On Role Logic
Viktor Kuncak and Martin Rinard
On Role Logic

Viktor Kuncak and Martin Rinard
Computer Science and Artificial Intelligence Laboratory
Massachusetts Institute of Technology
Cambridge, MA 02139, USA
{vkuncak, rinard}@csail.mit.edu

MIT CSAIL Technical Report No 925
Internal Manuscript VK0101, October 2003

Abstract

We present role logic, a notation for describing properties of relational structures in shape analysis, databases, and knowledge bases. We construct role logic using the ideas of de Bruijn's notation for lambda calculus, an encoding of first-order logic in lambda calculus, and a simple rule for implicit arguments of unary and binary predicates.

The unrestricted version of role logic has the expressive power of first-order logic with transitive closure. Using a syntactic restriction on role logic formulas, we identify a natural fragment RL^2 of role logic. We show that the RL^2 fragment has the same expressive power as two-variable logic with counting C^2, and is therefore decidable.

We present a translation of an imperative language into the decidable fragment RL^2, which allows compositional verification of programs that manipulate relational structures. In addition, we show how RL^2 encodes boolean shape analysis constraints and an expressive description logic.

Keywords: Program Verification, Shape Analysis, Static Analysis, Two-Variable Logic with Counting, Description Logic, First-Order Logic, Types, Roles, Object-Models

Draft of October 31, 2003, 1:37pm,
see http://www.mit.edu/~vkuncak/papers for later versions.

Contents

1 Introduction 2
2 Example 2
3 A Recipe for Role Logic 4
3.1 Lambda Calculus 4
3.2 De Bruijn Notation 4
3.3 Predicate Logic in Lambda Calculus 4
3.4 Implicit De Bruijn Indices 5
3.5 Shorthands 6
3.6 Role Logic 6
3.7 Lambda Calculus for Predicate Definitions 6
4 Role Logic Subset RL^2 and its Decidability 7
4.1 The Role Logic Subset RL^2 8
4.2 Two-Variable Logics C^2 and D^2 8
4.3 From C^2 to RL^2 via I^2 9
4.4 From RL^2 to D^2: Closing the Loop 12
5 Applications of Role Logic 12
5.1 Static Analysis Based on RL^2 12
5.2 Describing Boolean Shape Analysis Constraints 16
5.3 Encoding an Expressive Descriptive Logic 17
6 Related Work 17
7 Conclusions 18
1 Introduction

Systems as relational structures. Complex systems arising in many areas of Computer Science can be naturally represented as relational structures. The state of an imperative program can be specified using sets and relations denoted by unary and binary predicates \([24, 32, 66, 8]\), especially for object-oriented programs [36, 63]; a relational database is a finite relational structure \([18, 16]\); knowledge bases and deductive databases can also be based on predicate logic [1, 41, 53].

Shape analysis. Shape analysis techniques [65, 29, 33, 26, 27, 25, 17, 40, 39, 43, 37, 55] can verify and derive precise properties of objects in the heap. Shape analysis is therefore important for reasoning about programs written in modern imperative programming languages. Shape analysis is also promising as a general-purpose verification technique, because of its ability to reason about graphs as general structures, and the ability to summarize properties of unbounded sets of objects.

Many of the shape analysis techniques have a logical foundation: [65] is based on (two-valued and three-valued) first-order logic with transitive closure, [39, 40, 37, 55] is based on monadic second-order logic of trees, [26, 27] is based on graph grammars which are closely related to monadic second-order logic of trees [62]. Theorem proving is used in [33] to derive consequences of axioms about data structures. Many shape analyses perform abstract interpretation [19] to synthesize loop invariants [65, 29, 43].

Role logic. This paper presents role logic, a notation for describing properties of relational structures in shape analysis, databases, and knowledge bases. Role logic is an attempt to simultaneously achieve the simplicity of the role declarations of [43] with a transparent connection with the well-established first-order logic.

On the one hand, the full role logic has the expressive power of first-order logic with transitive closure, which makes it as expressive as the logic of \([65, 36]\) and more expressive than the original role constraints [43]. For example, role logic is closed under all propositional operations and generalizes boolean shape analysis constraints [48]. Role logic formulas easily translate into the traditional first-order logic notation.

On the other hand, like the specialized notation for declaring roles in [43], role logic allows natural description of common properties of imperative data structures with mutable references. Like dynamic logics [31] and description logics [1], role logic allows suppressing names of variables, which often leads to concise specifications. The conciseness of role logic makes it an appealing choice for lightweight annotations in a programming language.

Another property that role logic shares with description logics is that an interesting subset of role logic is decidable. We show the decidability of the fragment RL\(^2\) of role logic in Section 4 by establishing a correspondence with the two-variable logic with counting \(C^2\) [30, 57]. While many description logics are known to be representable in \(C^2\) but are potentially weaker than \(C^2\), the fragment RL\(^2\) of role logic matches precisely the expressive power of \(C^2\).

Contributions. The following are the main contributions of this paper:

1. We introduce role logic, which applies the ideas of implicit arguments and deBruijn's lambda calculus notation to first order logic (Section 3). The result is a concise way of specifying properties of first-order structures that arise in shape analysis, databases, and knowledge bases.

2. We define a variable-free subset RL\(^2\) of role logic (Section 4). We give a translation of RL\(^2\) formulas to formulas of two-variable logic with counting \(C^2\). This translation implies that RL\(^2\) is decidable, because \(C^2\) is decidable [30]. We further give a translation of \(C^2\) formulas to RL\(^2\) formulas. These two translations imply that RL\(^2\) is just as expressive as \(C^2\).

3. As the main application of role logic, in Section 5.1 we present a compositional shape analysis technique. We introduce a unified language for writing implementations, specifications, and conformance claims. The constructs of the language denote relations on program states expressible in the decidable fragment RL\(^2\). The analysis technique is based on generating verification conditions in RL\(^2\) and applying the decision procedure for RL\(^2\). The analysis verifies the correctness of dynamically changing referencing relationships between objects by showing that procedures conform to their specifications. By conjoining procedure specifications with global invariants, the analysis can also show that the program preserves the key data structure consistency properties necessary for the correct execution of the program.

4. We present two additional applications of role logic:
   (a) we show in Section 5.3 that a subset of role logic RL\(^2\) naturally corresponds to an expressive description logic [1, Chapter 5];
   (b) we note in Section 5.2 that boolean shape analysis constraints [48], which can describe the basic structure of data-flow facts in \([65]\), are a subset of constraints expressible in role logic.

2 Example

To give a flavor of role logic, we present an example that illustrates one aspect of a client-server manager system that assigns clients to servers. Figure 1 is a standard object model that graphically displays the system, using boxes to represent sets, arrows to represent relations, and intervals \(N:M\) to represent constraints on relations. Figure 2 describes the same system using role logic. Figure 3 presents a fragment of the code of the system. The code is expressed in an imperative language extended with specification constructs.

![Figure 1: An object model for a component of client-server manager](image-url)
GlobalInvariant =
{Servers} \land (\text{disjoint } \text{Servers, Clients}) \land
(\text{partition Clients, WaitingClients, AssignedClients}) \land
\lbrack \text{server } \Rightarrow \text{AssignedClients'} \land \text{Servers} \rbrack \land
\lbrack \text{clients } \cong \text{server} \rbrack \land
\lbrack \text{AssignedClients } \Rightarrow \text{card}^=\text{clients} \rbrack \land
\lbrack \text{Servers } \Rightarrow \text{card}^=\text{server} \rbrack \land
\lbrack \text{AssignedClients } \Rightarrow \text{card}^=\text{clients} \rbrack

Example consequence:

\[
P \equiv \lbrack \text{WaitingClients } \Rightarrow \lbrack \lnot(\text{clients } \land \text{server} \land \text{clients } \land \lnot \text{server} \rbrack \rbrack
\]

Figure 2: Global constraints of the client-server manager, expressed in role logic

Global constraints. Figure 2 describes the global constraints of a client-server manager system using a conjunction of role logic formulas. There are two basic kinds of objects in the system: servers and clients. We model these objects using two disjoint sets Clients and Servers. The set Clients is further partitioned into the set AssignedClients of objects that have been assigned to servers, and the set WaitingClients that have not been assigned yet. The disjoint, partition, and other constructs of set algebra of sets and relations (\cap, \cup, \setminus) are definable in role logic.

We require the set Servers to be non-empty, which we denote by \{Servers\}, with the meaning \lbrack \text{Ser}v\text{ers}(x)\rbrack. The constraint \lbrack \text{server } \Rightarrow \text{AssignedClients'} \land \text{Servers} \rbrack translates to \forall x. y. \text{server}(x, y) \Rightarrow \text{AssignedClients}(x) \land \text{Servers}(y). Namely, the brackets \{\} corresponds to a universal quantifier. An occurrence of a binary predicate (such as server) is implicitly supplied with the previous-innermost bound variable (here, x) and the innermost bound variable (here, y). The occurrence of an unary predicate Servers is supplied with the innermost bound variable (y), unless the unary predicate is printed in which case the previous-innermost bound variable (in this case x) is supplied instead. The constraint \lbrack \text{clients } \cong \text{server} \rbrack means that the relation clients is the inverse of the relation server. The constraint \lbrack \text{Servers } \Rightarrow \text{card}^=\text{clients} \rbrack translates into the formula \forall x. \text{Servers}(x) \Rightarrow \exists^=y. \text{clients}(x, y) in first-order logic with counting quantifiers.

Note that all of our translations of constraints in Figure 2 use only two variables, x and y. In fact, our entire example is expressed in the RL^2 fragment of role logic. In Section 4 we show that RL^2 corresponds to the decidable fragment C^2 of two-variable first-order logic with counting, and is therefore decidable. Figure 2 presents the formula P, denoting the fact that WaitingClients objects have no incoming or outgoing edges. If we apply the decision procedure for RL^2, we can show that GlobalInvariant \Rightarrow P is a valid formula, which means that P is a logical consequence of GlobalInvariant. By querying whether the GlobalInvariant implies properties of interest such as P, the developers can increase their confidence in the correctness and completeness of the design. Moreover, our technique can be used to show the conformance of the program with respect to the design.

proc assignClients() =
spec \text{old}(\text{GlobalInvariant}) \Rightarrow \lbrack \text{WaitingClients}\rbrack \land
\lbrack \text{AssignedClients } \cong \text{WaitingClients}\rbrack \land
\lbrack \text{AssignedClients } \cong \text{AssignedClients} \land \text{GlobalInvariant} \rbrack

proc assignOneClientIMPL() = {
    if \lbrack \text{WaitingClients}\rbrack {
        \text{cl} := \text{getWaitingClient}();
        \text{assignOneClientIMPL(cl)};
        \text{assignOneClientIMPL};
    } else {
        \text{assignOneClientIMPL(cl)};
    }
}
claim: assignOneClientIMPL \Rightarrow assignOneClient

proc assignOneClient(cl) =
spec \text{old}(\text{GlobalInvariant} \land
\lbrack \text{AssignedClients } \cong \text{WaitingClients}\rbrack \land
\lbrack \text{AssignedClients } \cong \text{AssignedClients} \land \text{GlobalInvariant} \rbrack

proc assignOneClientIMPL(cl) = {
    \text{sv} := \text{getServer}();
    if (\text{Card} (\text{sv} \land \text{clients}) \neq 4) {
        \text{AssignedClients} := \text{AssignedClients} \land \text{cl};
        \text{WaitingClients} := \text{WaitingClients} \land \text{cl};
        \text{sv.c}l\text{ients} := \text{sv.c}l\text{ients} \land \text{cl};
    } else {
        \text{assignOneClientIMPL(cl)};
    }
}
claim: assignOneClientIMPL \Rightarrow assignOneClient

proc getClient() : \text{set} =
spec \text{WaitingClients} \Rightarrow
\text{Skip} \land \text{getWaitingClient}()

proc getServer() : \text{set} =
spec \\{\text{Servers}\} \Rightarrow
\text{Skip} \land \text{getServer}()

Figure 3: A fragment of a program that assigns WaitingClients to Servers
Program fragment. Figure 3 shows a fragment of the code of the client-server manager. The top-level procedure in the code is a tail-recursive procedure assignClientsImpl that processes all WaitingClients objects and assigns them to Servers objects. The assignClientsImpl procedure terminates if there are no WaitingClients objects. Otherwise, it uses the getWaitingClient procedure to obtain an element of WaitingClients and assigns it to some Servers object using the assignOneClient procedure, and continues with the next WaitingClients object using a tail-recursive call.

The partial correctness of the procedure assignClientsImpl is given using the specification assignClients. The requirement that the procedure conforms to its specification is stated using the construct

\textbf{claim:} assignClientsImpl \Rightarrow assignClients

The verification of each procedure call site uses only procedure specification (summary) instead of the body of the procedure, which allows verification of recursive procedures. In this example, the implementations of procedures getWaitingClient and getServer are not available, which illustrates the advantage of assume/guarantee reasoning for partitioning a verification task.

Using the translation in Section 5.1, the claim constructs are reduced to verification conditions expressed in role logic. For a large class of constructs presented in Section 5.1, and our example in particular, the resulting verification conditions belong to the decidable RL^2 and can therefore be discharged using a decision procedure for RL^2.

Note that we are able to express detailed specifications of the correctness of procedures while remaining in the decidable logic. For example, the specification assignClients ensures that the entire global invariant in Figure 2 is preserved, and that no client objects are lost in the assignment process; after assignClients, the set AssignedClients is the union of the old value of AssignedClients and the old value of WaitingClients, whereas the new value of WaitingClients is an empty set.

3 A Recipe for Role Logic

In this section we motivate the role logic by constructing it in several steps. We start with first-order logic encoded in the simply typed lambda calculus; we then move to the notation that refers to each variable by its index. Finally, we impose a rule for implicitly supplying the indices of variables to predicate symbols. Later, in Section 3.6, we summarize the syntax and the semantics of role logic, and in Section 4 we present a decidable sublogic of role logic.

3.1 Lambda Calculus

Figure 4 presents simply typed lambda calculus with explicit type annotations in lambda abstraction (the Church-style simply typed lambda calculus [5, Section 3.2]). This calculus is our starting point.

As primitive types we use bool for boolean values, and obj for objects. As the only type constructor we use arrow \(\to\). We introduce \(\text{ref}^k\) as a shorthand type defined by

\[
\text{ref}^k \equiv \text{bool} \quad \text{ref}^{k+1} \equiv \text{obj} \to \text{ref}^k
\]

Simple types enable us to give a simple set-theoretic semantics to formulas by interpreting lambda abstractions as total functions. The resulting semantics is in Figure 4; the semantics is straightforward because we use lambda calculus itself as our meta-notation.

3.2 De Bruijn Notation

An alternative to referring to each bound variable by its name is to refer to each variable by its number, with number 1 denoting the most recently bound variable. This is the idea behind de Bruijn indices for lambda calculus [22, 4]. Figure 5 presents the syntax and the semantics of lambda calculus notation with de Bruijn indices. The environment maps the keyword \text{stack} to a stack (i.e., a list) of elements of the domain. If \(h\) is an element and \(l\) a list, then the notation \(h : l\) denotes the list with the head \(h\) and the tail \(l\). The abstraction pushes a value onto the stack; the index \(k\) retrieves the \(k\)-th element from the top of the stack.

3.3 Predicate Logic in Lambda Calculus

We next encode first-order logic with equality in lambda calculus. We use \text{EQ} to denote the binary equality relation. We assume that the interpretation of relation symbols is specified in the environment \(e\). We introduce conjunction and negation as logical operations acting on booleans (the remaining propositional operations are defined in terms of \(\land, \neg\), as usual). We use the abstraction in lambda calculus to encode bound variables of predicate calculus. This is the usual higher-order logic encoding of classical first-order logic, as used, for example, in Isabelle interactive theorem prover [58]. Figure 6 presents this encoding of quantifiers.
Form = ⟨Nat⟩

variable lookup
Nat = {1, 2, ...}

| Form Form | function application |
| λ: Type.Form | function abstraction |

Syntax

[[θ]] e = get i e
[[F_1 F_2]] e = ([[F_1]] e) ([[F_2]] e)
[[λ: T.F]] e = λd. [[F]] (push d e)

Semantics

gi e = nthi (e stack)
push de = e[stack := d : (e stack)]
rth i (h : l) = h
rth (i + 1) (h : l) = rth i l

Auxiliary Functions

Figure 5: De Bruijn Form of Simply Typed Lambda Calculus

{F} ≡ ∀(λ: obj.F)
[F] ≡ ¬¬F

Quantifier Brackets

When Γ(r) = ref then write r instead of r(k)(k-1)...(1)

Default Argument Rule

~F ≡ (λλF(1)(2)
F' ≡ (λλF(2)(2)
card^{=k} F ≡ {k (λF(1) ∧ ... ∧ (λF)(k) ∧
\Lambda_{1 \leq i < j \leq k} ¬EQ(θ i j) }^k

card^{=k} F ≡ card^{=k} F \land ¬card^{=k+1} F
(\Sigma_{i=1}^n Card F_i) \geq k ≡ \bigvee_{\sum_{i=1}^n k_i = k} \Lambda_{i=1}^n \text{card}^{=k_i} F_i
(\Sigma_{i=1}^n Card F_i) = k ≡ \bigvee_{\sum_{i=1}^n k_i = k} \Lambda_{i=1}^n \text{card}^{=k_i} F_i
disjoint F_1, ..., F_n ≡ \bigwedge_{1 \leq i < j \leq n} ¬(F_i \land F_j)
partition F; F_1, ..., F_n ≡ disjoint F_1, ..., F_n \land
[F \Leftrightarrow \bigwedge_{i=1}^n F_i]

F_1 \setminus F_2 ≡ F_1 \land ¬F_2

Shorthands

Figure 7: de Bruijn form of Predicate Calculus

To remain within first-order logic, we require the quantifier ∃ to have monomorphic type (obj → bool) → bool (see also Section 3.7).

3.4 Implicit De Bruijn Indices

Figure 7 shows how we combine the encoding of first-order logic in higher-order logic and de Bruijn’s notation for lambda calculi.

Example 1 First-order predicate calculus formula

∀x ∀y, f(x, y) ⇒ A(x) ∧ B(y)
can be written in this notation as

[[∀x)(λy.f(x, y)](A(x) ∧ B(y))

The outermost [ ] bracket acts as the quantifier ∀x; the variable x is referred to inside the formula as (2) because it is the second innermost bound variable. The innermost [ ] bracket acts as ∀y; the variable y is referred to as (1).

The interpretation environment e contains both the stack for de Bruijn indices and the bindings of relation symbols such...
as $A$ and $f$ in Example 1. Relational symbols of predicate logic correspond to variables of type $\text{ref}_k$. We use the abstraction over de Bruijn indices $\lambda T \text{ref}_k$ only when $T \equiv \text{obj}$, and write the abstraction simply $\lambda T F$. For every environment $e$, the value (e_stack) is a list of elements of type $\text{obj}$.

We next introduce the Default Argument Rule: we omit de Bruijn indices from the expression $r(k)(k-1)\ldots(1)$ when $r$ is a relation symbol, that is, when $\Gamma(r) = \text{ref}_0$. We interpret every occurrence of variable $r$ when $\Gamma(r) = \text{ref}_k$ as $r(k)(k-1)\ldots(1)$.

Example 2 The Default Argument Rule means that instead of

$$[[f(2)(1) \Rightarrow A(2) \land B(1)]]$$

we write

$$[[f \Rightarrow (\lambda A)(2) \land B]]$$

when $\Gamma(f) = \text{ref}_2$ and $\Gamma(A) = \Gamma(B) = \text{ref}_1$.

We lose no expressive power by the Default Argument Rule. For example, if we wish to denote $r(\bar{i}_1)(\bar{i}_2)(\bar{i}_3)$, we write $(\lambda \bar{a})(\bar{a})(\bar{a})(\bar{a})$. Note that the Default Argument Rule applies only to the relation symbols, not to all subformulas, so $(\lambda \lambda \lambda \lambda)$ with Default Argument rule is equivalent to $r$ without Default Argument Rule. In general, if $r$ is a $n$-ary relation, we write $(\lambda \bar{a}_n)r(\bar{i}_1)(\bar{i}_2)\ldots(\bar{i}_n)$ where we would previously write $r(\bar{i}_1)(\bar{i}_2)\ldots(\bar{i}_n)$.

3.5 Shorthands

Figure 7 introduces some shorthands. Tilde $\sim$ swaps two topmost stack elements (1) and (2). Prime $'$ replaces the top (1) with the element (2). An expression $\text{card}^{\bar{a}_n}_n F$, for an integer $k \geq 0$, corresponds to a counting quantifier in first-order logic [30]. A counting quantifier states that the number of elements with some property is greater than or equal to $k$. Figure 7 also introduces the shorthand for $\text{card}^{\bar{a}_n}_n F$ and the shorthand $\text{Card}$ for specifying a constraint on a sum of cardinalities. The shorthands containing $\leq$ are defined similarly.

These shorthands play two purposes. On the one hand they allow expressing certain properties in a more concise way. On the other hand, if we use the shorthands but give up the ability to refer to indices explicitly, we obtain a fragment of first-order logic that is equivalent to two-variable first-order logic with counting (Section 4) and therefore decidable [30].

Example 3 Using the shorthands, we write the formula

$$\forall x \forall y, f(x, y) \Rightarrow A(x) \land B(y)$$

as

$$[[f \Rightarrow A' \land B]]$$

The convenience of role logic is even more evident in larger formulas like

$$\forall x. A(x) \Rightarrow (\forall y. f(x, y) \Rightarrow B(y) \lor C(y)) \land (\forall z. g(x, z) \Rightarrow D(z))$$

which can be written as

$$[A \Rightarrow [f \Rightarrow B \lor C] \land [g \Rightarrow D]] \quad (1)$$

Figure 8: Transitive Closure Construct and Shorthands

Formulas of form (1) are useful for describing properties of first-order structures that arise in shape analysis, see e.g., [48, 47, 71].

3.6 Role Logic

Figure 9 summarizes the syntax of role logic. The semantics of role logic follows from Section 3.

We next explain the purpose of lambda abstraction in our logic.

3.7 Lambda Calculus for Predicate Definitions

In the resulting role logic of Figure 9 we retain the named variables in the environment, and we allow abstraction over these named variables. As a result, there two kinds of lambda abstraction: abstraction over de Bruijn indices and abstraction over named variables. Abstraction over a de Bruijn index is always over (1) which denotes an object of type obj, such abstraction is written $\lambda T F$. The abstraction over a named variable may abstract over variables of more complex types and is written $\lambda x : T.F$. There is only one kind of lambda calculus application; both $(\lambda f_1)f_2$ and $(\lambda x : T.F)F$ are reduced.

The purpose of the named lambda abstraction $\lambda x : T.F$ is twofold. First, when $T \equiv \text{obj}$, then we can write $\exists x : \text{obj}.F$ as in the usual first-order predicate calculus. Second, when $T$ is not obj, we can encode acyclic definitions of higher-order predicates that can be subsequently substituted away. Define the expression

$$\text{let } P : T = F_1 \text{ in } F_2$$
Form = Vars
| (Nat) named object or predicate
| EQ de Bruijn index of an object variable
| Form \wedge Form equality between (1) and (2)
| ¬Form conjunction
| \exists Form negation
| \lambda Form existential quantification over objects
| \lambda Vars : Type . Form de Bruijn abstraction over objects
| Form Form abstraction over named variables
| Form’ function application
| Form∗ at least k objects satisfy F
| card^k Form reflection transitive closure

Figure 9: The Syntax of Role Logic

to be equivalent to

(\lambda P : T . F_2) F_1

Such definitions are very useful for describing complex data structures.

Note that acyclic definitions introduced through typed lambda calculus via bindings \lambda x : T.F for T \neq bool do not make the logic higher-order, because we define the quantifier \exists to always have the monomorphic type (obj \rightarrow bool) \rightarrow bool, and the reflexive-transitive closure operator * to have the type

(obj \rightarrow obj \rightarrow bool) \rightarrow (obj \rightarrow obj \rightarrow bool)

Consider a well-typed formula F whose only free variables are relation symbols, and whose de Bruijn indices only refer to indices bound in the formula. Assume that we have applied the Default Argument Rule, so that all de Bruijn indices are explicit. Then we may treat de Bruijn abstraction as the usual abstraction over a disjoint set of variables. By strong normalization of simply typed lambda calculus [5], let F^0 be the normal form of F. We claim that in F^0 the only occurrence of lambda abstraction is within expressions of the form \exists(\lambda x : obj.F) or rtrans(\lambda x : obj.\lambda y : obj.F).

To show the claim, consider an occurrence of \lambda x : obj.F_0 in F^0. Let F_1 be the largest enclosing occurrence \lambda x_n : T_n.\lambda x_n : obj.F_0. Then F_1 cannot be the entire F^0, because F^0 has type bool by subject reduction. F_1 cannot occur within some application F_1.F_2, because F_1.F_2 would constitute a redex and F^0 is in normal form. Hence, F_1 can only occur in an expression of the form F_3.F_1. Let us consider the “spine” [38] of F_3.F_1, so F_3 \equiv F_1.F_1.F_{n-1} \ldots F_{n} \equiv \exists \lambda x : obj.F_1.\exists \lambda x : obj.F_1.\exists \lambda x : obj.F_1

where F_0 = \lambda v : obj.G, or v \equiv x and F_1 \equiv \lambda u : obj.\lambda v : obj.F_1. This finishes the proof of the claim.

We conclude that typed lambda calculus allows us to use flexible definitions of higher-order predicates to structure our specifications while keeping the language first-order, because we may substitute away all definitions using strong normalization of the typed lambda calculus.

4 Role Logic Subset RL^2 and Its Decidability

In this section we introduce a subset RL^2 of role logic (Figure 11) and show its decidability.

To show the decidability of RL^2, we give translations of formulas between the following four logics:

1. D^2: the formulas of the first-order logic with counting in which every subformula has at most two free variables (different subformulas may have different free variables);

2. C^2: the formulas of the two-variable logic with counting, which uses x and y as the only variable names; the satisfiability and finite satisfiability problem for C^2 was shown to be decidable in [30]; the satisfiability problem for C^2 was shown NEXPTIME-complete in [37];

3. P: de Bruijn version of the two-variable logic with counting, which uses only de Bruijn indices (1) and (2);

4. RL^2: a subset of role logic that contains no explicit de Bruijn indices.

Figure 10 sketches the idea of the proof of equivalence of these four logics. We give translations of formulas from D^2 to C^2 (Section 4.2, Figure 15) from C^2 to P (Section 4.3, Figure 18) from P to RL^2 (Section 4.3, Figure 19) and from RL^2 to D^2 (Section 4.4, Figure 20). These translations imply that the satisfiability problem for these four logics are equivalent, so by decidability of C^2 [30] we conclude that all these logics are decidable.
quantifiers:
\[ \{F\} = \text{card}^{\geq 1}F \]
\[ \neg \{F\} \]
relation image:
\[ FA \cap FA = \{FA \cap \sim FA\} \]
weakest precondition:
\[ \text{wp} FA = \{FA \Rightarrow FA\} \]

Figure 13: Some Shorthands for RL^2

4.1 The Role Logic Subset RL^2

Figure 11 presents the two-variable role logic RL^2. Compared to the full role logic in Figure 9, RL^2 omits the constructs for creating definitions, the constructs for explicitly referring to object variables, and transitive closure. Figure 12 summarizes the semantics of RL^2; this semantics is in accordance with the semantics of the full role logic derived in Section 3. Figure 13 defines shorthands that illustrate some constructs definable in RL^2.

We show that RL^2 has precisely the same expressive power as the set of the formulas of logic C^2, which is shown decidable in [30] over the set of all models, as well as over the set of finite models.

4.2 Two-Variable Logics C^2 and D^2

Figure 14 presents the logic C^2 [30]. The logic C^2 is first-order logic with equality and counting, restricted to formulas that contain only two fixed variable names x and y.

In this section we argue that a more flexible restriction on variable names yields logic with some definable relations. Let FV(F) denote the free variables of formula F.

**Definition 4** A D^2 formula is a formula F of first-order logic with counting such that |FV(G)| ≤ 2 for every subformula G of F.

Clearly every C^2 formula is a D^2 formula, but not vice versa, because the set of possible variables that may occur in D^2 formulas is countably infinite. The syntactic restriction on variables in Definition 4 is more general than in the definition in C^2, which makes D^2 more convenient for writing readable formulas.

We show that every D^2 formula is equivalent to a C^2 formula (modulo the renaming of free variables). Up to one technical detail, it suffices to rename bound variables in a D^2 formula to obtain a C^2 formula. We therefore derive the equivalence of D^2 and C^2 as a consequence of an observation about lambda calculus terms.

**Definition 5** Define the set of lambda calculus terms 2VarTerms as the smallest set that satisfies the following conditions:

1. v ∈ 2VarTerms if v is a variable and c ∈ 2VarTerms if c is a constant;
2. if T1, T2 ∈ 2VarTerms and |FV(T1) ∪ FV(T2)| ≤ 2, then (T1T2) ∈ 2VarTerms;
\begin{align*}
\text{Vars}_2 &= \{x, y\} \\
\text{Form} &= A(\text{Vars}_2) \quad \text{atomic formula with unary relation } A \\
&\quad | f(\text{Vars}_2, \text{Vars}_2) \quad \text{atomic formula with binary relation } f \\
&\quad | \text{Vars}_2 = \text{Vars}_2 \quad \text{equality between objects} \\
&\quad | \text{Form} \land \text{Form} \quad \text{conjunction} \\
&\quad | \neg \text{Form} \quad \text{negation} \\
&\quad | \exists^2 \text{Vars}_2, \text{Form} \quad \text{at least } k \text{ objects satisfy formula}
\end{align*}

Figure 14: The Syntax of Two-Variable Logic with Counting \( C^2 \)

3. \( T \in \text{2VarTerms} \), \( v \) is a variable, and \( |\text{FV}(T) \cup \{v\}| \leq 2 \), then \( \lambda v.T \in \text{2VarTerms} \).

From Definition 5 it follows that if \( T \in \text{2VarTerms} \), then \( |\text{FV}(T)| \leq 2 \) for every subterm \( T_1 \) of \( T \). Moreover, if \( \lambda v.T \in \text{2VarTerms} \) and \( v \notin \text{FV}(T) \), then \( |\text{FV}(T)| \leq 1 \).

We next define the set \( \text{capt}(v, F) \) of those bound variables \( z \) in formula \( F \) such that \( v \) occurs in the scope of a binding of \( z \).

**Definition 6**

\[
\begin{align*}
\text{capt}(v, u) &= \emptyset, \text{ if } u \text{ is a variable} \\
\text{capt}(v, F_1 F_2) &= \text{capt}(v, F_1) \cup \text{capt}(v, F_2) \\
\text{capt}(v, \lambda u.F) &= \begin{cases} \\
\text{capt}(v, F) \cup \{u\}, & \text{if } v \in \text{FV}(\lambda u.F) \\
\emptyset, & \text{otherwise}
\end{cases}
\end{align*}
\]

As usual, we say that \( T \) and \( T' \) are \( \alpha \)-equivalent if \( T' \) can be obtained from \( T \) by renaming bound variables.

**Lemma 7** For every \( T \in \text{2VarTerms} \) with \( \text{FV}(T) \subseteq \{u, v\} \), there exists a term \( T = \text{norm}(T) \) such that \( T' \) \( \alpha \)-equivalent to \( T \), all bound variables in \( T' \) are among \( \{x, y\} \), and either

1. \( \text{capt}(u, T') \subseteq \{x\} \) and \( \text{capt}(v, T') \subseteq \{y\} \), or
2. \( \text{capt}(u, T') \subseteq \{y\} \) and \( \text{capt}(v, T') \subseteq \{x\} \).

**Proof.** Let \( \text{FV}(T) \subseteq \{u, v\} \). Without loss of generality we may assume that \( \{u, v\} \cap \{x, y\} = \emptyset \). The proof is by induction on the structure of terms.

1. \( T = u \) for a variable \( u \). Let \( T = T' \), clearly \( \text{capt}(u, T') = \text{capt}(v, T') = \emptyset \).

2. \( T = T_1 T_2 \). Let \( T'_1 = \text{norm}(T_1) \) and \( T'_2 = \text{norm}(T_2) \) by induction hypothesis. Assume \( \text{capt}(u, T'_1) \subseteq \{x\} \) and \( \text{capt}(v, T'_1) \subseteq \{y\} \) (the other case is symmetric). We consider two cases for \( T'_2 \).

(a) \( \text{capt}(u, T'_2) \subseteq \{x\} \) and \( \text{capt}(v, T'_2) \subseteq \{y\} \). Then let \( \text{norm}(T) = T'_1 T'_2 \).

(b) \( \text{capt}(u, T'_2) \subseteq \{y\} \) and \( \text{capt}(v, T'_2) \subseteq \{x\} \). Let \( T'_2 \) be the result of swapping \( T'_2 \) all occurrences of bound variables \( x \) and \( y \). Then \( \text{capt}(u, T''_2) \subseteq \{x\} \) and \( \text{capt}(v, T''_2) \subseteq \{y\} \), so we let \( \text{norm}(T) = T'_1 T''_2 \).

In both cases, \( \text{capt}(u, \text{norm}(T)) \subseteq \{x\} \) and \( \text{capt}(v, \text{norm}(T)) \subseteq \{y\} \).

3. \( T = \lambda v.T_1 \). \( |\{u, v\}| = 2 \) and \( |\text{FV}(T_1) \cup \{v\}| \leq 2 \) by the definition of \( \text{2VarTerms} \), so it cannot be the case that both \( u \in \text{FV}(T_1) \) and \( v \in \text{FV}(T_1) \). Since \( \text{FV}(T_1) \subseteq \{u, v, w\} \), we conclude that \( \text{FV}(T_1) \subseteq \{u, w\} \) or \( \text{FV}(T_1) \subseteq \{v, w\} \).

Suppose therefore that \( \text{FV}(T_1) \subseteq \{u, w\} \) (the case \( \text{FV}(T_1) \subseteq \{v, w\} \) is symmetric). By induction hypothesis, let \( T'_1 = \text{norm}(T_1) \). Assume \( \text{capt}(u, T'_1) \subseteq \{x\} \) and \( \text{capt}(w, T'_1) \subseteq \{y\} \) (the case \( \text{capt}(u, T'_1) \subseteq \{y\} \) and \( \text{capt}(w, T'_1) \subseteq \{x\} \) is symmetric). Let \( \text{norm}(T) = \lambda w.F_1[w := x] \). Then \( \text{capt}(u, \text{norm}(T)) \subseteq \{x\} \) and \( \text{capt}(v, \text{norm}(T)) \subseteq \{y\} \).


To apply Lemma 7 to \( D^2 \) formulas, we represent all logical operations and quantifiers as constants. Variables in a lambda term then correspond to first-order variables. To ensure that the representation of formulas satisfies the condition \( |\text{FV}(T) \cup \{v\}| \leq 2 \) for each term \( \lambda\alpha.v \), we require the following condition:

\[\exists^2 x, F \equiv F \land \exists^2 x, \text{true}\]

We ensure this condition by applying the rule

\[\exists^2 x, F \equiv F \land \exists^2 x, \text{true}\]

for \( x \notin \text{FV}(F) \).

After ensuring the condition (2), we apply the translation in Figure 15. Lemma 7 justifies the correctness of the translation. The translated formula is of the same size as the original formula. The translation can clearly be performed in polynomial time, including the process of ensuring the condition (2). The translation time can be made close to linear by delaying the application of the substitution \( [w := x] \) and the swap operation.

**4.3 From \( C^2 \) to \( RL^2 \) via \( I^2 \)**

In this section we introduce logic \( I^2 \) (Figure 16). We then give translations from \( C^2 \) to \( I^2 \) (Figure 18), and from \( I^2 \) to \( RL^2 \) (Figure 19).
\[
T_{DC}[A(v)] = A(v) \\
T_{DC}[f(u,v)] = f(u,v) \\
T_{DC}[\neg F] = \neg T_{DC}[F] \\
T_{DC}[F_1 \land F_2] = \begin{cases} 
  F_1 \land F_2, & \text{if } \operatorname{capt}(u, F_1), \operatorname{capt}(u, F_2) \subseteq \{x\} \\
  \operatorname{capt}(v, F_1), \operatorname{capt}(v, F_2) \subseteq \{y\} \\
  \text{or} \\
  \operatorname{capt}(u, F_1), \operatorname{capt}(u, F_2) \subseteq \{y\} \\
  \operatorname{capt}(v, F_1), \operatorname{capt}(v, F_2) \subseteq \{x\} \\
F_1 \land (\text{swap } F_2), & \text{otherwise} 
\end{cases}
\]

\[F(V(F_1 \land F_2)) = \{u, v\}\]
\[F_1 = T_{DC}[F_1]\]
\[F_2 = T_{DC}[F_2]\]

\[
\begin{align*}
\text{swap } (A(v)) &= A(su, sv) \\
\text{swap } (f(u,v)) &= f(su, sv) \\
\text{swap } (\neg F) &= \neg (\text{swap } F) \\
\text{swap } (F_1 \land F_2) &= \text{swap } F_1 \land \text{swap } F_2 \\
\text{swap } (\exists^2 F, F) &= \exists^2 (sv), (\text{swap } F) \\
\end{align*}
\]

\[
T_{DC}[\exists^2 w. F] = \begin{cases} 
  \exists^2 x, (F'[w := x]), & \text{if } \operatorname{capt}(u, F') \subseteq \{x\}, \operatorname{capt}(w, F') \subseteq \{y\} \\
  \exists^2 y, (F'[w := y]), & \text{if } \operatorname{capt}(u, F') \subseteq \{y\}, \operatorname{capt}(w, F') \subseteq \{x\} 
\end{cases}
\]

\[F(V(F)) \subseteq \{u, v\}\]
\[F' = T_{DC}[F]\]

Figure 15: Translation of \(D^2\) formulas to \(C^2\) formulas.

\[
\text{Form} = A(\langle \text{Nat}_2 \rangle) \quad \text{atomic formula with unary relation } A \\
| f(\langle \text{Nat}_2 \rangle, \langle \text{Nat}_2 \rangle) \quad \text{atomic formula with binary relation } f \\
| \langle \text{Nat}_2 \rangle = \langle \text{Vars}_2 \rangle \quad \text{equality between objects} \\
| \text{Form} \land \text{Form} \quad \text{conjunction} \\
| \neg \text{Form} \quad \text{negation} \\
| \text{card}^k \text{Form} \quad \text{at least } k \text{ objects satisfy formula}
\]

Figure 16: The Syntax of Intermediate Logic \(I^2\)
\[ e ::= \text{Nat}_2 \rightarrow \text{Var}_2 \]
\[ \text{Tc}[A(i)] = A(e_i) \]
\[ \text{Tc}[f(i_1, i_2)] = f(e_{i_1}, e_{i_2}) \]
\[ \text{Tc}[(i_1 := i_2)] = (e_{i_1} = (e_{i_2}) \]
\[ \text{Tc}[F_1 \land F_2] = (\text{Tc}[F_1] \land \text{Tc}[F_2]) \]
\[ \text{Tc}[\neg F] = \neg \text{Tc}[F] \]
\[ \text{Tc}[	ext{card}^{e_1} F] = \exists^{e_1} v, (\text{Tc}[F][y \mapsto 1, x \mapsto 2, \theta = \{1\}]) \]
\[ \text{correctness criterion:} \]
\[ \text{Tc}[F] \in C = [F](C \circ e) \]

Figure 17: Translating \( F \) formulas to \( C \) formulas

**Intermediate logic.** Figure 16 presents logic \( F \). \( F \) is a version of \( C \) that uses two de Brujin indices instead of variables. We introduce \( F \) to separate the translation of \( C \) formulas to \( R \) in two phases: the first phase introduces de Brujin indices, and the second phase introduces Default Argument Rule.

For the sake of illustration, we first present a converse translation, from \( F \) to \( C \), although we do not need this translation to show the equivalence of \( D \), \( F \), \( C \), and \( R \).

**From \( F \) to \( C \).** Figure 17 presents the translation of \( F \) into \( C \). This translation amounts to introducing alternatively variables \( x \) and \( y \) for each counting quantifier, and resolving the indices appropriately. Using the criterion in Figure 17, the correctness of the translation follows by induction on the structure of formulas.

**From \( C \) to \( F \).** We turn to the translation from \( C \) to \( F \). Consider the \( C \) formula
\[ F \equiv \exists^{x_1} y_1, (\exists^{x_2} x_2, P(x, y)) \land Q(x, y) \]
The subformula \( P(x, y) \) refers to the variable \( y \), which is the 3rd bound variable starting from the innermost one. Therefore, the straightforward replacement of variables by de Brujin indices would require the access to \( \langle 3 \rangle \). To address this problem, the translation from \( C \) to \( F \) involves a preparatory \"alternating transformation\" on \( C \) formulas. For every formula \( F \), let \( B(F) \) denote some purely propositional combination of \( F \) and perhaps some other formulas. The alternating transformation eliminates all subformulas of the form \( \exists^{x_1} v, B(\exists^{x_2} x_2, G(v)) \) for \( v \in \text{Var}_2 \). In the resulting formula, the sequence of bound variables along any path in the formula tree is alternating, that is, satisfies the regular expression \( (y_1 y_2 \ldots y_n) \).

For the purpose of alternating transformation, we add the disjunction \( \lor \) to the language. We show how to eliminate successive quantification over \( x \) from \( \exists^{x_1} x_1, B(\exists^{x_2} x_2, G) \) (the case of \( \exists^{x_1} y_1, B(\exists^{x_2} y_2, G) \) is analogous). First, transform \( B \) into disjunction of canonical conjuncts of formulas \( H \), where each \( H \) satisfies one of the following conditions:

\[ e ::= \text{Var}_2 \rightarrow \text{Nat}_2 \]
\[ \text{Tc}[A(v)] = A(e_v) \]
\[ \text{Tc}[f(v_1, v_2)] = f(e_{v_1}, e_{v_2}) \]
\[ \text{Tc}[v_1 := v_2] = (e_{v_1} = (e_{v_2}) \]
\[ \text{Tc}[F_1 \land F_2] = (\text{Tc}[F_1] \land \text{Tc}[F_2]) \]
\[ \text{Tc}[\neg F] = \neg \text{Tc}[F] \]
\[ \text{Tc}[\exists^{x} x, P(x)] = \text{card}^{e_0}(\text{Tc}[F][y \mapsto 1, x \mapsto 2]) \]
\[ \text{invariant:} \quad e_0 = 1 \]
\[ \text{Tc}[\exists^{x} x, P(x)] = \text{card}^{e_0}(\text{Tc}[F][y \mapsto 1, x \mapsto 2]) \]
\[ \text{invariant:} \quad e_0 = 1 \]

**correctness criterion:**
\[ \text{Tc}[F] \in C = [F](C \circ e) \]

Figure 18: Translating normalized \( C \) formulas to \( F \) formulas

\( C1 \) \( H \) is quantifier-free;

\( C2 \) \( H \) is of the form \( \exists^{x} v, G(v) \) for \( v \in \text{Var}_2 \);

\( C2 \) \( H \) is of the form \( \exists^{x} v, G(v) \) for \( v \in \text{Var}_2 \);\]

Let \( B \equiv \bigwedge_{i=1}^{n} B_i \) where each \( B_i \) is a canonical conjunction (cube) of formulas satisfying conditions \( (C1), (C2), (C3) \). Because \( B_i \land B_j \) is contradictory for distinct cubes \( B_i \) and \( B_j \), the sets of objects \( o \) satisfying each \( B_i \) are disjoint, so
\[ |\{ o \mid B \in \text{Var}_2 \}| = \sum_{i=1}^{n} |\{ o \mid B \in \text{Var}_2 \}| \]
We can therefore replace counting quantifier on \( B_i \) with a propositional combination of counting quantifiers on \( B_i \) for \( 1 \leq i \leq n \) (as in quantifier elimination for boolean algebra, [67], [49, Section 3.2]). Specifically,
\[ \exists^{x=1} x, B \equiv \begin{cases} \bigcup_{y=x}^{n} \exists^{y} x, B \end{cases} \]

It is therefore sufficient to eliminate the successive quantification over \( x \) in \( \exists^{x_1} x_1, B(\exists^{x_2} x_2, G) \). Group the conjuncts in \( B_i \) as follows. Let \( F(V) \) denote free variables of formula \( F \). Let \( P(x) \) be the conjunction of conjuncts \( C \) of \( B_i \) such that \( x \in F(V) \), and let \( Q \) be the conjunction of all conjuncts \( C \) of \( B_i \) such that \( x \not\in F(V) \). All occurrences of \( \exists^{x} x, G \) in \( B_i \) are in \( Q \). We have
\[ \exists^{x_1} x_1, B_i \equiv \exists^{x_1} x_1, Q \land P(x) \equiv Q \land \exists^{x_1} x_1, P(x) \]
where the last equivalence follows easily by definition of the counting quantifier \( \exists^{x_1} x \). In the resulting formula \( Q \land \exists^{x_1} x, P(x) \), the subformula \( \exists^{x_2} x_2, G \) is in \( Q \) and is therefore not in the scope of the original quantifier. By repeating this transformation we ensure that all quantifiers are alternating.
After the alternating transformation, the translation from $C^2$ to $I^2$ is straightforward, and is presented in Figure 18. The correctness of the translation follows by induction of the structure of formulas. The translation in Figure 18 runs in linear time and produces an $I^2$ formula whose size is linear in the size of the original $C^2$ formula.

The alternating transformation that precedes the translation may cause exponential blowup of the formula size due to translation to disjunctive normal form, but for most formulas the transformation need not be applied. Moreover, if we allow introducing new predicate names, then we may replace $\exists x \forall y . B(\exists x_0 . x_0 . G(x,y))$ with $\exists x_0 . x_0 . B(\forall y . G(x,y))$ and conjoint the topmost formula with the formula $\forall y . P(y) \iff \exists x_0 . x_0 . G(x,y)$. Such transformation can be performed in linear time and preserves the satisfiability of formulas (see [30, Section 2.1, Page 18] and [30, Lemma 2.3]).

4.4 From $I^2$ to $D^2$: Closing the Loop

In the final step, we provide a translation from $I^2$ formulas to $D^2$ formulas. The logic $D^2$ is a convenient target of translation of $I^2$ formulas. (Namely, a simple attempt at translation from $I^2$ to $D^2$ runs into the difficulty of the following form. Formula $(\text{card}^{2^1} f)'$ is equivalent to $(\text{card}^{2^1} f(\langle 3 \rangle, (1)))$ which uses index $\langle 3 \rangle$ not available in $I^2$. Similarly, an attempt to translate from $I^2$ to $C^2$ runs into difficulty of variable capture.)

Figure 20 presents the translation from $RL^2$ to $D^2$. The correctness of the translation follows by induction on the structure of formulas. Furthermore, each subformula $G_1$ of a formula $T_RD[F]e$ is of the form $G_1 \equiv T_RD[G]e_1$ for some $G$ and $e_1$, and by induction it follows that the free variables of $T_RD[G]e_1$ are among $\{e_1, e_2, e_3\}$. Therefore, $\text{FV}(G_1) \leq 2$ and the result of translation is a $D^2$ formula.

Summary As indicated in Figure 10, we have presented translations from $D^2$ to $C^2$, from $C^2$ to $I^2$, from $I^2$ to $RL^2$, and from $RL^2$ to $D^2$. We conclude that $D^2$, $C^2$, $I^2$, and $RL^2$ are all equivalent logics, and, by [30], decidable.

The satisfiability problem for $C^2$ formulas is shown to be NEXPTIME-complete in [57]. We have observed that there are efficient polynomial transformations of formulas from $D^2$ to $C^2$, from $C^2$ to $I^2$, from $I^2$ to $RL^2$, and from $RL^2$ to $D^2$ that yield formulas equivalent for satisfiability. (Moreover, all transformations except from $C^2$ to $I^2$ yield equivalent formulas in the same vocabulary.) As a result, the satisfiability problem of all these logics is NEXPTIME-complete.

5 Applications of Role Logic

We next present three applications of role logic. In Section 5.1 we present a shape analysis technique based on generating verification conditions in RL$^2$ and applying the decision procedure for RL$^2$. In Section 5.2 we note that boolean shape analysis constraints [48] are a subset of constraints expressible in role logic. In Section 5.3 we show that a different subset of RL$^2$ corresponds to an expressive description logic [1, Chapter 5].

5.1 Static Analysis Based on RL$^2$

This section shows how to use the decidability of RL$^2$ for static analysis of imperative programs. Figure 21 presents
the syntax of a simple imperative language. Figure 22 presents predicates in RL^2 that describe the meaning of statements in this language.

**Program state.** The state of the program is a first-order structure interpreting the language $L = A \cup F$ where $A$ is a finite set of unary predicates and $F$ is a finite set of binary predicates. We fix a countable universe of objects $\text{obj}$, and assume that each structure has the same universe $\text{obj}$. To specify the structure, it suffices to give the set $eA \subseteq \text{obj}$ for each unary predicate $A \in A$, and a binary relation $ef \subseteq \text{obj} \times \text{obj}$ for each binary predicate $f \in F$.

**Extended language.** For each $k \in \{e, 0, 1, \ldots\}$ we define the language $L(k)$. We identify $L(0)$ with $L$, $A(e)$ with $A$ and $f(e)$ with $f$. For $k \in \{0, 1, \ldots\}$, we let $A(k)$ be a fresh unary predicate symbol, and $f(k)$ a fresh binary predicate symbol, and $L(k)$ be the set of all $A(k)$ and $f(k)$. The notation $\text{formRen}(i \rightarrow j) F$ for $i, j \in \{e, 0, 1, 2, \ldots\}$ denotes a formula resulting from $F$ by replacing all elements of $L(i)$ with the corresponding elements of $L(j)$.

**Describing relations in the extended language.** The meaning of each statement in our imperative language is a binary relation on $L$-structures. We describe a binary relation on structures with an RL^2 formula in the language $L(0) \cup L(1)$. The predicates in $L(1)$ denote the state components in the final state; the predicates in $L(0)$ denote the state components in the initial state. If $F$ is a formula in language $L(0)$, then $\mathcal{F}$ is a shorthand for the formula $\text{formRen}(e \rightarrow 0) F$ in the language $L(0)$; the purpose of $\mathcal{F}$ is to denote the value of the formula $F$ evaluated in the initial state.

**Assignment statements.** The imperative language in Figure 22 contains three forms of assignment statements.

The statement $A \leftarrow F$ evaluates to the formula $F$, which denotes a unary predicate. The statement makes $A$ true precisely for those objects for which $F$ was true in the initial state. Unary predicates other than $A$ as well as binary predicates remain unchanged.

The statement $F_1.f := F_2$ generalizes the statement $x.f = y$ in a language like Java by allowing simultaneous modification of fields of a set of objects. Formula $F_1$ specifies the set of objects whose fields are modified. Formula $F_2$ specifies the new value of the field $f$ for objects in $F_1$. Unary predicates and binary predicates other than $f$ remain unchanged. Note that $F_2$ may specify a relation, which is particularly interesting when $F_1$ denotes a set with more than one element because it allows the value of the field to depend on the source object of the field. As a special case, $F_1.f := y$ copies the entire field $y$ into field $f$ for all objects in the set given by $F_1$ and in particular, true.f := y copies the field $y$ into $f$. The statement $F_1.f := F_2$ is dual to $F_1.f := F_2$ and updates the inverse of the predicate $f$.

**Statements for specification.** The statement $\text{assume } F$ fills in the state transitions for which $F$ does not hold in the initial state. The statement $\text{assert } F$ behaves arbitrarily if the condition given by $F$ does not hold in the initial state. The state contains an additional predicate Error, which makes it easy to detect that an arbitrary behavior

\[
\begin{align*}
[P_1 \Rightarrow P_2] &= ([S_1]A) \\
&\quad -[S_2](B_1 \rightarrow A_1, \ldots, B_n \rightarrow A_n))
\end{align*}
\]

is not satisfiable, where:

$P_1(A_1, \ldots, A_n) = S_1$

$P_2(B_1, \ldots, B_n) = S_2$

$[S_2]$ has no fresh predicates

\[
[A := F] = [A \iff \langle F \rangle] \land \text{modUnary } A
\]

\[
[F_1.f := F_2] = ([F_1] \iff [f \iff F_2]) \land \text{modBinary } f
\]

\[
[F_1.f :\neg f := F_2] = ([F_1] \iff [\neg f \iff F_2]) \land \text{modBinary } f
\]

\[
[P(F_1, \ldots, F_n)] = [S](A_1 \rightarrow F_1, \ldots, A_n \rightarrow F_n)
\]

where $P(A_1, \ldots, A_n) = S$

\[
[\text{assume } F] = \langle F \rangle \land \text{skip}
\]

\[
[\text{assert } F] = \langle F \rangle \Rightarrow \text{skip}
\]

\[
[\text{spec } F] = \langle F \rangle
\]

\[
[S_1 \land S_2] = [S_1] \land [S_2]
\]

\[
[S_1 \lor S_2] = [S_1] \lor [S_2]
\]

\[
[S_1 ; S_2] = \text{formRen}(e \rightarrow k) [S_1] \land
\]

\[
([\text{Error} \Rightarrow \text{formRen}(0 \rightarrow k) [S_2]])
\]

$k$ - fresh element of $\{1, 2, \ldots\}$

\[
[\text{modify } E] = \Lambda(E)
\]

\[
\text{modUnary } A \equiv \Lambda_{B \in A} [B \iff \langle B \rangle] \land
\]

\[
\Lambda_g [g \iff \langle g \rangle] \land
\]

\[
[\text{Error} \iff \langle \text{Error} \rangle]
\]

\[
\text{modBinary } f \equiv \Lambda_{B \in A} [B \iff \langle B \rangle] \land
\]

\[
\Lambda_{g \neq f} [g \iff \langle g \rangle] \land
\]

\[
[\text{Error} \iff \langle \text{Error} \rangle]
\]

\[
\text{skip} \equiv \Lambda_{B \in A} [B \iff \langle B \rangle] \land
\]

\[
\Lambda_g [g \iff \langle g \rangle] \land
\]

\[
[\text{Error} \iff \langle \text{Error} \rangle]
\]

Figure 22: Predicates Describing the Semantics of the Language from Figure
\( F \) – a role logic formula
\( A \) – unary predicate
\( f \) – binary predicate

\[
\text{procedure} ::= \text{procName}(\text{unaryList}) = \text{stat} \\
\text{refinement} ::= \text{procName} \Rightarrow \text{procName} \\
\text{unaryList} ::= A \mid \text{unaryList}, A \\
\text{stat} ::= \text{asgnStat} \\
\text{spec} ::= \text{procName}(\text{paramList}) \\
\text{assume} ::= F \\
\text{assert} ::= F \\
\text{stat} ::= \text{stat} \lor \text{stat} \\
\text{stat} ::= \text{stat} \land \text{stat} \\
\text{stat} ::= \text{stat} ; \text{stat} \\
\text{asgnStat} ::= A := F \\
\text{F}_{\text{E}} ::= A \mid f | \text{EQ} | F_1 \land F_2 | \neg F \\
\text{paramList} ::= F \mid \text{paramList}, F \\
\text{items} ::= \text{modItem} \mid \text{items}, \text{modItem} \\
\text{modItem} ::= A ::= F \\
\text{F}_{\text{E}} ::= F_1, f ::= F_2 \\
\text{F}_{\text{E}} ::= F_1, \neg f ::= F_2 \\
\]

Figure 21: Syntax of a Small Imperative Language
proc assignClients() =
spec old(GlobalInvariant) \Rightarrow
  modify WaitingClients, AssignedClients,
  old(WaitingClients).server ::= Servers,
  Servers.clients ::= old(WaitingClients) &
  !{WaitingClients} &
  [AssignedClients <=>
   old(AssignedClients \ WaitingClients)] &
  GlobalInvariant

proc assignOneClient(cl) =
spec old(GlobalInvariant) &
  [cl => old(WaitingClients)] \Rightarrow
  modify WaitingClients, AssignedClients,
  cl.server ::= Servers,
  Servers.clients ::= cl) &
  [WaitingClients \ cl <=> old(WaitingClients)] &
  [AssignedClients <=> old(AssignedClients) \ cl] &
  GlobalInvariant

Figure 24: Specifications for assignClients and
class assignOneClient extended with side effect speci-
cfications.

occurred (the sequential composition operator ensures that
the Error value is propagated).

The statement spec FE allows describing relations on
states directly in terms of an extended RL2 formula FE.
Formula FE allows assignment statements and modifies state-
ments in addition to the constructs of RL2. The relation
symbols of RL2 may refer to relation symbols of the ex-

tended language, which allows stating relations between pre-

and postcondition. We also allow non-recursive procedure


calls in the specification when they expand to constructs not

containing sequential composition.

modify specifications. The construct

modify e1 \ldots \enn

is useful for specifying frame conditions. Each expression ei

specifies a set of possible modifications. Any finite number of

modifications can occur as the result of the action specified

by the modify specification.

Example 8 Figure 24 shows the specifications
assignClients and assignOneClient from Figure 3

extended with frame-condition specifications. The frame

condition for assignOneClient specifies that only the sets
WaitingClients and AssignedClients can change, which is

useful if the system contains some additional set of

objects, such as a set ProcessedClients. Next, the frame-

condition specifies that the only binary relations that were

modified are server and clients. The modified expression

(Servers.clients ::= cl) indicates that the the only way in

which the clients relation is changed is by introducing an

edge from a Servers object to the cl object, or by removing

an edge from a Servers object. (The removal of the edge does

not, in fact, occur in assignOneClientImpl in Figure 3,

but the frame condition is a conservative approximation.)

The amount of detail in specifications such as modifies

clauses depends on how strong property we need to prove.

The strength of the property, in turn, depends either on

some high-level program correctness requirement, or on

the amount of information we need about the procedure

to prove the properties of its callers. In Figure 3, we
did not use modify specification for assignOneClient
because we did not need it to prove the conformance
of assignClientsImpl with respect to assignClients.
However, even in Figure 3 we needed to know that, for

general, there are three forms of modification expres-
sions. The expression A \llt F specifies modifications that

remove an element from the set A or insert into A an element

that satisfies F. For example, after executing the statement

modify A \llt F


the set A may contain any subset of the set of objects


given by the expression A \lor F. The expression F1 \llt F2

specifies modifications that 1) remove a tuple (a1,a2) from

the relation interpreting the predicate f, when a1 satisfies F1,

or 2) insert a tuple (a1,a2) into the relation interpreting

f, when a2 satisfies F2. Similarly, F1 \llt \neg F2 allows removing

(a1,a2) from the interpretation of f when a2 satisfies F1, or

inserting (a1,a2) when a2 satisfies F2 and (a1,a2) satisfy \neg F2.

If \rho is the relation describing a modification given by

the expression e, then the meaning of modify e1 \ldots \enn is given

by the relation

(\rho1 \cup \ldots \cup \rhon)^k

(4)

where r^k denotes the transitive closure of relation r. The

simple semantics (4) provides good intuition about the

meaning of modify statement and makes it clear that the

modify statement is idempotent [44]. Figure 23 presents an

alternative semantics, which directly encodes a modify state-

ment as an RL2 formula. The advantage of the semantics in

Figure 23 is that it eliminates the need for transitive closure of

the transition relation.

Disjunction and conjunction. The language allows com-

puting disjunction and conjunction on statements. Disjunc-

tion \lor has a natural interpretation as a non-deterministic

choice of commands. Conjunction \land is useful for combi-


ing nondeterministic statements. Logical operations on state-

ments translate directly to the corresponding logical opera-

tions on RL2 formulas.

Computing sequential composition. When encoding

sequential composition of statements in RL2, we introduce

copies L(i) of predicate names in L for i \in \{1,2,\ldots\}. These

copies of predicate names denote the values of predicates

at program points between the initial and the final pro-

gram state. Because the definition of relation composition

\rho1 \circ \rho2 = \{ (x,z) \mid \exists y \ (x,y) \in \rho1 \land (y,z) \in \rho2 \} involves

existential quantification over y, we treat the newly intro-

duced predicates as being existentially quantified. The tech-

nique of introducing new predicate names allows us to

precisely compute relation composition even for non-

deterministic commands.

Procedure calls. The meaning of a procedure is also a

relation on states, where the initial state is extended with

one unary predicate symbol for each parameter name. In

the simple translation of Figure 22, a procedure call identi-

fies parameters with the sets that describe their values by
$M[\text{modify} e_1, \ldots, e_n] =$

let \( \{e_1, \ldots, e_n\} = \{
\{A_1 := F_1, \ldots, A_k := F_k, \quad F_{k+1} \land F_{k+1} := G_{k+1}, \ldots, F_t \land f_t := G_t, \quad F_{t+1} \land f_t := G_{t+1}, \ldots, F_m \land f_m := G_m\}\}
\)

in

\[
\bigwedge_{A \in \{A_1, \ldots, A_k\}} \big[ A \equiv \overline{A} \big] \land
\bigwedge_{A \in \{A_1, \ldots, A_k\}} \left[ (\overline{A} \land \bigwedge_{A_i \in A} \neg F_i) \Rightarrow \neg A \right] \land
\bigwedge_{f \in \{f_{k+1}, \ldots, f_m\}} \left[ \left( \bigwedge_{f_i \equiv f} \left( \neg F_i \land \bigwedge_{l \leq i} \neg F_l \right) \Rightarrow (f \equiv \overline{f}) \right) \right]
\]

\[
\bigwedge_{f \in \{f_{k+1}, \ldots, f_m\}} \left[ \left( \neg \overline{f} \land \bigwedge_{f_i \equiv f} \left( \neg (F_i \land G_i) \land \bigwedge_{l < i} \neg (F_l \land \neg G_l) \right) \Rightarrow \neg f \right) \right]
\]

Figure 23: Semantics of modify statement.

performing the substitution. Substitution suffices to give semantics to procedures because we assume that the recursion is split using refinement claims. Loops are represented as recursive procedures, so we effectively require loop invariants.

**Refinement claims.** If \( P_1 \) and \( P_2 \) are procedure names, the refinement claim \( P_1 \Rightarrow P_2 \) is a proof obligation that the relation given by the body of procedure \( P_1 \) is contained in the relation given by the body of \( P_2 \). The intended use of the refinement claim is the specification procedure summaries, which allows breaking the cycles in the call graphs of mutually recursive procedures. Figure 22 shows how each refinement claim reduces to a test whether an RL^2 formula is satisfiable. When generating the RL^2 formula, we rename the parameters of \( P_2 \) replacing them with the corresponding parameters of \( P_1 \).

To ensure that the satisfiability test treats newly introduced predicates as existentially quantified, we impose a restriction that the translation \([S_2]\) contains no newly introduced predicates from \( L(e) \) for \( e \in \{1, 2, \ldots\} \). We impose this restriction because \([S_2]\) appears under negation in the satisfaction test, so newly introduced predicates in \([S_2]\) would be universally quantified, thus violating the semantics of sequential composition for non-deterministic statements. The restriction on \( S_2 \) is satisfied when \( S_2 \) contains no sequential composition, which is typically the case for a large class of procedure summaries.

By providing sufficiently many procedure summaries, the partial correctness of a program is reduced to a finite number of refinement claims. By discharging these claims using a decision procedure for RL^2, we decide the partial correctness of the program.

**Fixpoint computation.** If some procedure summaries are not supplied by the programmer, they can be inferred using fixpoint computation. An algorithm for fixpoint computation can be derived from the fixpoint semantics of mutually recursive procedures using abstract interpretation [19, 21, 20, 70]. A special case of this approach is to select a finite subset of all RL^2 formulas and define a lattice structure on the set using the entailment of formulas. A simple way to define a finite subset of formulas is to consider only RL^2 formulas with quantifier depth at most \( k \), for some \( k \geq 1 \).

Boolean shape analysis constraints in Section 5.2 have quantifier depth at most two, so they can be used as a basis of fixpoint computation.

Figure 25: Boolean Shape Analysis Constraints expressed as a sublogic of RL^2

\[
F ::= \{C\} \mid \{C_1 \land C_2 \land R\} \mid F_1 \land F_2 \mid \neg F
\]

\[
C ::= A \mid C_1 \land C_2 \mid \neg C
\]

\[
R ::= f \mid \neg f \mid R_1 \lor R_2
\]

\[
A = \text{atomic unary predicate}
\]

\[
 f = \text{atomic binary predicate}
\]

5.2 Describing Boolean Shape Analysis Constraints

Boolean Shape Analysis Constraints [48] are a natural language for describing datalow facts of shape analyses [65]. Figure 25 presents the syntax of Boolean Shape Analysis Constraints as a subset of role logic. This presentation of Boolean Shape Analysis Constraints shows that they are a subset of the decidable fragment RL^2 of role logic. In fact, Boolean Shape Analysis Constraints do not use counting quantifiers, so they are already expressible in the two-variable predicate logic L^2 (without counting).

**A note on usability of role logic.** An anecdotal evidence of the usability of role logic is the fact that all results
ability of interesting description logics that contain transitive closure but do not have tree model property is an open problem [1, Page 214].

A note on terminology. The term “role” has different meanings in different formalisms for describing structures. In [43], a role corresponds to a unary predicate (set), in description logics [1], a role corresponds to a binary predicate (relation), and in entity-relationship diagrams in databases [16], a role corresponds to a position $i$ ($1 \leq i \leq n$) in a $n$-tuple of an $n$-ary relation. To avoid the confusion, we use the well-established terms of $n$-ary “predicate” (or “relation”), keep the name “role logic” for the logic described in Figure 9, because the term “role logic” appears appropriate regardless of the particular interpretation of the word “role”.

Description Logics Corresponding to $C^2$. The result [10, Theorem 4] reports that the description logic without transitive closure and relation composition (extended $DL^- \cup \{\text{trans, compose}\}$) corresponds precisely to $C^2$. The results of Section 4 and [10] imply that our logic $RL^2$ has the same expressive power as $DL^- \cup \{\text{trans, compose}\}$. One of the differences between $RL^2$ and $DL^- \cup \{\text{trans, compose}\}$ is that $RL^2$ contains the primitive operators $P'$ and does not contain the product operation of $DL^- \cup \{\text{trans, compose}\}$. Another difference is the foundation of role logic on de Bruijn lambda calculus notation, as described in Section 3.

6 Related Work

We have initially developed role logic to provide a foundation for role analysis [43, 42]. We have subsequently studied a simplification of role analysis constraints and showed a characterization of such constraints using formulas [46]. Parametric analysis based on three-valued logic was introduced in [64, 65] with interprocedural analysis in [63] and application to abstract data type verification in [52]. A characterization of dataflow facts used for shape analysis was presented in [71, 48]. A decidable logic for expressing connectivity properties of the heap was presented in [7].

Specifying the semantics of programs using predicates dates back to axiomatic program semantics [32, 24]. An approach that uses a first-order logic theorem prover tailed for program verification is [23].

Like [40, 39, 37, 55], in Section 5.1 we use an expressive yet decidable logic to encode fragments of straight-line code. Our approach differs primarily in using logic $RL^2$ over general graphs whose decidability follows from the decidability of $C^2$, where $RL^2$ uses graph types whose decidability follows from the decidability of monadic second-order logic over trees. We expect that these two logics can be combined in a fruitful way.

We have extended our language with constructs that make it possible to directly express higher-level state transformations, which is the idea related to the chemical reaction model of [26, 27], the verification of database transactions [6], the simultaneous assignments of [55], and in wide-spectrum languages [56, 3]. Verification of a form of modifies clauses using a theorem prover was presented [50, 44]. Further approaches to pointer and shape analysis include [17, 68, 15, 29, 25, 28, 69].
Description logics [1, 9] share many of the properties of role logic and have been traditionally applied to knowledge bases. It is likely that description logics can be used for shape analysis as well. It would be particularly interesting to consider description logics with transitive operators, whose decidability is related to the decidability of dynamic logic [31]. Reasoning about the satisfiability of expressive description logics over all structures and over finite structures is presented in [13, 14]. Reasoning about entity-relationship diagrams [16] is presented in [51]. Some connections between object models and heap invariants are presented in [45, 33].

Like the Alloy modelling language [30], role logic combines the notation of predicate calculus with the notation of relational algebras. It may be possible to combine the notation of Alloy with the notation of role logic, and to combine the benefits of bounded model checking used in Alloy Analyzer with the benefits of a decision procedure for $RL^2$.

A recent approach to reasoning about mutable imperative data structure is separation logic [34, 59, 60, 12, 11]. We are currently working in integrating some aspects of spatial logic to support more flexible notation for records in role logic.

Interactive theorem provers have also been used for reasoning about dynamically allocated data structures [54, 2]; it may be interesting to incorporate a decision procedure for $RL^2$ into these general tools.

7 Conclusions

We believe that role logic notation is a convenient way of expressing properties of first-order structures. First-order structures are a natural way to model the state in object-oriented programs, or the state of a knowledge base or database. Role logic can be combined with traditional variable-based notation in a natural way. Furthermore, interesting subsets of role logic are decidable. Decision procedures for role logic can therefore enable shape analysis of programs and have similar benefits as description logics in knowledge bases.

Acknowledgements We thank Patrick Lam for useful discussions, comments on the paper, and an implementation of an early version of role logic normalization algorithm in Fall 2001. We thank Andreas Podelski for discussion of using formulas to perform shape analysis; we thank Thomas Reps for discussions on summarizing procedures using two-vocabulary structures; we thank C. Scott Ananian for discussion of a draft of this paper in Spring 2003, we thank Derek Rayside, Moody Sagiv, and Greta Yersh for useful discussions, and Darko Marinov for comments on the paper.

References


