{CFG}(proc),$ $H'_c = H_c \uplus \{\langle o_x, f, o_y \rangle\}$	$o_f \in onstage(H_c, proc_i)$ $con(H'_c, offstage(H'_c))$
$p : x=y$	$\langle p@proc_i; s, H_c \uplus \{\langle proc_i, x, o_x \rangle\} \rangle \longrightarrow \langle p'@proc_i; s, H'_c \rangle$	$x \in local(proc),$ $y \in var(proc),$ $\langle proc_i, y, o_y \rangle \in H_c,$ $\langle p, p' \rangle \in E_{CFG}(proc),$ $H'_c = H_c \uplus \{\langle proc_i, x, o_y \rangle\}$	$con(H'_c, offstage(H'_c))$
$p : x=new$	$\langle p@proc_i; s, H_c \uplus \{\langle proc_i, x, o_x \rangle\} \rangle \longrightarrow \langle p'@proc_i; s, H'_c \rangle$	$x \in local(proc),$ $o_n$ fresh, $\langle p, p' \rangle \in E_{CFG}(proc),$ $H'_c = H_c \uplus \{\langle proc_i, x, o_n \rangle\} \uplus nulls,$ $nulls = \{o_n\} \times F \times \{null\}$	$con(H'_c, offstage(H'_c))$
$p : test(c)$	$\langle p@proc_i; s, H_c \rangle \longrightarrow \langle p'@proc_i; s, H_c \rangle$	$satisfied_c(c, proc_i, H_c),$ $\langle p, p' \rangle \in E_{CFG}(proc)$	$con(H_c, offstage(H_c))$

$satisfied_c(x==y, proc_i, H_c)$  iff  $\{o \mid \langle proc_i, x, o \rangle \in H_c\} = \{o \mid \langle proc_i, y, o \rangle \in H_c\}$

$satisfied_c(! (x==y), proc_i, H_c)$  iff not  $satisfied_c(x==y, proc_i, H_c)$

$accessible(o, proc_i, H_c) := (\exists p \in param(proc) : \langle proc_i, p, o \rangle \in H_c)$   
or not  $(\exists proc'_j \exists v \in var(proc') : \langle proc'_j, v, o \rangle \in H_c)$

Figure 6: Semantics of Basic Statements

Statement	Transition	Constraints	Role Consistency
$entry : -$	$\langle p@proc_i; s, H_c \rangle \longrightarrow \langle p'@proc_i; s, H_c \uplus nulls \rangle$	$nulls = \{\langle proc_i, v, null_c \rangle \mid v \in local(proc), \langle p, p' \rangle \in E_{CFG}(proc)\}$	$con(H_c, offstage(H_c))$
$p : proc'(x_k)_k$	$\langle p@proc_i; s, H_c \rangle \longrightarrow \langle entry@proc'_j; p'@proc_i; s, H'_c \rangle$	$j$ fresh in $p@proc_i; s,$ $\langle p, p' \rangle \in E_{CFG}(proc),$ $o_k : \langle proc_i, x_k, o_k \rangle \in H_c,$ $H'_c = H_c \uplus \{\langle proc'_j, p_k, o_k \rangle\}_k,$ $\forall k p_k = param_k(proc')$	$conW(ra, H_c, S),$ $ra = \{\langle o_k, preR_k(proc') \rangle\}_k,$ $S = offstage(H_c) \cup \{o_k\}_k$
$exit : -$	$\langle p@proc_i; s, H_c \rangle \longrightarrow \langle s, H_c \setminus AF \rangle$	$AF = \{\langle proc_i, v, n \rangle \mid \langle proc_i, v, n \rangle \in H_c\}$	$conW(ra, H_c, S),$ $ra = \{\langle parnd_k(proc_i), postR_k(proc) \rangle\}_k,$ $S = offstage(H_c) \cup \{o \mid \langle proc_i, v, o \rangle \in H_c\}$

$parnd_k(proc_i) = o$  where  $\langle proc_i, param_k(proc), o \rangle \in H_c$

Figure 7: Semantics of Procedure Call



1. **onstage objects** ( $\text{onstage}(H_c)$ ) referenced by a local variable or parameter of some activation frame;

$$\begin{aligned} \text{onstage}(H_c, \text{proc}_i) &:= \{o \mid \exists x \in \text{var}(\text{proc}) \\ &\quad \langle \text{proc}_i, x, o \rangle \in H_c\} \\ \text{onstage}(H_c) &:= \bigcup_{\text{proc}_i} \text{onstage}(H_c, \text{proc}_i) \end{aligned}$$

2. **offstage objects** ( $\text{offstage}(H_c)$ ) unreferenced by local or parameter variables.

$$\text{offstage}(H_c) := \text{nodes}(H_c) \setminus \text{onstage}(H_c)$$

Onstage objects need not have correct roles. Offstage objects must have correct roles assuming some role assignment for onstage objects.

**Definition 18** *Given a set of role definitions and a set of objects  $S_c \subseteq \text{nodes}(H_c)$ , we say that heap  $H_c$  is role consistent for  $S_c$ , and we write  $\text{con}(H_c, S_c)$ , iff there exists a role assignment  $\rho_c : \text{nodes}(H_c) \rightarrow R_0$  such that the predicate  $\text{locallyConsistent}(o, H_c, \rho_c, S_c)$  is satisfied for every object  $o \in S_c$ .*

We define  $\text{locallyConsistent}(o, H_c, \rho_c, S_c)$  to generalize the  $\text{locallyConsistent}(o, H_c, \rho_c)$  predicate, weakening the acyclicity condition.

**Definition 19**  *$\text{locallyConsistent}(o, H_c, \rho_c, S_c)$  holds iff conditions 1), 2), and 3) of Definition 2 are satisfied and the following condition holds:*

- 4') *It is not the case that graph  $H_c$  contains a cycle  $o_1, f_1, \dots, o_s, f_s, o_1$  such that  $o_1 = o, f_1, \dots, f_s \in \text{acyclic}(r)$ , and additionally  $o_1, \dots, o_s \in S_c$ .*

Here  $S_c$  is the set of onstage objects that are not allowed to create a cycle; objects in  $\text{nodes}(H_c) \setminus S_c$  are exempt from the acyclicity condition. The  $\text{locallyConsistent}(o, H_c, \rho_c, S_c)$  and  $\text{con}(H_c, S_c)$  predicates are monotonic in  $S_c$ , so a larger  $S_c$  implies a stronger invariant. For  $S_c = \text{nodes}(H_c)$ , consistency for  $S_c$  is equivalent with heap consistency from Definition 1. Note that the role assignment  $\rho_c$  specifies roles even for objects  $o \in \text{nodes}(H_c) \setminus S_c$ . This is because the role of  $o$  may influence the role consistency of objects in  $S_c$  which are adjacent to  $o$ .

At procedure calls, the role declarations for parameters restrict the set of potential role assignments. We therefore generalize  $\text{con}(H_c, S_c)$  to  $\text{conW}(\text{ra}, H_c, S_c)$ , which restricts the set of role assignments  $\rho_c$  considered for heap consistency.

**Definition 20** *Given a set of role definitions, a heap  $H_c$ , a set  $S_c \subseteq \text{nodes}(H_c)$ , and a partial role assignment  $\text{ra} \subseteq S_c \rightarrow R$ , we say that the heap  $H_c$  is consistent with  $\text{ra}$  for  $S_c$ , and we write  $\text{conW}(\text{ra}, H_c, S_c)$ , iff there exists a (total) role assignment  $\rho_c : \text{nodes}(H_c) \rightarrow R_0$  such that  $\text{ra} \subseteq \rho_c$  and for every object  $o \in S_c$  the predicate  $\text{locallyConsistent}(o, H_c, \rho_c, S_c)$  is satisfied.*

## 5.4 Role Consistency

We are now able to precisely state the role consistency requirements that must be satisfied for program execution. The role consistency requirements are in the fourth row of Figures 6 and 7. We assume the operational semantics is extended with transitions leading to a program state with heap  $\text{error}_c$  whenever role consistency is violated.

### 5.4.1 Offstage Consistency

At every program point, we require  $\text{con}(H_c, \text{offstage}(H_c))$  to be satisfied. This means that offstage objects have correct roles, but onstage objects may have their role temporarily violated.

### 5.4.2 Reference Removal Consistency

The Store statement  $\mathbf{x.f=y}$  has the following safety precondition. When a reference  $\langle o_x, f, o_f \rangle \in H_c$  for  $\langle \text{proc}_j, \mathbf{x}, o_x \rangle \in H_c$ , and  $\langle o_x, f, o_f \rangle \in H_c$  is removed from the heap, both  $o_x$  and  $o_f$  must be referenced from the current procedure activation record. It is sufficient to verify this condition for  $o_f$ , as  $o_x$  is already onstage by definition. The reference removal consistency condition enables the completion of the role change for  $o_f$  after the reference  $\langle o_x, f, o_f \rangle$  is removed and ensures that heap references are introduced and removed only between onstage objects.

### 5.4.3 Procedure Call Consistency

Our programming model ensures role consistency across procedure calls using the following protocol.

A procedure call  $\text{proc}'(x_1, \dots, x_p)$  in Figure 7 requires the role consistency precondition  $\text{conW}(\text{ra}, H_c, S_c)$ , where the partial role assignment  $\text{ra}$  requires objects  $o_k$ , corresponding to parameters  $x_k$ , to have roles  $\text{preR}_k(\text{proc}')$  expected by the callee, and  $S_c = \text{offstage}(H_c) \cup \{o_k\}_k$  for  $\langle \text{proc}_j, x_k, o_k \rangle \in H_c$ .

To ensure that the callee  $\text{proc}'_j$  never observes incorrect roles, we impose an *accessibility condition* for the callee's Load statements (see the fourth column of Figure 6). The accessibility condition prohibits access to any object  $o$  referenced by some local variable of a stack frame other than  $\text{proc}'_j$ , unless  $o$  is referenced by some parameter of  $\text{proc}'_j$ . Provided that this condition is not violated, the callee  $\text{proc}'_j$  only accesses objects with correct roles, even though objects that it does not access may have incorrect roles. In Section 7 we show how the role analysis ensures that the accessibility condition is never violated.

At the procedure exit point (Figure 7), we require correct roles for all objects referenced by the current activation frame  $\text{proc}'_j$ . This implies that heap operations performed by  $\text{proc}'_j$  preserve heap consistency for all objects accessed by  $\text{proc}'_j$ .

### 5.4.4 Explicit Role Check

The programmer can specify a stronger invariant at any program point using statement  $\text{roleCheck}(x_1, \dots, x_p, \text{ra})$ . As Figure 8 indicates,  $\text{roleCheck}$  requires the  $\text{conW}(\text{ra}, H_c, S_c)$  predicate to be satisfied for the supplied partial role assignment  $\text{ra}$  where  $S_c = \text{offstage}(H_c) \cup \{o_k\}_k$  for objects  $o_k$  referenced by given local variables  $x_k$ .

Statement	Transition	Constraints	Role Consistency
$p : \text{roleCheck}(x_1, \dots, x_n, ra)$	$\langle p@proc_i; s, H_c \rangle \longrightarrow \langle p'@proc_i; s, H_c \rangle$	$\langle p, p' \rangle \in E_{CFG}$	$\text{conW}(ra, H_c, S),$ $S = \text{offstage}(H_c) \cup \{o \mid \langle proc_i, x_k, o \rangle \in H_c\}$

Figure 8: Operational Semantics of Explicit Role Check

## 5.5 Instrumented Semantics

We expect the programmer to have a specific role assignment in mind when writing the program, with this role assignment changing as the statements of the program change the referencing relationships. So when the programmer wishes to change the role of an object, he or she writes a program that brings the object onstage, changes its referencing relationships so that it plays a new role, then puts it offstage in its new role. The roles of other objects do not change.<sup>2</sup>

To support these programmer expectations, we introduce an augmented programming model in which the role assignment  $\rho_c$  is conceptually part of the program's state. The role assignment changes only if the programmer changes it explicitly using the `setRole` statement. The augmented programming model has an underlying *instrumented semantics* as opposed to the *original semantics*.

**Example 21** The original semantics allows asserting different roles at different program points even if the structure of the heap was not changed, as in the following procedure `foo`.

```

role A1 { fields f : B1; }
role B1 { slots A1.f; }
role A2 { fields f : B2; }
role B2 { slots A2.f; }
procedure foo()
var x, y;
{
  x = new; y = new;
  x.f = y;
  roleCheck(x,y, x:A1,y:B1);
  roleCheck(x,y, x:A2,y:B2);
}

```

Both role checks would succeed since each of the specified partial role assignments can be extended to a valid role assignment. On the other hand, the check `roleCheck(x,y, x:A1,y:B2)` would fail.

The procedure `foo` in the instrumented semantics can be written as follows.

```

procedure foo()
var x, y;
{
  x = new; y = new;
  x.f = y;
  setRole(x:A1); setRole(y:B1);
  roleCheck(x,y, x:A1,y:B1);
}

```

<sup>2</sup>An extension to the programming model supports *cascading role changes* in which a single role change propagates through the heap changing the roles of offstage objects, see Section 8.2.

```

setRole(x:A2); setRole(y:B2);
roleCheck(x,y, x:A2,y:B2);
}

```

The `setRole` statement makes the role change of object explicit.

The instrumented semantics extends the concrete heap  $H_c$  with a role assignment  $\rho_c$ . Figure 9 outlines the changes in instrumented semantics with respect to the original semantics. We introduce a new statement `setRole(x:r)`, which modifies a role assignment  $\rho_c$ , giving  $\rho_c[o_x \mapsto r]$ , where  $o_x$  is the object referenced by  $x$ . All statements other than `setRole` preserve the current role assignment. For every consistency condition  $\text{conW}(ra, H_c, S_c)$  in the original semantics, the instrumented semantics uses the corresponding condition  $\text{conW}(\rho_c \cup ra, H_c, S_c)$  and fails if  $\rho_c$  is not an extension of  $ra$ . Here we consider  $\text{con}(H_c, S)$  to be a shorthand for  $\text{conW}(\emptyset, H_c, S)$ . For example, the new role consistency condition for the Copy statement `x=y` is  $\text{conW}(\rho_c, H_c, \text{offstage}(H_c))$ . The New statement assigns an identifier unknown to the newly created object  $o_n$ . By definition, a node with unknown does not satisfy the `locallyConsistent` predicate. This means that `setRole` must be used to set a a valid role of  $o_n$  before  $o_n$  moves offstage.

By introducing an instrumented semantics we are not suggesting an implementation that explicitly stores roles of objects at run-time. We instead use the instrumented semantics as the basis of our role analysis and ensure that all role checks can be statically removed. Because the instrumented semantics is more restrictive than the original semantics, our role analysis is a conservative approximation of both the instrumented semantics and the original semantics.

## 6 Intraprocedural Role Analysis

This section presents an intraprocedural role analysis algorithm. The goal of the role analysis is to statically verify the role consistency requirements described in the previous section.

The key observation behind our analysis algorithm is that we can incrementally verify role consistency of the concrete heap  $H_c$  by ensuring role consistency for every node when it goes offstage. This allows us to represent the statically unbounded offstage portion of the heap using summary nodes with “may” references. In contrast, we use a “must” interpretation for references from and to onstage nodes. The exact representation of onstage nodes allows the analysis to verify role consistency in the presence of temporary violations of role constraints.

Our analysis representation is a graph in which nodes represent objects and edges represent references between ob-

Statement	Transition	Constraints	Role Consistency
$p : \mathbf{x} = \mathbf{new}$	$\langle p @ \text{proc}_i; s, H_c \uplus \{ \langle \text{proc}_i, \mathbf{x}, o_x \rangle \}, \rho_c \rangle \longrightarrow \langle p' @ \text{proc}_i; s, H'_c, \rho'_c \rangle$	$\mathbf{x} \in \text{local}(\text{proc}),$ $o_n \text{ fresh},$ $\langle p, p' \rangle \in E_{\text{CFG}}(\text{proc}),$ $H'_c = H_c$ $\uplus \{ \langle \text{proc}_i, \mathbf{x}, o_n \rangle \}$ $\uplus \{ o_n \} \times F \times \{ \text{null} \},$ $\rho'_c = \rho_c[o_n \mapsto \text{unknown}]$	$\text{conW}(\rho'_c, H'_c, \text{offstage}(H'_c))$
$p : \mathbf{setRole}(\mathbf{x} : \mathbf{r})$	$\langle p @ \text{proc}_i; s, H_c, \rho_c \rangle \longrightarrow \langle p' @ \text{proc}_i; s, H_c, \rho'_c \rangle$	$\mathbf{x} \in \text{local}(\text{proc}_i),$ $\langle \text{proc}_i, \mathbf{x}, o_x \rangle \in H_c,$ $\rho'_c = \rho_c[o_x \mapsto \mathbf{r}],$ $\langle p, p' \rangle \in E_{\text{CFG}}$	$\text{conW}(\rho'_c, H_c, \text{offstage}(H_c))$
$p : \mathbf{stat}$	$\langle s, H_c, \rho_c \rangle \longrightarrow \langle s', H'_c, \rho_c \rangle$	$\langle s, H_c \rangle \longrightarrow \langle s', H'_c \rangle$	$P \wedge \text{conW}(\rho_c \cup \text{ra}, H'_c, S)$ for every original condition $P \wedge \text{conW}(\text{ra}, H'_c, S)$

Figure 9: Instrumented Semantics

jects. There are two kinds of nodes: *onstage nodes* represent onstage objects, with each onstage node representing one onstage object; and *offstage nodes*, with each offstage node corresponding to a set of objects that play that role. To increase the precision of the analysis, the algorithm occasionally generates multiple offstage nodes that represent disjoint sets of objects playing the same role. Distinct offstage objects with the same role  $r$  represent disjoint sets of objects of role  $r$  with different reachability properties from onstage nodes.

We frame role analysis as a data-flow analysis operating on a distributive lattice  $\mathcal{P}(\text{RoleGraphs})$  of sets of role graphs with set union  $\cup$  as the join operator. In this section we present an algorithm for intraprocedural analysis. We use  $\text{proc}_c$  to denote the topmost activation record in a concrete heap  $H_c$ . In Section 7 we generalize the algorithm to the compositional interprocedural analysis.

## 6.1 Abstraction Relation

Every data-flow fact  $\mathcal{G} \subseteq \text{RoleGraphs}$  is a set of role graphs  $G \in \mathcal{G}$ . Every role graph  $G \in \text{RoleGraphs}$  is either a bottom role graph  $\perp_G$  representing the set of all concrete heaps (including  $\text{error}_c$ ), or a tuple  $G = \langle H, \rho, K \rangle$  representing non-error concrete heaps, where

- $H \subseteq N \times F \times N$  is the abstract heap with nodes  $N$  representing objects and fields  $F$ . The abstract heap  $H$  represents heap references  $\langle n_1, f, n_2 \rangle$  and variables of the currently analyzed procedure  $(\text{proc}, x, n)$  where  $x \in \text{local}(\text{proc})$ . Null references are represented as references to abstract node  $\text{null}$ . We define abstract onstage nodes  $\text{onstage}(H) = \{ n \mid \langle \text{proc}, x, n \rangle \in H, x \in \text{local}(\text{proc}) \cup \text{param}(\text{proc}) \}$  and abstract offstage nodes  $\text{offstage}(H) = \text{nodes}(H) \setminus \text{onstage}(H) \setminus \{ \text{proc}, \text{null} \}$ .
- $\rho : \text{nodes}(H) \rightarrow R_0$  is an abstract role assignment,  $\rho(\text{null}) = \text{null}_R$ ;
- $K : \text{nodes}(H) \rightarrow \{i, s\}$  indicates the kind of each node; when  $K(n) = i$ , then  $n$  is an individual node representing at most one object, and when  $K(n) = s$ ,  $n$  is a summary node representing zero or more objects. We

require  $K(\text{proc}) = K(\text{null}) = i$ , and require all onstage nodes to be individual,  $K[\text{onstage}(H)] = \{i\}$ .

The abstraction relation  $\alpha$  relates a pair  $\langle H_c, \rho_c \rangle$  of concrete heap and concrete role assignment with an abstract role graph  $G$ .

**Definition 22** *We say that an abstract role graph  $G$  represents concrete heap  $H_c$  with role assignment  $\rho_c$  and write  $\langle H_c, \rho_c \rangle \alpha G$ , iff  $G = \perp_G$  or:  $H_c \neq \text{error}_c$ ,  $G = \langle H, \rho, K \rangle$ , and there exists a function  $h : \text{nodes}(H_c) \rightarrow \text{nodes}(H)$  such that*

- 1)  $H_c$  is role consistent:  $\text{conW}(\rho_c, H_c, \text{offstage}(H_c))$ ,
- 2) identity relations of onstage nodes with offstage nodes hold: if  $\langle o_1, f, o_2 \rangle \in H_c$  and  $\langle o_2, g, o_3 \rangle \in H_c$  for  $o_1 \in \text{onstage}(H_c)$ ,  $o_2 \in \text{offstage}(H_c)$ , and  $\langle f, g \rangle \in \text{identities}(\rho_c(o_1))$ , then  $o_3 = o_1$ ;
- 3)  $h$  is a graph homomorphism: if  $\langle o_1, f, o_2 \rangle \in H_c$  then  $\langle h(o_1), f, h(o_2) \rangle \in H$ ;
- 4) an individual node represents at most one concrete object:  $K(n) = i$  implies  $|h^{-1}(n)| \leq 1$ ;
- 5)  $h$  is bijection on edges which originate or terminate at onstage nodes: if  $\langle n_1, f, n_2 \rangle \in H$  and  $n_1 \in \text{onstage}(H)$  or  $n_2 \in \text{onstage}(H)$ , then there exists exactly one  $\langle o_1, f, o_2 \rangle \in H_c$  such that  $h(o_1) = n_1$  and  $h(o_2) = n_2$ ;
- 6)  $h(\text{null}_c) = \text{null}$  and  $h(\text{proc}_c) = \text{proc}$ ;
- 7) the abstract role assignment  $\rho$  corresponds to the concrete role assignment:  $\rho_c(o) = \rho(h(o))$  for every object  $o \in \text{nodes}(H_c)$ .

Note that the error heap  $\text{error}_c$  can be represented only by the bottom role graph  $\perp_G$ . The analysis uses  $\perp_G$  to indicate a potential role error.

Condition 3) implies that role graph edges are a conservative approximation of concrete heap references. These edges are in general “may” edges. Hence it is possible for an offstage node  $n$  that  $\langle n, f, n_1 \rangle, \langle n, f, n_2 \rangle \in H$  for  $n_1 \neq n_2$ . This cannot happen when  $n \in \text{onstage}(H)$  because of 5). Another consequence of 5) is that an edge in  $H$  from an onstage node



Transition	Definition	Conditions
$\langle H, \rho, K \rangle \xrightarrow{x=y.f} G'$	$\langle H, \rho, K \rangle \xrightarrow{n_y.f} G_1 \xrightarrow{x=y.f} G_2 \xrightarrow{n_x} G'$	$\langle \text{proc}, x, n_x \rangle, \langle \text{proc}, y, n_y \rangle \in H$
$\langle H, \rho, K \rangle \xrightarrow{x=y} G'$	$\langle H, \rho, K \rangle \xrightarrow{x=y} G_1 \xrightarrow{n_1} G'$	$\langle \text{proc}, x, n_1 \rangle \in H$
$\langle H, \rho, K \rangle \xrightarrow{x=new} G'$	$\langle H, \rho, K \rangle \xrightarrow{x=new} G_1 \xrightarrow{n_1} G'$	$\langle \text{proc}, x, n_1 \rangle \in H$
$\langle H, \rho, K \rangle \xrightarrow{s} G'$	$\langle H, \rho, K \rangle \xrightarrow{s} G'$	$s \in \{x.f=y, \text{test}(c), \text{setRole}(x:r), \text{roleCheck}(x_{1..p}, ra)\}$

Figure 12: Abstract Execution  $\rightsquigarrow$

The symbolic execution  $\xrightarrow{st}$  followed by the contraction relation  $\succeq$  corresponds to the instrumented operational semantics  $\rightarrow$ .

Figure 12 shows rules for the abstract execution relation  $\rightsquigarrow^{st}$ . Only Load statement uses the expansion relation, because the other statements operate on objects that are already onstage. Load, Copy, and New statements may remove a local variable reference from an object, so they use contraction relation to move the object offstage if needed. For the rest of the statements, the abstract execution reduces to symbolic execution  $\Longrightarrow$  described in Section 6.2.3.

**Nondeterminism and Failure** The  $\rightsquigarrow^{st}$  relation is not a function because the expansion relation  $\preceq$  can generate a set of role graphs from a single role graph. Also, there might be no  $\rightsquigarrow^{st}$  transitions originating from a given state  $G$  if the symbolic execution  $\Longrightarrow$  produces no results. This corresponds to a trace which cannot be extended further due to a `test` statement which fails in state  $G$ . This is in contrast to a transition from  $G$  to  $\perp_G$  which indicates a potential role consistency violation or a null pointer dereference. We assume that  $\Longrightarrow$  and  $\succeq$  relations contain the transition  $\langle \perp_G, \perp_G \rangle$  to propagate the error role graph. In most cases we do not write the explicit transitions to error states.

### 6.2.1 Expansion

Figure 13 shows the expansion relation  $\preceq^{n,f}$ . Given a role graph  $\langle H, \rho, K \rangle$  expansion attempts to produce a set of role graphs  $\langle H', \rho', K' \rangle$  in each of which  $\langle n, f, n_0 \rangle \in H'$  and  $K(n_0) = i$ . Expansion is used in abstract execution of the Load statement. It first checks for null pointer dereference and reports an error if the check fails. If  $\langle n, f, n' \rangle \in H$  and  $K(n') = i$  already hold, the expansion returns the original state. Otherwise,  $\langle n, f, n' \rangle \in H$  with  $K(n') = s$ . In that case, the summary node  $n'$  is first instantiated using instantiation relation  $\uparrow_{n'}^{n_0}$ . Next, the split relation  $\parallel_{n_0}^{n'}$  is applied. Let  $\rho(n_0) = r$ . The split relation ensures that  $n_0$  is not a member of any cycle of offstage nodes which contains only edges in  $\text{acyclic}(r)$ . We explain instantiation and split in more detail below.

**Instantiation** Figure 14 presents the instantiation relation. Given a role graph  $G = \langle H, \rho, K \rangle$ , instantiation  $\uparrow_{n'}^{n_0}$

generates the set of role graphs  $\langle H', \rho', K' \rangle$  such that each concrete heap represented by  $\langle H, \rho, K \rangle$  is represented by one of the graphs  $\langle H', \rho', K' \rangle$ . Each of the new role graphs contains a fresh individual node  $n_0$  that satisfies `localCheck`. The edges of  $n_0$  are a subset of edges from and to  $n'$ .

Let  $H_0$  be a subset of the references between  $n'$  and onstage nodes, and let  $H_1$  be a subset of the references between  $n'$  and offstage nodes. References in  $H_0$  are moved from  $n'$  to the new node  $n_0$ , because they represent at most one reference, while references in  $H_1$  are copied to  $n_0$  because they may represent multiple concrete heap references. Moving a reference is formalized via the `swing` operation in Figure 14.

The instantiation of a single graph can generate multiple role graphs depending on the choice of  $H'_0$  and  $H'_1$ . The number of graphs generated is limited by the existing references of node  $n'$  and by the `localCheck` requirement for  $n_0$ . This is where our role analysis takes advantage of constraints associated with role definitions to reduce the number of aliasing possibilities that need to be considered.

**Split** The split relation is important for verifying operations on data structures such as skip lists and sparse matrices. It is also useful for improving the precision of the initial set of role graphs on procedure entry (Section 7.2.1).

The goal of the split relation is to exploit the acyclicity constraints associated with role definitions. After a node  $n_0$  is brought onstage, split represents the acyclicity condition of  $\rho(n_0)$  explicitly by eliminating impossible paths in the role graph. It uses additional offstage nodes to encode the reachability information implied by the acyclicity conditions. This information can then be used even after the role of node  $n_0$  changes. In particular, it allows the acyclicity condition of  $n_0$  to be verified when  $n_0$  moves offstage.

**Example 24** Consider a role graph for an acyclic list with nodes LN and a header node L. The instantiated node  $n_0$  is in the middle of the list. Figure 16 a) shows a role graph with a single summary node representing all offstage LN-nodes. Figure 16 b) shows the role graph after applying the split relation. The resulting role graph contains two LN summary nodes. The first LN summary node represents objects definitely reachable from  $n_0$  along `next` edges; the second summary NL node represents objects definitely not reachable from  $n_0$ .

Figure 15 shows the definition of the split operation on node  $n_0$ , denoted by  $\parallel_{n_0}^{n'}$ . Let  $G = \langle H, \rho, K \rangle$  be the initial

Transition	Definition	Condition
$\langle H, \rho, K \rangle \xrightarrow{n, f} \langle H, \rho, K \rangle$		$\langle n, f, n' \rangle \in H, n' \in \text{onstage}(H)$
$\langle H, \rho, K \rangle \xrightarrow{n, f} G'$	$\langle H, \rho, K \rangle \xrightarrow[n']{n_0} \langle H_1, \rho_1, K_1 \rangle \parallel G'$	$\langle n, f, n' \rangle \in H, n' \in \text{offstage}(H)$ $\langle n, f, n_0 \rangle \in H_1$

Figure 13: Expansion Relation

$\langle H, \rho, K \rangle \xrightarrow[n']{n_0} \langle H', \rho', K' \rangle$	$H' = H \setminus H_0 \cup H'_0 \cup H'_1$ $\rho' = \rho[n_0 \mapsto \rho(n')]$ $K' = K[n_0 \mapsto i]$ $\text{localCheck}(n_0, \langle H', \rho', K' \rangle)$ $H_0 \subseteq H \cap (\text{onstage}(H) \times F \times \{n'\} \cup \{n'\} \times F \times \text{onstage}(H))$ $H_1 \subseteq H \cap (\text{offstage}(H) \times F \times \{n'\} \cup \{n'\} \times F \times \text{offstage}(H))$ $H'_0 = \text{swing}(n', n_0, H_0)$ $H'_1 \subseteq \text{swing}(n', n_0, H_1)$
--	--

$$\text{swing}(n_{\text{old}}, n_{\text{new}}, H) = \{ \langle n_{\text{new}}, f, n \rangle \mid \langle n_{\text{old}}, f, n \rangle \in H \} \cup \\ \{ \langle n, f, n_{\text{new}} \rangle \mid \langle n, f, n_{\text{old}} \rangle \in H \} \cup \\ \{ \langle n_{\text{new}}, f, n_{\text{new}} \rangle \mid \langle n_{\text{old}}, f, n_{\text{old}} \rangle \in H \}$$

Figure 14: Instantiation Relation

$$\langle H, \rho, K \rangle \xrightarrow[n']{n_0} \langle H, \rho, K \rangle, \quad \text{acycCheck}(n_0, \langle H, \rho, K \rangle, \text{offstage}(H)) \\ \langle H, \rho, K \rangle \xrightarrow[n']{n_0} \langle H', \rho', K' \rangle, \quad \neg \text{acycCheck}(n_0, \langle H, \rho, K \rangle, \text{offstage}(H))$$

where

$$\begin{aligned} H' &= (H \setminus H_{\text{cyc}}) \cup H_{\text{off}} \cup B_{\text{fNR}} \cup B_{\text{fR}} \cup B_{\text{tNR}} \cup B_{\text{tR}} \cup N_{\text{f}} \cup N_{\text{t}} \\ H_{\text{cyc}} &= \{ \langle n_1, f, n_2 \rangle \mid n_1 \text{ or } n_2 \in S_{\text{cyc}} \} \\ H_{\text{off}} &= \{ \langle n'_1, f, n'_2 \rangle \mid n_1 = c(n'_1), n_2 = c(n'_2), \\ &\quad n_1, n_2 \in \text{offstage}_1(H), n_1 \text{ or } n_2 \in S_{\text{cyc}}, \\ &\quad \langle n_1, f, n_2 \rangle \in H \} \\ &\quad \setminus (S_{\text{R}} \times \text{acyclic}(r) \times S_{\text{NR}}) \\ H \cap (\text{onstage}(H) \times F \cup \{n_0\} \times \text{acyclic}(r)) \times S_{\text{cyc}} &= A_{\text{fNR}} \uplus A_{\text{fR}} \\ H \cap S_{\text{cyc}} \times (\text{acyclic}(r) \times \{n_0\} \cup F \times \text{onstage}(H)) &= A_{\text{tNR}} \uplus A_{\text{tR}} \\ B_{\text{fNR}} &= \{ \langle n_1, f, h_{\text{NR}}(n_2) \rangle \mid \langle n_1, f, n_2 \rangle \in A_{\text{fNR}} \} \\ B_{\text{fR}} &= \{ \langle n_1, f, h_{\text{R}}(n_2) \rangle \mid \langle n_1, f, n_2 \rangle \in A_{\text{fR}} \} \\ B_{\text{tNR}} &= \{ \langle h_{\text{NR}}(n_1), f, n_2 \rangle \mid \langle n_1, f, n_2 \rangle \in A_{\text{tNR}} \} \\ B_{\text{tR}} &= \{ \langle h_{\text{R}}(n_1), f, n_2 \rangle \mid \langle n_1, f, n_2 \rangle \in A_{\text{tR}} \} \\ N_{\text{f}} &= \{ \langle n_0, f, n' \rangle \mid n' \in S_{\text{R}}, \langle n_0, f, c(n') \rangle \in H, f \in \text{acyclic}(r) \} \\ N_{\text{t}} &= \{ \langle n', f, n_0 \rangle \mid n' \in S_{\text{NR}}, \langle c(n'), f, n_0 \rangle \in H, f \in \text{acyclic}(r) \} \\ S_{\text{cyc}} &= \{ n \mid \exists n_1, \dots, n_{p-1} \in \text{offstage}(H) : \\ &\quad \langle n_0, f_0, n_1 \rangle, \dots, \langle n_k, f_k, n \rangle, \langle n, f_{k+1}, n_{k+2} \rangle, \langle n_{p-1}, f_{p-1}, n_0 \rangle \in H, \\ &\quad f_0, \dots, f_{p-1} \in \text{acyclic}(r) \} \\ \text{offstage}_1(H) &= \text{offstage}(H) \setminus \{n_0\} \\ r &= \rho(n_0) \\ \rho'(c(n)) &= \rho(n) \\ K'(c(n)) &= K(n) \end{aligned}$$

Figure 15: Split Relation

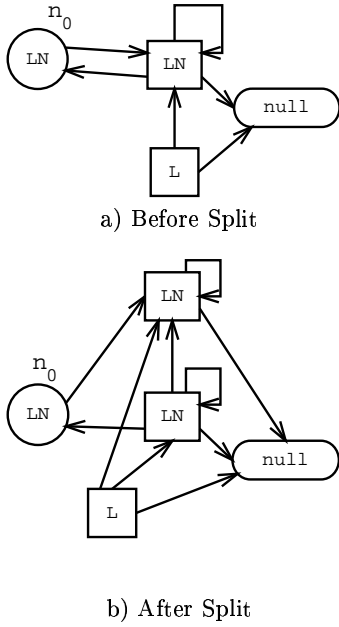


Figure 16: A Role Graph for an Acyclic List

role graph and  $\rho(n_0) = r$ . If  $\text{acyclic}(r) = \emptyset$ , then the split operation returns the original graph  $G$ ; otherwise it proceeds as follows. Call a path in graph  $H$  *cycle-inducing* if all of its nodes are offstage and all of its edges are in  $\text{acyclic}(r)$ . Let  $S_{\text{cyc}}$  be the set of nodes  $n$  such that there is a cycle-inducing path from  $n_0$  to  $n$  and a cycle-inducing path from  $n$  to  $n_0$ .

The goal of the split operation is to split the set  $S_{\text{cyc}}$  into a fresh set of nodes  $S_{\text{NR}}$  representing objects definitely not reachable from  $n_0$  along edges in  $\text{acyclic}(r)$  and a fresh set of nodes  $S_{\text{R}}$  representing objects definitely reachable from  $n_0$ . Each of the newly generated graphs  $H'$  has the following properties:

- 1) merging the corresponding nodes from  $S_{\text{NR}}$  and  $S_{\text{R}}$  in  $H'$  yields the original graph  $H$ ;
- 2)  $n_0$  is not a member of any cycle in  $H'$  consisting of offstage nodes and edges in  $\text{acyclic}(r)$ ;
- 3) onstage nodes in  $H'$  have the same number of fields and aliases as in  $H$ .

Let  $S_0 = \text{nodes}(H) \setminus S_{\text{cyc}}$  and let  $h_{\text{NR}} : S_{\text{cyc}} \rightarrow S_{\text{NR}}$  and  $h_{\text{R}} : S_{\text{cyc}} \rightarrow S_{\text{R}}$  be bijections. Define a function  $c : \text{nodes}(H') \rightarrow \text{nodes}(H)$  as follows:

$$c(n) = \begin{cases} n, & n \in S_0 \\ h_{\text{R}}^{-1}(n), & n \in S_{\text{R}} \\ h_{\text{NR}}^{-1}(n), & n \in S_{\text{NR}} \end{cases}$$

Then  $H' \subseteq \{\langle n'_1, f, n'_2 \rangle \mid \langle c(n'_1), f, c(n'_2) \rangle \in H\}$ .

Because there are two copies of  $S_0$  in  $H'$ , there might be multiple edges  $\langle n'_1, f, n'_2 \rangle$  in  $H'$  corresponding to an edge  $\langle c(n_1), f, c(n_2) \rangle \in H$ .

If both  $n'_1$  and  $n'_2$  are offstage nodes other than  $n_0$ , we always include  $\langle n'_1, f, n'_2 \rangle$  in  $H'$  unless  $\langle n'_1, f, n'_2 \rangle \in S_{\text{R}} \times \text{acyclic}(r) \times S_{\text{NR}}$ . The last restriction prevents cycles in  $H'$ .

For an edge  $\langle n_1, f, n_2 \rangle \in H$  where  $n_1 \in \text{onstage}(H)$  and  $n_2 \in S_{\text{cyc}}$  we include in  $H'$  either the edge  $\langle n_1, f, h_{\text{NR}}(n_2) \rangle$  or  $\langle n_1, f, h_{\text{R}}(n_2) \rangle$  but not both. Split generates multiple graphs  $H'$  to cover both cases. We proceed analogously if  $n_2 \in \text{onstage}(H)$  and  $n_1 \in S_{\text{cyc}}$ . The node  $n_0$  itself is treated in the same way as onstage nodes for  $f \notin \text{acyclic}(r)$ . If  $f \in \text{acyclic}(r)$  then we choose references to  $n_0$  to have a source in  $S_{\text{NR}}$ , whereas the reference from  $n_0$  have the target in  $S_{\text{R}}$ .

Details of the split construction are given in Figure 15. The intuitive meaning of the sets of edges is the following:

- $H_{\text{off}}$  : edges between offstage nodes
- $B_{\text{fNR}}$  : edges from onstage nodes to  $S_{\text{NR}}$
- $B_{\text{fR}}$  : edges from onstage nodes to  $S_{\text{R}}$
- $B_{\text{tNR}}$  : edges from  $S_{\text{NR}}$  to onstage nodes
- $B_{\text{tR}}$  : edges from  $S_{\text{R}}$  to onstage nodes
- $N_{\text{f}}$  :  $\text{acyclic}(r)$ -edges from  $n_0$  to  $S_{\text{R}}$
- $N_{\text{t}}$  :  $\text{acyclic}(r)$ -edges from  $S_{\text{NR}}$  to  $n_0$

The sets  $B_{\text{fNR}}$  and  $B_{\text{fR}}$  are created as images of the sets  $A_{\text{fNR}}$  and  $A_{\text{fR}}$  which partition edges from onstage nodes to nodes in  $S_{\text{cyc}}$ . Similarly, the sets  $B_{\text{tNR}}$  and  $B_{\text{tR}}$  are created as images of the sets  $A_{\text{tNR}}$  and  $A_{\text{tR}}$  which partition edges from nodes in  $S_{\text{cyc}}$  to onstage nodes.

We note that if in the split operation  $S_{\text{cyc}} = \emptyset$  then the operation has no effect and need not be performed. In Figure 16, after performing a single split, there is no need to split for subsequent elements of the list. Examples like this indicate that split will not be invoked frequently during the analysis.

## 6.2.2 Contraction

Figure 17 shows the non-error transitions of the contraction relation  $\stackrel{n}{\sim}$ . The analysis uses contraction when a reference to node  $n$  is removed. If there are other references to  $n$ , the result is the original graph. Otherwise  $n$  has just gone offstage, so analysis invokes `nodeCheck`. If the check fails, the result is  $\perp_G$ . If the role check succeeds, the contraction invokes normalization operation to ensure that the role graph remains bounded. For simplicity, we use normalization whenever `nodeCheck` succeeds, although it is sufficient to perform normalization only at program points adjacent to back edges of the control-flow graph.

**Normalization** Figure 18 shows the normalization relation. Normalization accepts a role graph  $\langle H, \rho, K \rangle$  and produces a normalized role graph  $\langle H', \rho', K' \rangle$  which is a factor graph of  $\langle H, \rho, K \rangle$  under the equivalence relation  $\sim$ . Two offstage nodes are equivalent under  $\sim$  if they have the same role and the same reachability from onstage nodes. Here we consider node  $n$  to be reachable from an onstage node  $n_0$  iff there is some path from  $n_0$  to  $n$  whose edges belong to  $\text{acyclic}(\rho(n_0))$  and whose nodes are all in offstage( $H$ ). Note that, by construction, normalization avoids merging nodes which were previously generated in the split operation  $\parallel$ , while still ensuring a bound on the size of the role graph. For a procedure with  $l$  local variables,  $f$  fields and  $r$  roles the number of nodes in a role graph is on the order of  $r2^l$  so the

$\langle H, \rho, K \rangle \succeq^n \langle H, \rho, K \rangle$	$\exists \mathbf{x} \in \text{var}(\text{proc}) :$ $\langle \text{proc}, \mathbf{x}, n \rangle \in H$
$\langle H, \rho, K \rangle \succeq^n \text{normalize}(\langle H, \rho, K \rangle)$	$\text{nodeCheck}(n, \langle H, \rho, K \rangle, \text{offstage}(H))$

Figure 17: Contraction Relation

$$\text{normalize}(\langle H, \rho, K \rangle) = \langle H', \rho', K' \rangle$$

where  $H' = \{ \langle n_1 / \sim, f, n_2 / \sim \rangle \mid \langle n_1, f, n_2 \rangle \in H \}$   
 $\rho'(n / \sim) = \rho(n)$   
 $K'(n / \sim) = \begin{cases} i, & n / \sim = \{n\}, K(n) = i \\ s, & \text{otherwise} \end{cases}$   
 $n_1 \sim n_2$  iff  $n_1 = n_2$  or  
 $(n_1, n_2 \in \text{offstage}(H), \rho(n_1) = \rho(n_2),$   
 $\forall n_0 \in \text{onstage}(H) : (\text{reach}(n_0, n_1) \text{ iff } \text{reach}(n_0, n_2)))$   
 $\text{reach}(n_0, n) \text{ iff } \exists n_1, \dots, n_{p-1} \in \text{offstage}(n), \exists f_1, \dots, f_p \in \text{acyclic}(\rho(n_0)) :$   
 $\langle n_0, f_1, n_1 \rangle, \dots, \langle n_{p-1}, f_p, n \rangle \in H$

Figure 18: Normalization

maximum size of a chain in the lattice is of the order of  $2^{r^2}$ . To ensure termination we consider role graphs equal up to isomorphism. Isomorphism checking can be done efficiently if normalization assigns canonical names to the equivalence classes it creates.

### 6.2.3 Symbolic Execution

Figure 19 shows the symbolic execution relation  $\xrightarrow{\text{st}}$ . In most cases, the symbolic execution of a statement acts on the abstract heap in the same way that the statement would act on the concrete heap. In particular, the Store statement always performs strong updates. The simplicity of symbolic execution is due to conditions 3) and 5) in the abstraction relation  $\alpha$ . These conditions are ensured by the  $\preceq$  relation which instantiates nodes, allowing strong updates. The symbolic execution also verifies the consistency conditions that are not verified by  $\preceq$  or  $\succeq$ .

**Verifying Reference Removal Consistency** The abstract execution  $\xrightarrow{\text{st}}$  for the Store statement can easily verify the Store safety condition from section 5.4.2, because the set of onstage and offstage nodes is known precisely for every role graph. It returns  $\perp_G$  if the safety condition fails.

**Symbolic Execution of setRole** The  $\text{setRole}(\mathbf{x}:\mathbf{r})$  statement sets the role of node  $n_x$  referenced by variable  $\mathbf{x}$  to  $\mathbf{r}$ . Let  $G = \langle H, \rho, K \rangle$  be the current role graph and let  $\langle \text{proc}, \mathbf{x}, n_x \rangle \in H$ . If  $n_x$  has no adjacent offstage nodes, the role change always succeeds. In general, there are restrictions on when the change can be done. Let  $\langle H_c, \rho_c \rangle$  be a concrete heap with role assignment represented by  $G$  and  $h$  be a homomorphism from  $H_c$  to  $H$ . Let  $h(o_x) = n_x$ . Let  $r_0 = \rho_c(o_x)$ . The symbolic execution must make sure that the condition  $\text{conW}(\rho_c, H_c, \text{offstage}(H_c))$  continues to hold after the role change. Because the set of onstage nodes does not change, it suffices to ensure that the original roles

for offstage nodes are consistent with the new role  $r$ . The acyclicity constraint involves only offstage nodes, so it remains satisfied. The other role constraints are local, so they can only be violated for offstage neighbors of  $n_x$ . To make sure that no violations occur, we require:

1.  $\mathbf{r} \in \text{field}_f(\rho(n))$  for all  $\langle n, f, n_x \rangle \in H$ , and
2.  $\langle \mathbf{r}, f \rangle \in \text{slot}_i(\rho(n))$  for all  $\langle n_x, f, n \rangle \in H$  and every slot  $i$  such that  $\langle r_0, f \rangle \in \text{slot}_i(\rho(n))$

This is sufficient to guarantee  $\text{conW}(\rho_c, H_c, \text{offstage}(H_c))$ . To ensure condition 2) in Definition 22 of the abstraction relation, we require that for every  $\langle f, g \rangle \in \text{identities}(\mathbf{r})$ ,

1.  $\langle f, g \rangle \in \text{identities}(r_0)$  or
2. for all  $\langle n_x, f, n \rangle \in H$ :  $K(n) = i$  and  $(\langle n, g, n' \rangle \in H \text{ implies } n' = n_x)$ .

**Symbolic Execution of roleCheck** To symbolically execute  $\text{roleCheck}(x_1, \dots, x_p, \text{ra})$ , we ensure that the  $\text{conW}$  predicate of the concrete semantics is satisfied for the concrete heaps which correspond to the current abstract role graph. The symbolic execution for  $\text{roleCheck}$  returns the error graph  $\perp_G$  if  $\rho$  is inconsistent with  $\text{ra}$  or if any of the nodes  $n_i$  referenced by  $x_i$  fail to satisfy  $\text{nodeCheck}$ .

### 6.2.4 Node Check

The analysis uses the  $\text{nodeCheck}$  predicate to incrementally maintain the abstraction relation. We first define the predicate  $\text{localCheck}$ , which roughly corresponds to the predicate  $\text{locallyConsistent}$  (Definition 2), but ignores the nonlocal acyclicity condition and additionally ensures condition 2) from Definition 22.

**Definition 25** For a role graph  $G = \langle H, \rho, K \rangle$ , an individual node  $n$  and a set  $S$ , the predicate  $\text{localCheck}(n, G)$  holds iff the following conditions are met. Let  $r = \rho(n)$ .



Statement $s$	Transition	Conditions
$\mathbf{x} = \mathbf{y}.f$	$\langle H \uplus \{\text{proc}, \mathbf{x}, n_x\}, \rho, K \rangle \xrightarrow{s} \langle H \uplus \{\text{proc}, \mathbf{x}, n_f\}, \rho, K \rangle$	$\langle \text{proc}, \mathbf{y}, n_y \rangle, \langle n_y, f, n_f \rangle \in H$
$\mathbf{x}.f = \mathbf{y}$	$\langle H \uplus \{n_x, f, n_f\}, \rho, K \rangle \xrightarrow{s} \langle H \uplus \{n_x, f, n_y\}, \rho, K \rangle$	$\langle \text{proc}, \mathbf{x}, n_x \rangle, \langle \text{proc}, \mathbf{y}, n_y \rangle \in H$ $n_f \in \text{onstage}(H)$
$\mathbf{x} = \mathbf{y}$	$\langle H \uplus \{\text{proc}, \mathbf{x}, n_x\}, \rho, K \rangle \xrightarrow{s} \langle H \uplus \{\text{proc}, \mathbf{x}, n_y\}, \rho, K \rangle$	$\langle \text{proc}, \mathbf{y}, n_y \rangle \in H$
$\mathbf{x} = \text{new}$	$\langle H \uplus \{\text{proc}, \mathbf{x}, n_x\}, \rho, K \rangle \xrightarrow{s} \langle H \uplus \{\text{proc}, \mathbf{x}, n_n\}, \rho', K \rangle$	$n_n$ fresh $\rho' = \rho[n_n \mapsto \text{unknown}]$
$\text{test}(c)$	$\langle H, \rho, K \rangle \xrightarrow{s} \langle H, \rho, K \rangle$	$\text{satisfied}(c, H)$
$\text{setRole}(\mathbf{x}:r)$	$\langle H, \rho, K \rangle \xrightarrow{s} \langle H, \rho[n_x \mapsto r], K \rangle$	$\langle \text{proc}, \mathbf{x}, n_x \rangle \in H$ $\text{roleChOk}(n_x, r, \langle H, \rho, K \rangle)$
$\text{roleCheck}(x_{1..p}, ra)$	$\langle H, \rho, K \rangle \xrightarrow{s} \langle H, \rho, K \rangle$	$\forall i \langle \text{proc}, \mathbf{x}_i, n_i \rangle \in H$ $\text{nodeCheck}(n_i, \langle H, \rho, K \rangle, S)$ $S = \text{offstage}(H) \cup \{n_i\}_i$ $\rho(n_i) = ra(n_i)$

$\text{satisfied}(\mathbf{x}=\mathbf{y}, H_c)$  iff  $\{o \mid \langle \text{proc}, \mathbf{x}, o \rangle \in H_c\} = \{o \mid \langle \text{proc}, \mathbf{y}, o \rangle \in H_c\}$

$\text{satisfied}(!(\mathbf{x}=\mathbf{y}), H_c)$  iff not  $\text{satisfied}(\mathbf{x}=\mathbf{y}, H_c)$

Figure 19: Symbolic Execution of Basic Statements

- 1A. (*Outgoing fields check*) For fields  $f \in F$ , if  $\langle n, f, n' \rangle \in H$  then  $\rho(n') \in \text{field}_f(r)$ .
- 2A. (*Incoming slots check*) Let  $\{\langle n_1, f_1 \rangle, \dots, \langle n_k, f_k \rangle\} = \{\langle n', f \rangle \mid \langle n', f, n \rangle \in H\}$  be the set of all aliases of node  $n$  in abstract heap  $H$ . Then  $k = \text{slotno}(r)$  and there exists a permutation  $p$  of the set  $\{1, \dots, k\}$  such that  $\langle \rho(n_i), f_i \rangle \in \text{slot}_{p_i}(r)$  for all  $i$ .
- 3A. (*Identity Check*) If  $\langle n, f, n' \rangle \in H$ ,  $\langle n', g, n'' \rangle \in H$ ,  $\langle f, g \rangle \in \text{identities}(r)$ , and  $K(n') = i$ , then  $n = n''$ .
- 4A. (*Neighbor Identity Check*) For every edge  $\langle n', f, n \rangle \in H$ , if  $K(n') = i$ ,  $\rho(n') = r'$  and  $\langle f, g \rangle \in \text{identities}(r')$  then  $\langle n, g, n' \rangle \in H$ .
- 5A. (*Field Sanity Check*) For every  $f \in F$  there is exactly one edge  $\langle n, f, n' \rangle \in H$ .

Conditions 1A and 2A correspond to conditions 1) and 2) in Definition 2. Condition 3) in Definition 19 is not necessarily implied by condition 3A) if some of the neighbors of  $n$  are summary nodes. Condition 3) cannot be established based only on summary nodes, because verifying an identity constraint for field  $f$  of node  $n$  where  $\langle n, f, n' \rangle \in H$  requires knowing the identity of  $n'$ , not only its existence and role. We therefore rely on Condition 2) of the Definition 22 to ensure that identity relations of neighbors of node  $n$  are satisfied before  $n$  moves offstage.

The predicate  $\text{acycCheck}(n, G, S)$  verifies the acyclicity condition from Definition 19.

**Definition 26** We say that node  $n$  satisfies an acyclicity check in graph  $G = \langle H, \rho, K \rangle$  with respect to set  $S$ , and we write  $\text{acycCheck}(n, G, S)$ , iff it is not the case that  $H$  contains a cycle  $n_1, f_1, \dots, n_s, f_s, n_1$  where  $n_1 = n$ ,  $f_1, \dots, f_s \in \text{acyclic}(\rho(n))$  and  $n_1, \dots, n_s \in S$ .

This enables us to define the  $\text{nodeCheck}$  predicate.

**Definition 27**  $\text{nodeCheck}(n, G, S)$  holds iff both predicates  $\text{localCheck}(n, G)$  and  $\text{acycCheck}(n, G, S)$  hold.

## 7 Interprocedural Role Analysis

This section describes the interprocedural aspects of our role analysis. Interprocedural role analysis can be viewed as an instance of the functional approach to interprocedural data-flow analysis [41]. For each program point  $p$ , role analysis approximates program traces from procedure entry to point  $p$ . The solution in [41] proposes tagging the entire data-flow fact  $G$  at point  $p$  with the data flow fact  $G_0$  at procedure entry. In contrast, our analysis computes the correspondence between heaps at procedure entry and heaps at point  $p$  at the granularity of sets of objects that constitute role graphs. This allows our analysis to detect which regions of the heap have been modified. We approximate the concrete executions of a procedure with *procedure transfer relations* consisting of 1) an initial context and 2) a set of *effects*. Effects are fine-grained transfer relations which summarize load and store statements and can naturally describe local heap modifications. In this paper we assume that procedure transfer relations are supplied and we are concerned with a) verifying that transfer relations are a conservative approximation of procedure implementation b) instantiating transfer relations at call sites.

### 7.1 Procedure Transfer Relations

A transfer relation for a procedure  $\text{proc}$  extends the procedure signature with an initial context  $\text{context}(\text{proc})$ , and procedure effects  $\text{effect}(\text{proc})$ .

#### 7.1.1 Initial Context

Figures 20 and 21 contain examples of initial context specification. An initial context is a description of the initial role graph  $\langle H_{\text{IC}}, \rho_{\text{IC}}, K_{\text{IC}} \rangle$  where  $\rho_{\text{IC}}$  and  $K_{\text{IC}}$  are determined by a `nodes` declaration and  $H_{\text{IC}}$  is determined by a `edges` declaration. The initial role graph specifies a set of concrete heaps

at procedure entry and assigns names for sets of nodes in these heaps. The next definition is similar to Definition 22.

**Definition 28** We say that a concrete heap  $\langle H_c, \rho_c \rangle$  is represented by the initial role graph  $\langle H_{ic}, \rho_c, K_{ic} \rangle$  and write  $\langle H_c, \rho_c \rangle \alpha_0 \langle H_{ic}, \rho_c, K_{ic} \rangle$ , iff there exists a function  $h_0 : \text{nodes}(H_c) \rightarrow \text{nodes}(H_{ic})$  such that

1.  $\text{conW}(\rho_c, H_c, h_0^{-1}(\text{read}(\text{proc})))$ ;
2.  $h_0$  is a graph homomorphism;
3.  $K_{ic}(n) = i$  implies  $|h_0^{-1}(n)| \leq 1$ ;
4.  $h_0(\text{null}_c) = \text{null}$  and  $h_0(\text{proc}_c) = \text{proc}$ ;
5.  $\rho_c(o) = \rho_c(h_0(o))$  for every object  $o \in \text{nodes}(H_c)$ .

Here  $\text{read}(\text{proc})$  is the set of initial-context nodes read by the procedure (see below). For simplicity, we assume one context per procedure; it is straightforward to generalize the treatment to multiple contexts.

A context is specified by declaring a list of nodes and a list of edges.

A list of nodes is given with `nodes` declaration. It specifies a role for every node at procedure entry. Individual nodes are denoted with lowercase identifiers, summary nodes with uppercase identifiers. By using summary nodes it is possible to indicate disjointness of entire heap regions and reachability between nodes in the heap.

There are two kinds of edges in the initial role graph: parameter edges and heap edges. A parameter edge  $p \rightarrow pn$  is interpreted as  $\langle \text{proc}, p, pn \rangle \in H_{ic}$ . We require every parameter edge to have an individual node as a target, we call such node a *parameter node*. The role of a parameter node referenced by  $\text{param}_i(\text{proc})$  is always  $\text{preR}_i(\text{proc})$ . Since different nodes in the initial role graph denote disjoint sets of concrete objects, parameter edges

```
p1 -> n1
p2 -> n1
```

imply that parameters `p1` and `p2` must be aliased,

```
p1 -> n1
p2 -> n2
```

force `p1` and `p2` to be unaliased, whereas

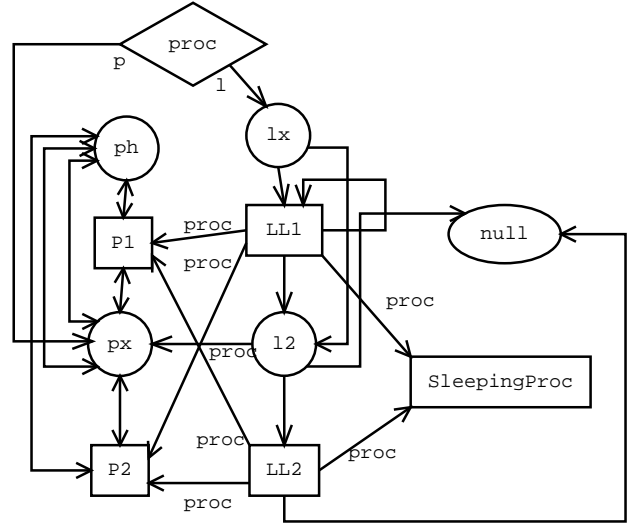
```
p1 -> n1|n2
p2 -> n1|n2
```

allow for both possibilities. A heap edge  $n \text{-f-} m$  denotes  $\langle n, f, m \rangle \in H_{ic}$ . The shorthand notation

```
n1 -f-> n2
    -g-> n3
```

denotes two heap edges  $\langle n1, f, n2 \rangle, \langle n1, g, n3 \rangle \in H_{ic}$ . An expression  $n1 \text{-f-} n2|n3$  denotes two edges  $n1 \text{-f-} n2$  and  $n1 \text{-f-} n3$ . We use similar shorthands for parameter edges.

**Example 29** Figure 20 shows an initial context graph for the `kill` procedure from Example 17. It is a refinement of the role reference diagram of Figure 1 as it gives description of the heap specific to the entry of `kill` procedure. The initial context makes explicit the fact that there is only one header node for the list of running processes (`ph`) and one



```
nodes ph : RunningHeader,
      P1, px, P2 : RunningProc,
      lx : LiveHeader,
      LL1, l2, LL2 : LiveList;
edges p-> px, l-> px,
      ph -next-> P1|px
      -prev-> px|P2,
      P1 -next-> P1|px
      -prev-> ph|P1,
      px -next-> P2|ph
      -prev-> P1|ph,
      P2 -next-> P2|ph
      -prev-> P2|px,
      lx -next-> LL1|l2,
      LL1 -next-> LL1|l2
      -proc-> P1|P2|SleepingProc
      l2 -next-> LL2|null
      -proc-> px,
      LL2 -next-> LL2|null
      -proc-> P1|P2|SleepingProc
```

Figure 20: Initial Context for `kill` Procedure

header node for the list of all active processes (`lx`). More importantly, it shows that traversing the list of active processes reaches a node `l2` whose `proc` field references the parameter node `px`. This is sufficient for the analysis to conclude that there will be no null pointer dereferences in the `while` loop of `kill` procedure since `l2` is reached before `null`.

We assume that the initial context always contains the role reference diagram RRD (Definition 8). Nodes from RRD are called *anonymous nodes* and are referred to via role name. This further reduces the size of initial context specifications by leveraging global role definitions. In Figure 20 there is no need to specify edges originating from `SleepingProc` or even mention the node `SleepingTree`, since role definitions alone contain enough information on this part of the heap to enable the analysis of the procedure.

```

procedure insert(l : L,
               x : IsolatedN ->> LN)
nodes ln, xn;
edges l-> ln, x-> xn,
      ln -next-> LN|null;
effects ln|LN . next = xn,
       ! xn.next = LN|null;
local c, p;
{
  p = l;
  c = l.next;
  while (c!=null) {
    p = c;
    c = p.next;
  }
  p.next = x;
  x.next = c;
  setRole(x:LN);
}

```

Figure 21: Insert Procedure for Acyclic List

### 7.1.2 Procedure Effects

Procedure effects conservatively approximate the region of the heap that the procedure accesses and indicate changes to the referencing relationships in that region. There are two kinds of effects: read effects and write effects.

A *read effect* specifies a set  $\text{read}(\text{proc})$  of initial graph nodes accessed by the procedure. It is used to ensure that the accessibility condition in Section 5.4.3 is satisfied. If the set of nodes denoted by  $\text{read}(\text{proc})$  is mapped to a node  $n$  which is onstage in the caller but is not an argument of the procedure call, a role check error is reported at the call site.

*Write effects* are used to modify caller's role graph to conservatively model the procedure call. A write effect  $e_1.f = e_2$  approximates Store operations within a procedure. The expression  $e_1$  denotes objects being written to,  $f$  denotes the field written, and  $e_2$  denotes the set of objects which could be assigned to the field. Write effects are *may* effects by default, which means that the procedure is free not to perform them. It is possible to specify that a write effect *must* be performed by prefixing it with a “!” sign.

**Example 30** In Figure 21, the `insert` procedure inserts an isolated cell into the end of an acyclic singly linked list. As a result, the role of the cell changes to LN. The initial context declares parameter nodes `ln` and `xn` (whose initial roles are deduced from roles of parameters), and mentions anonymous LN node from a default copy of the role reference diagram RRD. The code of the procedure is summarized with two write effects. The first write effect indicates that the procedure may perform zero or more Store operations to field `next` of nodes mapped to `ln` or `LN` in  $\text{context}(\text{proc})$ . The second write effect indicates that the execution of the procedure must perform a Store to the field `next` of `xn` node where the reference stored is either a node mapped onto anonymous LN node or `null`.

Effects also describe assignments that procedures perform on the newly created nodes. Here we adopt a simple solution of using a single summary node denoted `NEW` to represent

```

procedure insertSome(l : L)
nodes ln;
edges l-> ln,
      ln -next-> LN|null;
effects ln|LN . next = NEW,
       NEW.next = LN|null;
aux c, p, x;
{
  p = l;
  c = l.next;
  while (c!=null) {
    p = c;
    c = p.next;
  }
  x = new;
  p.next = x;
  x.next = c;
  setRole(x:LN);
}

```

Figure 22: Insert Procedure with Object Allocation

all nodes created inside the procedure. We write  $\text{nodes}_0(H_c)$  for the set  $\text{nodes}(H_c) \cup \{\text{NEW}\}$ .

**Example 31** Procedure `insertSome` in Figure 22 is similar to procedure `insert` in Figure 21, except that the node inserted is created inside the procedure. It is therefore referred to in effects via generic summary node `NEW`.

We represent all may write effects as a set  $\text{mayWr}(\text{proc})$  of triples  $\langle n_j, f, n'_j \rangle$  where  $n, n'_j \in \text{nodes}_0(H_c)$  and  $f \in F$ . We represent must write effects as a sequence  $\text{mustWr}_j(\text{proc})$  of subsets of the set  $K_c^{-1}(i) \times F \times \text{nodes}_0(H_c)$ . Here  $1 \leq j \leq \text{mustWrNo}(\text{proc})$ .

To simplify the interpretation of the declared procedure effects in terms of concrete reads and writes, we require the union  $\cup_i \text{mustWr}_i(\text{proc})$  to be disjoint from the set  $\text{mayWr}(\text{proc})$ . We also require the nodes  $n_1, \dots, n_k$  in a must write effect  $n_1 | \dots | n_k.f = e_2$  to be individual nodes. This allows strong updates when instantiating effects (Section 7.3.2).

### 7.1.3 Semantics of Procedure Effects

We now give precise meaning to procedure effects. Our definition is slightly complicated by the desire to capture the set of nodes that are actually read in an execution while still allowing a certain amount of observational equivalence for write effects.

The effects of procedure `proc` define a subset of permissible program traces in the following way. Consider a concrete heap  $H_c$  with role assignment  $\rho_c$  such that  $\langle H_c, \rho_c \rangle \alpha_0 \langle H_c, \rho_c, K_c \rangle$  with graph homomorphism  $h_0$  from Definition 28. Consider a trace  $T$  starting from a state with heap  $H_c$  and role assignment  $\rho_c$ . Extract the subsequence of all loads and stores in trace  $T$ . Replace load  $\text{x=y.f}$  by concrete read  $\text{read } o_x$  where  $o_x$  is the concrete object referenced by `x` at the point of Load, and replace Store  $\text{x.f=y}$  by a concrete write  $\text{write } o_x.f = o_y$  where  $o_x$  is the object referenced by `x` and  $o_y$  object referenced by `y` at the point of Store. Let

$p_1, \dots, p_k$  be the sequence of all concrete read statements and  $q_1, \dots, q_k$  the sequence of all concrete write statements. We say that trace  $T$  starting at  $H_c$  conforms to the effects iff for all choices of  $h_0$  the following conditions hold:

1.  $h_0(o) \in \text{read}(\text{proc})$  for every  $p_i$  of the form `read o`
2. there exists a subsequence  $q_{i_1}, \dots, q_{i_t}$  of  $q_1, \dots, q_k$  such that
  - (a) executing  $q_{i_1}, \dots, q_{i_t}$  on  $H_c$  yields the same result as executing the entire sequence  $q_1, \dots, q_k$
  - (b) the sequence  $q_{i_1}, \dots, q_{i_t}$  implements write effects of procedure `proc`

A typical way to obtain a sequence  $q_{i_1}, \dots, q_{i_t}$  from the sequence  $q_1, \dots, q_k$  is to consider only the last write for each pair  $\langle o_i, f \rangle$  of object and field.

We say that a sequence  $q_{i_1}, \dots, q_{i_t}$  implements write effects `mayWr(proc)` and `mustWri(proc)` for  $1 \leq i \leq i_0$ ,  $i_0 = \text{mustWrNo}$  if and only if there exists an injection  $s : \{1, \dots, i_0\} \rightarrow \{i_1, \dots, i_t\}$  such that

1.  $\langle h'(o), f, h'(o') \rangle \in \text{mustWr}_i(\text{proc})$  for every concrete write  $q_{s(i)}$  of the form `o.f = o'`, and
2.  $\langle h'(o), f, h'(o') \rangle \in \text{mayWr}(\text{proc})$  for all concrete writes  $q_i$  of the form `o.f = o'` for  $i \in \{i_1, \dots, i_t\} \setminus \{s(1), \dots, s(i_0)\}$ .

Here  $h'(n) = h_0(n)$  for  $n \in \text{nodes}(H_c)$  where  $H_c$  is the initial concrete heap and  $h'(n) = \text{NEW}$  otherwise.

It is possible (although not very common) for a single concrete heap  $H_c$  to have multiple homomorphisms  $h_0$  to the initial context  $H_{\text{IC}}$ . Note that in this case we require the trace  $T$  to conform to effects for *all* possible valid choices of  $h_0$ . This places the burden of multiple choices of  $h_0$  on procedure transfer relation verification (Section 7.2) but in turn allows the context matching algorithm in Section 7.3.1 to select an arbitrary homomorphism between a caller's role graph and an initial context.

## 7.2 Verifying Procedure Transfer Relations

In this section we show how the analysis makes sure that a procedure conforms to its specification, expressed as an initial context with a list of effects. To verify procedure effects, we extend the analysis representation from Section 6.1. A non-error role graph is now a tuple  $\langle H, \rho, K, \tau, E \rangle$  where:

1.  $\tau : \text{nodes}(H) \rightarrow \text{nodes}_0(H_{\text{IC}})$  is initial context transformation that assigns an initial context node  $\tau(n) \in \text{nodes}(H_{\text{IC}})$  to every node  $n$  representing objects that existed prior to the procedure call, and assigns `NEW` to every node representing objects created during procedure activation;
2.  $E \subseteq \bigcup_i \text{mustWr}_i(\text{proc})$  is a list of must write effects that procedure has performed so far.

The initial context transformation  $\tau$  tracks how objects have moved since the beginning of procedure activation and is essential for verifying procedure effects which refer to initial context nodes.

We represent the list  $E$  of performed must effects as a partial map from the set  $K_{\text{IC}}^{-1}(i) \times F$  to  $\text{nodes}_0(H_{\text{IC}})$ . This allows

the analysis to perform must effect folding by recording only the last must effect for every pair  $\langle n, f \rangle$  of individual node  $n$  and field  $f$ .

$$\llbracket \text{entry} \bullet \rrbracket = \left\{ \langle H, \rho, K, \tau, E \rangle \mid \begin{array}{l} P : \{\text{proc}\} \times \{\text{param}_i(\text{proc})\}_i \rightarrow N, P \subseteq H_{\text{IC}} \\ H_0 = (H_{\text{IC}} \setminus \{\text{proc}\} \times \text{param}(\text{proc}) \times N) \cup P \\ n_i = P(\text{proc}, \text{param}_i(\text{proc})) \\ H_1 \subseteq H_0 \\ H_1 \setminus H_0 \subseteq \{\langle n', f, n'' \rangle \mid \{n_1, n_2\} \cap \{n_i\}_i \neq \emptyset\} \\ \forall j : \text{localCheck}(n_j, \langle H, \rho, K \rangle, \text{nodes}(H_1)) \\ H_1 \parallel^{n_1} H_2 \parallel^{n_2} \dots \parallel^{n_p} H \\ \rho = \rho_{\text{IC}} \\ K = K_{\text{IC}} \\ \tau = \rho_{\text{IC}} \\ E = \emptyset \end{array} \right\}$$

Figure 23: The Set of Role Graphs at Procedure Entry

### 7.2.1 Role Graphs at Procedure Entry

Our role analysis creates the set of role graphs at procedure entry point from the initial context `context(proc)`. This is simple because role graphs and the initial context have similar abstraction relations (Sections 6.1 and 7.1). The difference is that parameters in role graphs point to exactly one node, and parameter nodes are onstage nodes in role graphs which means that all their edges are “must” edges.

Figure 23 shows the construction of the initial set of role graphs. First the graph  $H_0$  is created such that every parameter `parami(proc)` references exactly one parameter node  $n_i$ . Next graph  $H_1$  is created by using `localCheck` to ensure that parameter nodes have the appropriate number of edges. Finally, the instantiation is performed on parameter nodes to ensure acyclicity constraints if the initial context does not make them explicit already.

### 7.2.2 Verifying Basic Statements

To ensure that a procedure conforms to its transfer relation the analysis uses the initial context transformation  $\tau$  to assign every `Load` and `Store` statement to a declared effect. Figure 24 shows new symbolic execution of `Load`, `Store` and `New` statements.

The symbolic execution of `Load` statement `x=y.f` makes sure that the node being loaded is recorded in some read effect. If this is not the case, an error is reported.

The symbolic execution of the `Store` statement `x.f=y` first retrieves nodes  $\tau(n_x)$  and  $\tau(n_y)$  in the initial role graph context that correspond to nodes  $n_x$  and  $n_y$  in the current role graph. If the effect  $\langle \tau(n_x), f, \tau(n_y) \rangle$  is declared as a may write effect the execution proceeds as usual. Otherwise, the effect is used to update the list  $E$  of must-write effects. The list  $E$  is checked at the end of procedure execution.

The symbolic execution of the `New` statement updates the initial context transformation  $\tau$  assigning  $\tau(n_n) = \text{NEW}$  for the new node  $n_n$ .

Statement s	Transition	Constraints
$x = y.f$	$\langle H \uplus \{\text{proc}, x, n_x\}, \rho, K, \tau, E \rangle \xrightarrow{s} \langle H \uplus \{\text{proc}, x, n_f\}, \rho, K, \tau, E \rangle$	$\langle \text{proc}, y, n_y \rangle, \langle n_y, f, n_f \rangle \in H$ $\tau(n_f) \in \text{read}(\text{proc})$
$x = y.f$	$\langle H \uplus \{\text{proc}, x, n_x\}, \rho, K, \tau, E \rangle \xrightarrow{s} \perp_G$	$\langle \text{proc}, y, n_y \rangle, \langle n_y, f, n_f \rangle \in H$ $\tau(n_f) \notin \text{read}(\text{proc})$
$x.f = y$	$\langle H \uplus \{n_x, f, n_f\}, \rho, K, \tau, E \rangle \xrightarrow{s} \langle H \uplus \{n_x, f, n_y\}, \rho, K, \tau, E \rangle$	$\langle \text{proc}, x, n_x \rangle, \langle \text{proc}, y, n_y \rangle \in H$ $\langle \tau(n_x), f, \tau(n_y) \rangle \in \text{mayWr}(\text{proc})$
$x.f = y$	$\langle H \uplus \{n_x, f, n_f\}, \rho, K, \tau, E \rangle \xrightarrow{s} \langle H \uplus \{n_x, f, n_y\}, \rho, K, \tau, E' \rangle$	$\langle \text{proc}, x, n_x \rangle, \langle \text{proc}, y, n_y \rangle \in H$ $\langle \tau(n_x), f, \tau(n_y) \rangle \in \cup_i \text{mustWr}_i(\text{proc})$ $E' = \text{updateWr}(E, \langle \tau(n_x), f, \tau(n_y) \rangle)$
$x.f = y$	$\langle H \uplus \{n_x, f, n_f\}, \rho, K, \tau, E \rangle \xrightarrow{s} \perp_G$	$\langle \text{proc}, x, n_x \rangle, \langle \text{proc}, y, n_y \rangle \in H$ $\langle \tau(n_x), f, \tau(n_y) \rangle \notin \text{mayWr}(\text{proc}) \cup \cup_i \text{mustWr}_i(\text{proc})$
$x = \text{new}$	$\langle H \uplus \{\text{proc}, x, n_x\}, \rho, K, \tau, E \rangle \xrightarrow{s} \langle H \uplus \{\text{proc}, x, n_n\}, \rho, K, \tau', E \rangle$	$n_n$ fresh $\tau' = \tau[n_n \mapsto \text{NEW}]$

$$\text{updateWr}(E, \langle n_1, f, n_2 \rangle) = E[\langle n_1, f \rangle \mapsto n_2]$$

Figure 24: Verifying Load, Store, and New Statements

The  $\tau$  transformation is similarly updated during other abstract heap operations. Instantiation of node  $n'$  into node  $n_0$  assigns  $\tau(n_0) = \tau(n')$ , split copies values of  $\tau$  into the new set of isomorphic nodes, and normalization does not merge nodes  $n_1$  and  $n_2$  if  $\tau(n_1) \neq \tau(n_2)$ .

### 7.2.3 Verifying Procedure Postconditions

At the end of the procedure, the analysis verifies that  $\rho(n_i) = \text{postR}_i(\text{proc})$  where  $\langle \text{proc}, \text{param}_i(\text{proc}), n_i \rangle \in H$ , and then performs node check on all onstage nodes using predicate  $\text{nodeCheck}(n, \langle H, \rho, K \rangle, \text{nodes}(H))$  for all  $n \in \text{onstage}(H)$ .

At the end of the procedure, the analysis also verifies that every performed effect in  $E = \{e_1, \dots, e_k\}$  can be attributed to exactly one declared must effect. This means that  $k = \text{mustWrNo}(\text{proc})$  and there exists a permutation  $s$  of set  $\{1, \dots, k\}$  such that  $e_{s(i)} \in \text{mustWr}_i(\text{proc})$  for all  $i$ .

## 7.3 Analyzing Call Sites

The set of role graphs at the procedure call site is updated based on the procedure transfer relation as follows. Consider procedure  $\text{proc}$  containing call site  $p \in N_{\text{CFG}}(\text{proc})$  with procedure call  $\text{proc}'(x_1, \dots, x_p)$ . Let  $\langle H_{\text{IC}}, \rho_{\text{IC}}, K_{\text{IC}} \rangle = \text{context}(\text{proc}')$  be the initial context of the callee.

Figure 25 shows the transfer function for procedure call sites. It has the following phases:

- Parameter Check** ensures that roles of parameters conform to the roles expected by the callee  $\text{proc}'$ .
- Context Matching** ( $\text{matchContext}$ ) ensures that the caller's role graphs represent a subset of concrete heaps represented by  $\text{context}(\text{proc}')$ . This is done by deriving a mapping  $\mu$  from the caller's role graph to  $\text{nodes}(H_{\text{IC}})$ .
- Effect Instantiation** ( $\xrightarrow{\text{FX}}$ ) uses effects  $\text{mayWr}(\text{proc}')$  and  $\text{mustWr}_i(\text{proc}')$  in order to approximate all structural changes to the role graph that  $\text{proc}'$  may perform.

$$\begin{aligned} \llbracket \text{proc}'(x_1, \dots, x_p) \rrbracket(\mathcal{G}) = & \\ \text{if } \exists G \in \mathcal{G} : \neg \text{paramCheck}(G) \text{ then } \{ \perp_G \} & \\ \text{else try } \mathcal{G}_1 = \text{matchContext}(\mathcal{G}) & \\ \text{if failed then } \{ \perp_G \} & \\ \text{else } \{ G'' \mid \langle G, \mu \rangle \in \mathcal{G}_1 & \\ \langle \text{addNEW}(G), \mu \rangle \xrightarrow{\text{FX}} \langle G', \mu \rangle \xrightarrow{\text{RR}} G'' \} & \end{aligned}$$

$$\begin{aligned} \text{paramCheck}(\langle H, \rho, K, \tau, E \rangle) \text{ iff} & \\ \forall n_i : \text{nodeCheck}(n_i, G, \text{offstage}(H) \cup \{n_i\}_i) & \\ n_i \text{ are such that } \langle \text{proc}, x_i, n_i \rangle \in H & \end{aligned}$$

$$\begin{aligned} \text{addNEW}(\langle H, \rho, K, \tau, E \rangle) = & \\ \langle H \cup \{n_0\} \times F \times \{\text{null}\}, & \\ \rho[n_0 \mapsto \text{unknown}], & \\ K[n_0 \mapsto s], & \\ \tau[n_0 \mapsto \text{NEW}], & \\ E \rangle & \end{aligned}$$

where  $n_0$  is fresh in  $H$

Figure 25: Procedure Call

- Role Reconstruction** ( $\xrightarrow{\text{RR}}$ ) uses final roles for parameter nodes and global role declarations  $\text{postR}_i(\text{proc}')$  to reconstruct roles of all nodes in the part of the role graph representing modified region of the heap.

The parameter check requires  $\text{nodeCheck}(n_i, G, \text{offstage}(H) \cup \{n_i\}_i)$  for the parameter nodes  $n_i$ . The other three phases are explained in more detail below.

### 7.3.1 Context Matching

Figure 26 shows our context matching function. The  $\text{matchContext}$  function takes a set  $\mathcal{G}$  of role graphs and produces a set of pairs  $\langle G, \mu \rangle$  where  $G = \langle H, \rho, K, \tau, E \rangle$  is a role graph and  $\mu$  is a homomorphism from  $H$  to  $H_{\text{IC}}$ . The homomorphism  $\mu$  guarantees that  $\alpha^{-1}(G) \subseteq \alpha_0^{-1}(\text{context}(\text{proc}'))$

$$\text{matchContext}(\mathcal{G}) = \text{match}(\{\langle G, \text{nodes}(G) \times \{\perp\} \rangle \mid G \in \mathcal{G}\})$$

$$\text{match} : \mathcal{P}(\text{RoleGraphs} \times (N \cup \{\perp\})^N) \rightarrow \mathcal{P}(\text{RoleGraphs} \times N^N)$$

$$\begin{aligned} \text{match}(\Gamma) = & \\ & \Gamma_0 := \{\langle G, \mu \rangle \in \Gamma \mid \mu^{-1}(\perp) \neq \emptyset\}; \\ & \text{if } \Gamma_0 = \emptyset \text{ then return } \Gamma; \\ & \langle \langle H, \rho, K, \tau, E \rangle, \mu \rangle := \text{choose } \Gamma_0; \\ & \Gamma' = \Gamma \setminus \langle \langle H, \rho, K, \tau, E \rangle, \mu \rangle; \\ & \text{paramnodes} := \{n \mid \exists i : \langle \text{proc}, x_i, n \rangle \in H\}; \\ & \text{inaccessible} := \text{onstage}(H) \setminus \text{paramnodes}; \\ & n_0 := \text{choose } \mu^{-1}(\perp); \\ & \text{candidates} := \{n' \in \text{nodes}(H_{\text{IC}}) \mid \\ & \quad (n_0 \notin \text{inaccessible} \text{ and } \rho_{\text{IC}}(n') = \rho(n_0)) \text{ or} \\ & \quad (n_0 \in \text{inaccessible} \text{ and } n' \notin \text{read}(\text{proc}'))\} \\ & \quad \bigcap_{\substack{\langle n_0, f, n \rangle \in H \\ \mu(n) \neq \perp}} \left\{ n' \mid \langle n', f, \mu(n) \rangle \in H_{\text{IC}} \right\} \\ & \quad \bigcap_{\substack{\langle n, f, n_0 \rangle \in H \\ \mu(n) \neq \perp}} \left\{ n' \mid \langle \mu(n), f, n' \rangle \in H_{\text{IC}} \right\}; \\ & \text{if candidates} = \emptyset \text{ then fail}; \\ & \text{if candidates} = \{n'_0\}, K(n_0) = s, K_{\text{IC}}(n'_0) = i, \mu^{-1}(n'_0) = \emptyset \\ & \quad \text{then match}(\Gamma' \cup \{\langle G', \mu[n_1 \mapsto n'_0] \rangle \mid \langle H, \rho, K, \tau, E \rangle \uparrow_{n_0}^{n_1} G'\}) \\ & \text{else } n'_0 := \text{choose } \{n' \in \text{candidates} \mid K(n') = s \text{ or} \\ & \quad (K(n_0) = i, \mu^{-1}(n') = \emptyset)\} \\ & \quad \text{match}(\Gamma' \cup \langle \langle H, \rho, K, \tau, E \rangle, \mu[n_0 \mapsto n'_0] \rangle); \end{aligned}$$

Figure 26: The Context Matching Algorithm

since the homomorphism  $h_0$  from Definition 28 can be constructed from homomorphism  $h$  in Definition 22 by putting  $h_0 = \mu \circ h$ . This implies that it is legal to call  $\text{proc}'$  with any concrete graph represented by  $G$ .

The algorithm in Figure 26 starts with empty maps  $\mu = \text{nodes}(G) \times \{\perp\}$  and extends  $\mu$  until it is defined on all  $\text{nodes}(G)$  or there is no way to extend it further. It proceeds by choosing a role graph  $\langle H, \rho, K, \tau, E \rangle$  and node  $n_0$  for which the mapping  $\mu$  is not defined yet. It then finds candidates in the initial context that  $n_0$  can be mapped to. The candidates are chosen to make sure that  $\mu$  remains a homomorphism. The accessibility requirement—that a procedure may see no nodes with incorrect role—is enforced by making sure that nodes in  $\text{inaccessible}$  are never mapped into nodes in  $\text{read}$  for the callee. As long as this requirement holds, nodes in  $\text{inaccessible}$  can be mapped onto nodes of any role since their role need not be correct anyway. We generally require that the set  $\mu^{-1}(n'_0)$  for individual node  $n'_0$  in the initial context contain at most one node, and this node must be individual. In contrast, there might be many individual and summary nodes mapped onto a summary node. We relax this requirement by performing instantiation of a summary node of the caller if, at some point, that is the only way to extend the mapping  $\mu$  (this corresponds to the first recursive call in the definition of  $\text{match}$  in Figure 26).

The algorithm is nondeterministic in the order in which nodes to be matched are selected. One possible ordering

of nodes is depth-first order in the role graph starting from parameter nodes. If some nondeterministic branch does not succeed, the algorithm backtracks. The function fails if all branches fail. In that case the procedure call is considered illegal and  $\perp_G$  is returned. The algorithm terminates since every procedure call lexicographically increases the sorted list of numbers  $|\mu[\text{nodes}(H)]|$  for  $\langle \langle H, \rho, K, \tau, E \rangle, \mu \rangle \in \Gamma$ .

### 7.3.2 Effect Instantiation

The result of the matching algorithm is a set of pairs  $\langle G, \mu \rangle$  of role graphs and mappings. These pairs are used to instantiate procedure effects in each of the role graphs of the caller. Figure 30 gives rules for effect instantiation. The analysis first verifies that the region read by the callee is included in the region read by the caller. Then it uses  $\text{map } \mu$  to find the inverse image  $S$  of the performed effects. The effects in  $S$  are grouped by the source  $n$  and field  $f$ . Each field  $n.f$  is applied in sequence. There are three cases when applying an effect to  $n.f$ :

1. There is only one node target of the write in  $\text{nodes}(H)$  and the effect is a must write effect. In this case we do a strong update.
2. The condition in 1) is not satisfied, and the node  $n$  is offstage. In this case we conservatively add all relevant edges from  $S$  to  $H$ .

3. The condition in 1) is not satisfied, but the node  $n$  is onstage i.e. it is a parameter node<sup>3</sup>. In this case there is no unique target for  $n.f$ , and we cannot add multiple edges either as this would violate the invariant for onstage nodes. We therefore do case analysis choosing which effect was performed last. If there are no must effects that affect  $n$ , then we also consider the case where the original graph is unchanged.

### 7.3.3 Role Reconstruction

Procedure effects approximate structural changes to the heap, but do not provide information about role changes for non-parameter nodes. We use the role reconstruction algorithm  $\xrightarrow{RR}$  in Figure 27 to conservatively infer possible roles of nodes after the procedure call based on role changes for parameters and global role definitions.

Role reconstruction first finds the set  $N_0$  of all nodes that might be accessed by the callee since these nodes might have their roles changed. Then it splits each node  $n \in N_0$  into  $|R|$  different nodes  $\rho(n, r)$ , one for each role  $r \in R$ . The node  $\rho(n, r)$  represents the subset of objects that were initially represented by  $n$  and have role  $r$  after procedure executes. The edges between nodes in the new graph are derived by simultaneously satisfying 1) structural constraints between nodes of the original graph; and 2) global role constraints from the role reference diagram. The nodes  $\rho(n, r)$  not connected to the parameter nodes are garbage collected in the role graph. In practice, we generate nodes  $\rho(n, r)$  and edges on demand starting from parameters making sure that they are reachable and satisfy both kinds of constraints.

## 8 Extensions

This section presents two extensions of the basic role system. The first extension allows statically unbounded number of aliases for objects. The second extension allows the analysis to verify more complex role changes. Additional ways of extending roles are given in [31].

### 8.1 Multislots

A multislot  $\langle r', f \rangle \in \text{multislots}(r)$  in the definition of role  $r$  allows any number of aliases  $\langle o', f, o \rangle \in H_c$  for  $\rho_c(o') = r'$  and  $\rho_c(o) = r$ . We require multislots  $\text{multislots}(r)$  to be disjoint from all  $\text{slot}_i(r)$ . To handle multislots in role analysis we relax the condition 5) in Definition 22 of the abstraction relation by allowing  $h$  to map more than one concrete edge  $\langle o', f, o \rangle$  onto abstract edge  $\langle n', f, n \rangle \in H$  terminating at an onstage node  $n$  provided that  $\langle \rho(n'), f \rangle \in \text{multislots}(\rho(n))$ . The `nodeCheck` and expansion relation  $\preceq$  are then extended appropriately. Note that a role graph does not represent the exact number of references that fill each multislot. The analysis therefore does not attempt to recognize actions that remove the last reference from the multislot. Once an object plays a role with a multislot, all subsequent roles that it plays must also have the multislot.

<sup>3</sup>Non-parameter onstage nodes are never affected by effects, as guaranteed by the matching algorithm.

```

role BufferNode {
  fields next : BufferNode | null;
  slots BufferNode.next | main.buffer;
  acyclic next;
}
role WorkNode {
  fields next : WorkNode | null;
  WorkNode.next | main.work;
  acyclic next;
}

procedure main()
rootvar buffer : BufferNode | null,
       work : WorkNode | null;
auxvar x, y;
{
  // create buffer and work lists
  ...
  // swap buffer and work
  x = buffer;
  y = work;
  buffer = y;
  work = x;
  setRoleCascade(x:WorkNode, y:BufferNode);
}

```

Figure 28: Example of a Cascading Role Change

### 8.2 Cascading Role Changes

In some cases it is desirable to change roles of an entire set of offstage objects without bringing them onstage. We use the statement `setRoleCascade( $x_1 : r_1, \dots, x_n : r_n$ )` to perform such *cascading role change* of a set of nodes. The need for cascading role changes arises when roles encode reachability properties.

**Example 32** Procedure `main` in Figure 28 has two root variables, `buffer` and `work`, each being a root for a singly linked acyclic list. Elements of the first list have `BufferNode` role and elements of the second list have `WorkNode` role. At some point procedure swaps the root variables `buffer` and `work`, which requires all nodes in both lists to change the roles. These role changes are triggered by the `setRoleCascade` statement. The statement indicates new roles for onstage nodes, and the analysis cascades role changes to offstage nodes.

Given a role graph  $\langle H, \rho, K, E \rangle$  cascading role change finds a new valid role assignment  $\rho'$  where the onstage nodes have desired roles and the roles of offstage nodes are adjusted appropriately. Figure 29 shows abstract execution of the `setRoleCascade` statement. Here  $\text{neighbors}(n, H)$  denotes nodes in  $H$  adjacent to  $n$ . The condition  $\text{cascadingOk}(n, H, \rho, K, \rho')$  makes sure it is legal to change the role of node  $n$  from  $\rho(n)$  to  $\rho'(n)$  given that the neighbors of  $n$  also change role according to  $\rho'$ . This check resembles the check for `setRole` statement in Section 6.2.3. Let  $r = \rho(n)$  and  $r' = \rho'(n)$ . Then  $\text{cascadingOk}(n, H, \rho, K, \rho')$  requires the following conditions:

1.  $\langle n, f, n_1 \rangle \in H$  implies  $\rho'(n_1) \in \text{field}_f(r')$

$$\begin{aligned}
& \langle \langle H, \rho, K, \tau, E \rangle, \mu \rangle \xrightarrow{\text{RR}} \langle H', \rho', K', \tau', E' \rangle \\
& \langle \text{proc}, x_i, n_i \rangle \in H \\
& N_0 = \mu^{-1}[\text{read}(\text{proc}')] \\
& s : N_0 \times R \rightarrow N \text{ where } s(n, r) \text{ are all different nodes fresh in } H \\
& \rho' = \rho \setminus (N_0 \times R) \cup \{ \langle s(n, r), r \rangle \mid n \in N_0, r \in R \} \\
& \quad \setminus (\{n_i\}_i \times R) \cup \{ \langle n_i, \text{postR}_i(\text{proc}') \rangle \} \\
& K'(s(n, r)) = K(n) \\
& \tau'(s(n, r)) = \tau(n) \\
& E' = E \\
& H_0 = H \setminus \{ \langle n_1, f, n_2 \rangle \mid n_1 \in N_0 \text{ or } n_2 \in N_0 \} \\
& \quad \cup \{ \langle s(n_1, r_1), f, s(n_2, r_2) \rangle \mid \langle n_1, f, n_2 \rangle \in H, \langle r_1, f, r_2 \rangle \in \text{RRD} \} \\
& \quad \cup \{ \langle n_1, f, s(n_2, r_2) \rangle \mid \langle n_1, f, n_2 \rangle \in H, \langle \rho_C(\mu(n_1)), f, r_2 \rangle \in \text{RRD} \} \\
& \quad \cup \{ \langle s(n_1, r_1), f, n_2 \rangle \mid \langle n_1, f, n_2 \rangle \in H, \langle r_1, f, \rho_C(\mu(n_2)) \rangle \in \text{RRD} \} \\
& H' = \text{GC}(H_0)
\end{aligned}$$

Figure 27: Call Site Role Reconstruction

$ \begin{aligned} & \langle H, \rho, K, \tau, E \rangle \xrightarrow{\text{S}} \langle H', \rho', K, \tau, E \rangle \\ & s = \text{setRoleCascade}(x_1 : r_1, \dots, x_n : r_n) \end{aligned} $	$ \begin{aligned} & n_i : \langle \text{proc}, x_i, n_i \rangle \in H \\ & \rho'(n_i) = r_i \\ & \rho'(n) = \rho(n), n \in \text{onstage}(H) \setminus \{n_i\}_i \\ & N_0 = \{n \in \text{offstage}(H) \mid \exists n' \in \text{neighbors}(n, H) : \rho(n') \neq \rho'(n')\} \\ & \forall n \in N_0 : \text{cascadingOk}(n, H, \rho, K, \rho') \end{aligned} $
--	---

Figure 29: Abstract Execution for `setRoleCascade`

2.  $\text{slotno}(r') = \text{slotno}(r) = k$ , and for every list  $\langle n_1, f_1, n \rangle, \dots, \langle n_k, f_k, n \rangle \in H$  if there is a permutation  $p : \{1, \dots, k\} \rightarrow \{1, \dots, k\}$  such that  $\langle \rho(n_i), f_i \rangle \in \text{slot}_{p_i}(r)$ , then there is a permutation  $p' : \{1, \dots, k\} \rightarrow \{1, \dots, k\}$  such that  $\langle \rho(n_i), f_i \rangle \in \text{slot}_{p'_i}(r')$ .
3. identity relations were already satisfied or can be explicitly checked:  $\langle f, g \rangle \in \text{identities}(\rho'(n))$  implies
  - (a)  $\langle f, g \rangle \in \text{identities}(\rho(n))$  or
  - (b) for all  $\langle n, f, n' \rangle \in H$ :  $K(n') = i$ , and if  $\langle n', g, n'' \rangle \in H$  then  $n'' = n$
4. either  $\text{acyclic}(\rho'(n)) \subseteq \text{acyclic}(\rho(n))$  or  $\text{acycCheck}(n, \langle H, \rho', K \rangle, \text{offstage}(H))$ .

In practice there may be zero or more solutions that satisfy constraints for a given cascading role change. Selecting any solution that satisfies the constraints is sound with respect to the original semantics. A useful heuristic for searching the solution space is to first explore branches with as few roles changed as possible. If no solutions are found, an error is reported.

## 9 Related Work

Typestate, as a type system extension for statically verifying dynamically changing properties, was proposed in [44, 43]. Aliasing causes problems for typestate-based systems because the declared typestates of all aliases must change whenever the state of the referred object changes. Faced with the complexity of aliasing, [44] resorted to a more controlled language model which avoids aliasing. More recently

proposed typestate approaches use linear types for heap references to support state changes of dynamic allocated objects without addressing aliasing issues [10].

Motivated by the need to enforce safety properties in low-level software systems, [42, 46, 9] use extensions of linear types to describe aliasing of objects and rely on language design to avoid non-local type inference. These systems take a *construction based approach* that specifies data structures as unfoldings of basic elaboration steps [46]. Similarly to shape types [15, 14] and graph types [29, 34], this allows tree-like data structures to be expressed more precisely than using our roles, but cannot approximate data structures such as sparse matrices. More importantly, this approach makes it difficult to express nodes that are members of multiple data structures. Handling multiple data structures is the essential ingredient of our approach because the role of an object depends on data structures in which it participates.

Like shape analysis techniques [5, 17, 39, 40] we have therefore adopted the *constraint based approach* which characterizes data structures in terms of the constraints that they satisfy. The constraint based approach allows us to handle a wider range of data structure while giving up some precision. Like [47, 48] we perform non-local inference of program properties, but while [47, 48] focus on linear integer constraints and handle recursive data structures conservatively, we do not handle integer arithmetic but have a more precise representation of the heap. At a higher level, these approaches all focus on detailed properties of individual data structures. We view our research as focusing more on global aspects such as the participation of objects in multiple data structures.

The path matrix approaches [18, 17] have been used to implement efficient interprocedural analyses that infer one



level of referencing relationships, but are not sufficiently precise to track must aliases of heap objects for programs with destructive updates of more complex data structures.

The use of the instantiation relation in role analysis is analogous to the materialization operation of [39, 40]. Role analysis can also track reachability properties, but we use an abstraction relation based on graph homomorphism rather than 3-valued logic. Our split operation achieves a similar goal to the focus operation of [40]. However, the generic focus algorithm of [32] cannot handle the reachability predicate which is needed for our split operation. This is because it conservatively refuses to focus on edges between two summary nodes to avoid generating an infinite number of structures. Rather than requiring definite values for reachability predicate, our role analysis splits by reachability properties in the abstract role graph, which illustrates the flexibility of the homomorphism-based abstraction relation. Another difference with [40] is that our role analysis does not require the developer to supply the predicate update formulae for instrumentation predicates.

A precise interprocedural analysis [38] extends shape analysis techniques to treat activation records as dynamically allocated structures. The approach also effectively synthesizes an application-specific set of contexts. Our approach differs in that it uses a less precise but more scalable treatment of procedures. It also uses a compositional approach that analyzes each procedure once to verify that it conforms to its specification. Like [48] our interprocedural analysis can apply both may and must effects, but our contexts are general graphs with summary nodes and not trees.

Roles are similar to the ADDS and ASAP data structure description languages [25, 26, 23]. These systems use sound techniques to apply the data structure invariants for parallelization and general dependence testing but do not verify that the data structure invariants are preserved by destructive updates of data structures [24].

The object-oriented community has long been aware of benefits that dynamically changing classes give in large systems [37]. Recognizing these benefits, researchers have proposed dynamic techniques that change the class of an object to reflect its state changes [16, 20, 4, 13]. These systems illustrate the need for a static system that can verify the correct use of objects with changing roles.

## 10 Conclusion

This paper proposes two key ideas: aliasing relationships should determine, in large part, the state of each object, and the type system should use the resulting object states as its fundamental abstraction for describing procedure interfaces and object referencing relationships. We present a role system that realizes these two key ideas in a concrete system, and present an analysis algorithm that can verify that the program correctly respects the constraints of this role system. The result is that programmers can use roles for a variety of purposes: to ensure the correctness of extended procedure interfaces that take the roles of parameters into account, to verify important data structure consistency properties, to express how procedures move objects between data structures, and to check that the program correctly implements correlated relationships between the states of mul-

iple objects. We therefore expect roles to improve the reliability of the program and its transparency to developers and maintainers.

## REFERENCES

- [1] Thomas Ball, Rupak Majumdar, Todd Millstein, and Sriram K. Rajamani. Automatic predicate abstraction of C programs. In *Proceedings of the SIGPLAN '01 Conference on Programming Language Design and Implementation*, 2001.
- [2] Barendsen and J. E. W. Smetsers. Conventional and uniqueness typing in graph rewrite systems. In *Proceedings of the 13th Conference on the Foundations of Software Technology and Theoretical Computer Science 1993, Bombay*, New York, NY, 1993. Springer-Verlag.
- [3] R. Cartwright and M. Fagan. Soft typing. In *Proceedings of the ACM SIGPLAN '91 Conference on Programming Language Design and Implementation (PLDI)*, number 6 in 26, pages 278–292, 1991.
- [4] Craig Chambers. Predicate classes. In Oscar M. Nierstrasz, editor, *Proceedings of the European Conference on Object-Oriented Programming (ECOOP)*, volume 707, pages 268–296, Berlin, Heidelberg, New York, Tokyo, 1993. Springer-Verlag.
- [5] David R. Chase, Mark Wegman, and F. Kenneth Zadeck. Analysis of pointers and structures. In *Proceedings of the SIGPLAN '90 Conference on Programming Language Design and Implementation*, 1990.
- [6] Ramkrishna Chatterjee, Barbara G. Ryder, and William Landi. Relevant context inference. In *Proceedings of the 26th Annual ACM Symposium on the Principles of Programming Languages*, pages 133–146, 1999.
- [7] Ben-Chung Cheng and Wen mei W. Hwu. Modular interprocedural pointer analysis using access paths. In *Proceedings of the SIGPLAN '00 Conference on Programming Language Design and Implementation*, 2000.
- [8] David G. Clarke, John M. Potter, and James Noble. Ownership types for flexible alias protection. In *Proceedings of the 13th Annual Conference on Object-Oriented Programming Systems, Languages and Applications*, 1998.
- [9] Karl Cray, David Walker, and Greg Morrisett. Typed memory management in a calculus of capabilities. In *Proceedings of the 26th Annual ACM Symposium on the Principles of Programming Languages*, 1999.
- [10] Robert DeLine and Manuel Fahndrich. Enforcing high-level protocols in low-level software. In *Proceedings of the SIGPLAN '01 Conference on Programming Language Design and Implementation*, 2001.
- [11] Alain Deutsch. Interprocedural may-alias analysis for pointers: beyond  $k$ -limiting. *ACM SIGPLAN Notices*, 29(6):230–241, 1994.

$$\begin{aligned}
& \langle \langle H, \rho, K, \tau, E \rangle, \mu \rangle \xrightarrow{\text{FX}} \langle \perp_G, \mu \rangle \text{ where } \tau[\mu^{-1}[\text{read}(\text{proc}')] ] \not\subseteq \text{read}(\text{proc}) \\
& \langle \langle H, \rho, K, \tau, E \rangle, \mu \rangle \xrightarrow{\text{FX}} G_t \text{ where } \tau[\mu^{-1}[\text{read}(\text{proc}')] ] \subseteq \text{read}(\text{proc}) \\
& \qquad \qquad \qquad \langle H, \rho, K, \tau, E \rangle \vdash^{n_1, f_1} G_1 \vdash \dots \vdash^{n_t, f_t} G_t \\
S = & \{ \langle n, f, n' \rangle \in H \mid \langle \mu(n), f, \mu(n') \rangle \in \text{mayWr}(\text{proc}') \cup \cup_i \text{mustWr}_i(\text{proc}') \} \\
& \{ \langle n_1, f_1 \rangle, \dots, \langle n_t, f_t \rangle \} = \{ \langle n, f \rangle \mid \langle n, f, n' \rangle \in S \}
\end{aligned}$$

Single Write Effect Instantiation:

$$\langle H_1, \rho_1, K_1, \tau_1, E_1 \rangle \vdash^{n, f} G'$$

iff

case	condition	result
deterministic effect	$ \{n_1 \mid \langle n, f, n_1 \rangle \in S\}  = \{n_0\}$ and $\exists i : \langle \mu(n), f, \mu(n_0) \rangle \in \text{mustWr}_i(\text{proc}')$	$G' = \langle H_2, \rho_1, K_1, \tau_1, E_2 \rangle$ $H_2 = H_1 \setminus \{ \langle n, f, n_1 \rangle \mid \langle n, f, n_1 \rangle \in H_1 \}$ $\cup \{ \langle n, f, n_0 \rangle \}$ $E_2 = \text{updateWr}(E_1, \langle \tau(n), f, \tau(n_0) \rangle)$
nondeterministic effect for non-parameters	$ \{n_1 \mid \langle n, f, n_1 \rangle \in S\}  > 1$ or $\exists n_1 : \langle \mu(n), f, \mu(n_1) \rangle \in \text{mayWr}(\text{proc}')$ $n \in \text{offstage}(H)$ $\{ \langle \tau(n), f, \tau(n_1) \rangle \mid \langle n, f, n_1 \rangle \in S \} \subseteq \text{mayWr}(\text{proc})$	$G' = \langle H_2, \rho_1, K_1, \tau_1, E_2 \rangle$ $H_2 = \text{orem}(H_1) \cup \{ \langle n, f, n_1 \rangle \mid \langle n, f, n_1 \rangle \in S \}$
	$ \{n_1 \mid \langle n, f, n_1 \rangle \in S\}  > 1$ or $\exists n_1 : \langle \mu(n), f, \mu(n_1) \rangle \in \text{mayWr}(\text{proc}')$ $n \in \text{offstage}(H)$ $\{ \langle \tau(n), f, \tau(n_1) \rangle \mid \langle n, f, n_1 \rangle \in S \} \not\subseteq \text{mayWr}(\text{proc})$	$G' = \perp_G$
nondeterministic effect for parameters	$ \{n_1 \mid \langle n, f, n_1 \rangle \in S\}  > 1$ or $\exists n_1 : \langle \mu(n), f, \mu(n_1) \rangle \in \text{mayWr}(\text{proc}')$ $n \notin \text{offstage}(H)$ $\{ \langle \tau(n), f, \tau(n_1) \rangle \mid \langle n, f, n_1 \rangle \in S \} \subseteq \text{mayWr}(\text{proc})$	$G' = \langle H_2, \rho_1, K_1, \tau_1, E_2 \rangle$ $H_0 = H_1 \setminus \{ \langle n, f, n_1 \rangle \mid \langle n, f, n_1 \rangle \in H_1 \}$ $H_2 = H_1$ or $H_2 = H_0 \cup \{ \langle n, f, n_1 \rangle \}$ $\langle n, f, n_1 \rangle \in S$
	$\neg(\{n_1 \mid \langle n, f, n_1 \rangle \in S\} = \{n_1\})$ and $\exists i : \langle \mu(n), f, \mu(n_0) \rangle \in \text{mustWr}_i(\text{proc}')$ $n \notin \text{offstage}(H)$ $\{ \langle \tau(n), f, \tau(n_1) \rangle \mid \langle n, f, n_1 \rangle \in S \} \not\subseteq \text{mayWr}(\text{proc})$	$G' = \perp_G$

$$\text{orem}(H_1) = \begin{cases} H_1 \setminus \{ \langle n, f, n' \rangle \mid \langle n, f, n' \rangle \in H_1 \}, & \text{if } \exists i \exists n' : \langle \mu(n), f, \mu(n') \rangle \in \text{mustWr}_i(\text{proc}') \\ H_1, & \text{otherwise} \end{cases}$$

Figure 30: Effect Instantiation

- [12] Amer Diwan, Kathryn McKinley, and J. Elliot B. Moss. Type-based alias analysis. In *Proceedings of the SIGPLAN '98 Conference on Programming Language Design and Implementation*, 1998.
- [13] S. Drossopoulou, F. Damiani, M. Dezani-Ciancaglini, and P. Giannini. Fickle: Dynamic object reclassification. In *ECOOP'01*, LNCS. Springer, 2001. To appear.
- [14] Pascal Fradet and Daniel Le Metayer. Structured gamma. Technical Report 989, IRISA, 1996.
- [15] Pascal Fradet and Daniel Le Metayer. Shape types. In *Proceedings of the 24th Annual ACM Symposium on the Principles of Programming Languages*, 1997.
- [16] Erich Gamma, Richard Helm, Ralph Johnson, and John Vlisside. *Design Patterns. Elements of Reusable Object-Oriented Software*. Addison-Wesley, Reading, Mass., 1994.
- [17] Rakesh Ghiya and Laurie Hendren. Is it a tree, a DAG, or a cyclic graph? In *Proceedings of the 23rd Annual ACM Symposium on the Principles of Programming Languages*, St. Petersburg Beach, FL, 1996.
- [18] Rakesh Ghiya and Laurie J. Hendren. Connection analysis: A practical interprocedural heap analysis for C. In *Proceedings of the 8th Workshop on Languages and Compilers for Parallel Computing*, 1995.
- [19] Rakesh Ghiya and Laurie J. Hendren. Putting pointer analysis to work. In *Proceedings of the 25th Annual ACM Symposium on the Principles of Programming Languages*, 1998.
- [20] Georg Gottlob, Michael Schrefl, and Brigitte Roeck. Extending object-oriented systems with roles. *ACM Transactions on Information Systems*, 14(3), 1994.
- [21] Samuel Z. Guyer and Calvin Lin. An annotation language for optimizing software libraries. In *Second Conference on Domain Specific Languages*, 1999.
- [22] David Harel, Dexter Kozen, and Jerzy Tiuryn. *Dynamic Logic*. The MIT Press, Cambridge, Mass., 2000.
- [23] Laurie J. Hendren, Joseph Hummel, and Alexandru Nicolau. A general data dependence test for dynamic, pointer-based data structures. In *Proceedings of the SIGPLAN '94 Conference on Programming Language Design and Implementation*, 1994.
- [24] Joseph Hummel. *Data Dependence Testing in the Presence of Pointers and Pointer-Based Data Structures*. PhD thesis, Dept. of Computer Science, Univ. of California at Irvine, 1998.
- [25] Joseph Hummel, Laurie J. Hendren, and Alexandru Nicolau. Abstract description of pointer data structures: An approach for improving the analysis and optimization of imperative programs. *ACM Letters on Programming Languages and Systems*, 1(3), September 1993.
- [26] Joseph Hummel, Laurie J. Hendren, and Alexandru Nicolau. A language for conveying the aliasing properties of dynamic, pointer-based data structures. In *Proceedings of the 8th International Parallel Processing Symposium*, Cancun, Mexico, April 26–29 1994.
- [27] Samin Ishtiaq and Peter W. O'Hearn. Bi as an assertion language for mutable data structures. In *Proceedings of the 28th Annual ACM Symposium on the Principles of Programming Languages*, 2001.
- [28] Pierre Jouvelot and David K. Gifford. Algebraic reconstruction of types and effects. In *Proceedings of the 18th Annual ACM Symposium on the Principles of Programming Languages*, 1991.
- [29] Nils Klarlund and Michael I. Schwartzbach. Graph types. In *Proceedings of the 20th Annual ACM Symposium on the Principles of Programming Languages*, Charleston, SC, 1993.
- [30] Naoki Kobayashi. Quasi-linear types. In *Proceedings of the 26th Annual ACM Symposium on the Principles of Programming Languages*, 1999.
- [31] Viktor Kuncak. Designing an algorithm for role analysis. Master's thesis, Massachusetts Institute of Technology, 2001.
- [32] Tal Lev-Ami. TVLA: A framework for kleene based logic static analyses. Master's thesis, Tel-Aviv University, Israel, 2000.
- [33] Nancy Lynch and Frits Vaandrager. Forward and backward simulations – Part I: Untimed systems. *Information and Computation*, 121(2), 1995.
- [34] Anders Moeller and Michael I. Schwartzbach. The pointer assertion logic engine. In *Proceedings of the SIGPLAN '01 Conference on Programming Language Design and Implementation*, 2001.
- [35] John Plevyak, Vijay Karamcheti, and Andrew A. Chien. Analysis of dynamic structures for efficient parallel execution. In *Workshop on Languages and Compilers for Parallel Architectures*, 1993.
- [36] William Pugh. Skip lists: A probabilistic alternative to balanced trees. In *Communications of the ACM* 33(6):668–676, 1990.
- [37] Trygve Reenskaug. *Working With Objects*. Prentice Hall, 1996.
- [38] Noam Rinetzkky and Mooly Sagiv. Interprocedural shape analysis for recursive programs. In *Proceedings of the 10th International Conference on Compiler Construction*, 2001.
- [39] Mooly Sagiv, Thomas Reps, and Reinhard Wilhelm. Solving shape-analysis problems in languages with destructive updating. In *Proceedings of the 23rd Annual ACM Symposium on the Principles of Programming Languages*, St. Petersburg Beach, FL, 1996.

- [40] Mooly Sagiv, Thomas Reps, and Reinhard Wilhelm. Parametric shape analysis via 3-valued logic. In *Proceedings of the 26th Annual ACM Symposium on the Principles of Programming Languages*, 1999.
- [41] Micha Sharir and Amir Pnueli. Two approaches to interprocedural data flow analysis problems. In *Program Flow Analysis: Theory and Applications*. Prentice-Hall, Inc., 1981.
- [42] F. Smith, D. Walker, and G. Morrisett. Alias types. In *Proceedings of the 14th European Symposium on Programming*, Berlin, Germany, March 2000.
- [43] Robert E. Strom and Daniel M. Yellin. Extending type-state checking using conditional liveness analysis. *IEEE Transactions on Software Engineering*, May 1993.
- [44] Robert E. Strom and Shaula Yemini. Typestate: A programming language concept for enhancing software reliability. *IEEE Transactions on Software Engineering*, January 1986.
- [45] Philip Wadler. Linear types can change the world! In *IFIP TC 2 Working Conference on Programming Concepts and Methods, Sea of Galilee, Israel*, 1990.
- [46] David Walker and Greg Morrisett. Alias types for recursive data structures. In *Workshop on Types in Compilation*, 2000.
- [47] Zhichen Xu, Barton Miller, and Thomas Reps. Safety checking of machine code. In *Proceedings of the SIGPLAN '00 Conference on Programming Language Design and Implementation*, 2000.
- [48] Zhichen Xu, Thomas Reps, and Barton Miller. Type-state checking of machine code. In *Proceedings of the 15th European Symposium on Programming*, 2001.