A Constraint Language for Static Semantic Analysis Based on Scope Graphs with Proofs

Hendrik van Antwerpen, Pierre Néron, Andrew Tolmach, Eelco Visser, Guido Wachsmuth

Report TUD-SERG-2015-012
A Constraint Language for Static Semantic Analysis Based on Scope Graphs

Hendrik van Antwerpen
TU Delft, The Netherlands
h.vanantwerpen@tudelft.nl

Pierre Néron
TU Delft, The Netherlands
p.j.m.neron@tudelft.nl

Andrew Tolmach
Portland State University, USA
tolmach@pdx.edu

Eelco Visser
TU Delft, The Netherlands
visser@acm.org

Guido Wachsmuth
TU Delft, The Netherlands
guwc@acm.org

Abstract
In previous work, we introduced scope graphs as a formalism for describing program binding structure and performing name resolution in an AST-independent way. In this paper, we show how to use scope graphs to build static semantic analyzers. We use constraints extracted from the AST to specify facts about binding, typing, and initialization. We treat name and type resolution as separate building blocks, but our approach can handle language constructs—such as record field access—for which binding and typing are mutually dependent. We also refine and extend our previous scope graph theory to address practical concerns including ambiguity checking and support for a wider range of scope relationships. We describe the details of constraint generation for a model language that illustrates many of the interesting static analysis issues associated with modules and records.

Categories and Subject Descriptors D.3.1 [Programming Languages]: Formal Definitions and Theory; D.3.2 [Programming Languages]: Language classifications; F.3.1 [Logics and Meanings of Programs]: Specifying and Verifying and Reasoning about Programs; D.3.4 [Programming Languages]: Processors; F.3.2 [Logics and Meanings of Programs]: Semantics of Programming Languages; D.2.6 [Software Engineering]: Programming Environments

Keywords Language Specification; Name Binding; Types; Domain Specific Languages; Meta-Theory

1. Introduction
Language workbenches [6] are tools that support the implementation of full-fledged programming environments for (domain-specific) programming languages. Ongoing research investigates how to reduce implementation effort by factoring out language-independent implementation concerns and providing high-level meta-languages for the specification of syntactic and semantic aspects of a language [18]. Such meta-languages should (i) have a clear and clean underlying theory; (ii) handle a broad range of common language features; (iii) be declarative, but be realizable by practical algorithms and tools; (iv) be factored into language-specific and language-independent parts, to maximize re-use; and (v) apply to erroneous programs as well as to correct ones.

In recent work we showed how name resolution for lexically-scoped languages can be formalized in a way that meets these criteria [14]. The name binding structure of a program is captured in a scope graph which records identifier declarations and references and their scoping relationships, while abstracting away program details. Its basic building blocks are scopes, which correspond to sets of program points that behave uniformly with respect to resolution. A scope contains identifier declarations and references, each tagged with its position in the original AST. Scopes can be connected by edges representing lexical nesting or import of named collections of declarations such as modules or records. A scope graph is constructed from the program AST using a language-dependent traversal, but thereafter, it can be processed in a largely language-independent way. A resolution calculus gives a formal definition of what it means for a reference to resolve to a declaration. Resolutions are described as paths in the scope graph obeying certain (language-specific) criteria; a given reference may resolve to one or many declarations (or to none). A derived resolution algorithm computes the set of declarations to which each reference resolves, and is sound and complete with respect to the calculus.

In this paper, we refine and extend the scope graph framework of [14] to a full framework for static semantic analysis. In essence, this involves unifying a type checker with our existing name resolution machinery. Ideally, we would like to keep these two aspects separated as much as possible for maximum modularity. And indeed, for many language constructs, a simple two-stage approach—name resolution using the scope graph followed by a separate type checking step—would work. But the full story is more complicated, because sometimes name resolution also depends on type resolution. For example, in a language that uses dot notation for object field projection, determining the resolution of \( x \) in the expression \( x.x \) requires first determining the object type of \( x \), which in turn requires name resolution again. Thus, we require a unified mechanism for expressing and solving arbitrarily interdependent naming and typing resolution problems.

To address this challenge, we base our framework on a language of constraints. Term equality constraints are a standard choice for...
We extend the name resolution algorithm of [14] to be parametric over scope reachability and visibility policies defined over (generalized) scope graph edge labels.

We give an algorithm for solving combined name and type resolution problems and prove that it is sound with respect to the satisfiability specification.

Outline In Section 2, we introduce the constraint language using example programs in a small model language. In Section 3, we formally define the syntax and semantics of the constraint language by defining a satisfaction relation on constraints and an extended resolution calculus. In Section 4 we develop a constraint solver and prove that it is sound with respect to the semantics. In Section 5 we relate this work to previous work by ourselves and others, and discuss limitations and ideas for future work.

2. Constraints for Static Semantics

In this section we introduce our approach to constraint-based name and type resolution. We show how scope graph constraints are used to model name binding and combine them with typing constraints to model type consistency. We illustrate the ideas using LMR (Language with Modules and Records), a small model language that serves as an example programs in a small model language. In Section 3, we extend the name resolution algorithm of [14] to be parametric over scope reachability and visibility policies defined over (generalized) scope graph edge labels.

We give an algorithm for solving combined name and type resolution problems and prove that it is sound with respect to the satisfiability specification.

Outlines In Section 2, we introduce the constraint language using example programs in a small model language. In Section 3, we formally define the syntax and semantics of the constraint language by defining a satisfaction relation on constraints and an extended resolution calculus. In Section 4 we develop a constraint solver and prove that it is sound with respect to the semantics. In Section 5 we relate this work to previous work by ourselves and others, and discuss limitations and ideas for future work.

2. Constraints for Static Semantics

In this section we introduce our approach to constraint-based name and type resolution. We show how scope graph constraints are used to model name binding and combine them with typing constraints to model type consistency. We illustrate the ideas using LMR (Language with Modules and Records), a small model language that is used as an example language for static semantic analysis tools (Fig. 1). Given the abstract syntax tree of a program, a language-specific extractor produces a set of constraints that express the name binding and type of the program. A language-independent solver attempts to find a solution for the set of extracted constraints, and produces a (partial) name and type assignment. Note that the constraint language is not intended as a domain-specific meta-language (such as NaBL [12]) to be used by language designers using a language workbench. Rather, it is intended to be used as an internal language for the implementation of such meta-languages. (v) The application to erroneous programs is work in progress.

Contributions The specific technical contributions of this paper are the following:

• We introduce a constraint notation for the specification of scope graphs and name resolution that is complementary to the description of traditional typing constraints.

• We extend the scope graph framework of [14] with uniqueness and completeness constraints to express properties such as “there are no duplicate declarations in this scope” or “every declared field in this record is initialized.”

• We introduce generalized scope graph edge labels to model a wide range of scope combination policies including transitive and non-transitive imports, and non-overriding includes.

• We give a specification for satisfiability of combined sets of name and type resolution constraints.
Scope Graph Constraints The edges of a scope graph determine the connections between scopes, declarations, and references. Edges are specified directly by means of scope graph constraints \( C(G) \) in the grammar of Fig. 7, where the ground terms \( D, R, \) and \( S \) represent declarations, references, and scopes, respectively. For now, we only consider the two basic edges that connect declarations and references to scopes:

- A declaration constraint \( s \xrightarrow{x^D} \) specifies that declaration \( x^D \) belongs to scope \( s \). Graphically: \( \xrightarrow{x^D} \)
- A reference constraint \( x^R \xrightarrow{s} \) specifies that reference \( x^R \) belongs to scope \( s \). Graphically: \( \xrightarrow{s} \)

The “solution” to a set of scope graph constraints is a well-formed scope graph, i.e. one in which each declaration and reference belongs to (is connected by an edge with) exactly one scope. Note that the existence of nodes (declarations, references, and scopes) of the scope graph is specified implicitly by their appearance in an edge constraint. For convenience, we sometimes write \( S_c(x^R) = s \) for \( x^R \xrightarrow{s} \) and \( S_c(x^D) = s \) for \( x^D \xrightarrow{s} \). We define by comprehension the sets of declarations and references belonging to a scope \( s \), as \( D(s) = \{ x^D \mid S_c(x^D) = s \} \) and \( R(s) = \{ x^R \mid S_c(x^R) = s \} \). In most contexts, constraints and derived notations are implicitly parameterized by the scope graph under consideration; when they need to be explicitly parameterized by a scope graph \( G \), we use a subscript notation (e.g. \( D_G(s) \)).

Resolution Constraints The basic intuition behind scope graphs is that a reference resolves to a declaration iff there is a path from the reference node to the declaration node. In this case we say that the declaration is visible from the reference. Resolution constraints \( C^{Res} \) in the grammar represent requirements on successful name resolution:

- A resolution constraint \( R \rightarrow D \) specifies that a given reference must resolve to a given declaration. Typically, the declaration is specified as a declaration variable \( \delta \). For example, in Fig. 2 the constraints \( x^4_1 \rightarrow \delta_4 \) and \( x^3_5 \rightarrow \delta_3 \) require that references \( x^4_1 \) and \( x^3_5 \) resolve to (as yet unknown) declarations \( \delta_4 \) and \( \delta_3 \), respectively.

A solution to a set of resolution constraints is a substitution mapping each declaration variable to a declaration, such that applying this substitution to the constraints generates valid resolutions according to the scope graph resolution calculus (which we formalize in Section 3). In Fig. 2, since the only paths starting at \( x^4_1 \) and \( x^3_5 \) both end at declaration \( x^2_2 \), the (sole) solution to these constraints is a substitution mapping both \( \delta_4 \) and \( \delta_3 \) to \( x^2_2 \). Applying this substitution yields the valid resolutions \( x^4_1 \mapsto x^2_2 \) and \( x^3_5 \mapsto x^2_2 \).

In addition to constraints about the resolution of references, \( C^{Res} \) also includes constraints on properties of name collections \( N \), which are multisets of identifiers. For now we only consider the uniqueness constraint:

- A uniqueness constraint \( !N \) specifies that a given name collection \( N \) contains no duplicates.
- A declaration name collection \( D(s) \) is obtained by projecting the identifiers from the set of declarations in scope \( s \).

Thus, for example, in Fig. 2 the constraint \( !D(1) \) requires that scope \( 1 \) should have no duplicate declarations. These types of constraints are satisfied when the property they specify holds.

Typing Constraints Typing constraints \( C^{Ty} \) represent requirements for type consistency of the program:

- A type declaration constraint \( D : T \) associates a type with a declaration. This constraint is used in two flavors: associating a type variable \( \tau \) with a concrete declaration, or associating a type variable with a declaration variable. In Fig. 2, the constraints \( x^6_0 \rightarrow \tau_2 \) and \( x^5_3 \rightarrow \tau_7 \) associate distinct type variables with declarations \( x^6_0 \) and \( x^5_3 \). (For ease of reading, we choose type variable names corresponding to subexpression label numbers.) The constraint \( \delta_3 : \tau_7 \) requires the type of the declaration to which \( x^3_5 \) resolves to be the same as the type \( \tau_7 \) of the reference considered as an expression.

- A type equality constraint \( T \equiv T \) specifies that two types should be equal. In Fig. 2, the constraint \( \tau_2 \equiv \tau_7 \) arises from the constant expression \( x_1 \), and the constraint \( \tau_7 \equiv \tau_5 \) arises from the fact that the \( \equiv \) operator takes integer operands. The constraint \( \tau_7 \equiv \text{Bool} \) arises in two ways, from the fact that \( \equiv \) returns a Boolean and the fact that \( \equiv \) requires one; since constraints should be thought of as a set, we list each distinct constraint only once.

A solution to a set of typing constraints is a substitution on declarations and type variables that satisfies all the constraints. For example, the substitution for \( \tau_7 \) can be deduced either from the constraints \( \tau_7 \equiv \tau_5 \) and \( \tau_5 \equiv \text{Int} \), or from the constraints \( \tau_7 \equiv \text{Int} \), \( \tau_7 \equiv \text{Bool} \) and the unification of \( \tau_7 \) and \( \tau_5 \) (via \( \delta_3 = x^3_5 \)).

Note that for a program to be both well-formed and well-typed, we need to find a single substitution on declaration and type variables that allows both resolution and typing constraints to be satisfied simultaneously. In this simple example, it is clear that the declaration variables are determined solely by the resolution constraints, but this will not always be the case in general.

2.2 Lexical Scope

Only very trivial programs have just a single scope. The left part of Fig. 3 shows an LMR example that illustrates nested lexical scopes. Scope graphs use edges between scopes to model inclusion of the (visible) declarations in one scope in another. They can be used to model lexical nesting or direct import of all the names from one scope into another, according to the label on the edge.

- A direct edge constraint \( s_1 \xrightarrow{l} s_2 \) specifies a direct \( l \)-labeled edge from scope \( s_1 \) to \( s_2 \). (Graphically: \( \xrightarrow{l} \)). The general meaning of such an edge is that the declarations visible in \( s_2 \) are also visible in \( s_1 \). Or, following the direction of the arrow, that a reference in \( s_1 \) can be resolved by searching for a declaration in \( s_2 \).
def n1 = true2
    def f3 = { 
        fun (n4:Int5) { 
            f6(n7) 
        } 
    }
module A1 { 
    def a2 = 43 
}
module B4 { 
    import A5 
    def b6 = ... the record by importing (the associated scope of) 
    the record declaration (via a reference to the name of the type, here

The essence of module-like constructs is that they encapsulate a collection of declarations and make these available through import of the module. That requires an association between the encapsulated declarations and the declaration of the module, which is modeled by associated scopes:

* An association constraint \( x^R \rightarrow s \) specifies \( s \) as the associated scope of declaration \( x^R \). Associated scopes can be used to connect the declaration (e.g. a module) of a collection of names to the scope declaring those names (e.g. the body of a module). Graphically: \( \begin{array}{c} x^R \rightarrow \alpha \end{array} \).

The LMR program in the right part of Fig. 3 consists of two modules \( \alpha_3 \) and \( \alpha_4 \) and an import of the former into the latter. The declarations in these modules are contained in (2) and (3). Each of these scopes is associated with the corresponding declaration of the name of the module, which is represented in a scope graph diagram with an open arrow, e.g. (1). These scopes are also child scopes of the program global scope (1).

Imports A nominal import makes the declarations in an associated scope visible in another, not necessarily lexically related, target scope. A nominal import is represented by (1) a regular reference to the name of the scope being imported, and (2) an import edge of that name into the target scope:

- A nominal edge constraint \( s \xrightarrow{\text{import}} x^R \) specifies a nominal labeled edge from scope \( s \) to reference \( x^R \). (Graphically: \( \begin{array}{c} s \xrightarrow{\text{import}} x^R \end{array} \)) Such an edge makes visible in \( s \) all declarations that are visible in the associated scope of the declaration to which \( x^R \) resolves, according to the label on the edge.

For example, import \( \alpha_5 \) is represented by the reference \( \alpha_5^R \) in scope (2) and an import arrow (3) \( \xrightarrow{\text{import}} \alpha_5 \). It is also possible to import the declarations of another scope directly, using an (ordinary) nameless edge; this feature is used in the next sub-section.

Resolving through Imports Name resolution in the presence of associated scopes and imports proceeds as follows. If a scope \( S_1 \) contains an import \( \alpha_5^R \), which resolves to a declaration \( \alpha_5^D \) with associated scope \( S_2 \), then all declarations in \( S_2 \) are reachable in \( S_1 \). Thus, in the example, reference \( \alpha_5^R \) resolves to declaration \( \alpha_5^D \) since the import \( \alpha_5^R \) resolves to declaration \( \alpha_5^D \) and the associated scope (2) of \( \alpha_5^R \) contains declaration \( \alpha_5^D \). Note that the resolution calculus is parameterized by the policy used to disambiguate conflicting resolutions. Here we use a default policy that prefers imported declarations over declarations in parents; alternatives are discussed in Section 3.4.

2.4 Type-Dependent Name Resolution So far, we have seen how to use resolution constraints to express the dependence of type resolution on name resolution. However, for some language constructs the resolution of a name to its declaration depends on the type of another expression. For example, in a field access expression \( e.f \), in order to resolve the field \( f \), one first needs to find the type of the expression \( e \) and then to look for \( f \) in the scope associated with the type. This scheme induces dependencies on type resolution, not only from name resolution but also from scope graph construction (one does not know in which scope the reference \( f \) lies). We model such type-dependent name resolution by using scope graph constraints with scope variables. The examples in Fig. 4 illustrate the approach.

Field Declaration and Initialization Before we can study field access proper, we need to consider modeling of record types, field declarations, and record initialization. We identify each record type by the declaration of the record name in its type definition, e.g. \( \\text{Rec}(A_5^R) \). We model the fields of a record type definition as declarations (here just \( x^R \) in a scope (here, scope (2)) associated with the record type name declaration \( A_5^D \). The resolution constraint \( \text{IR}(2) \) forbids duplicate field names.

To construct a new record of a declared record type (e.g. \( A_5^R \)), we create a new parentless scope (here, scope (3)) which imports the field names of the record by importing (the associated scope of) the record declaration (via a reference to the name of the type, here
A Constraint Language for Static Semantic Analysis based on Scope Graphs with Proofs

Figure 4. Field access.

The constraint language is parameterized by a family of type constructors \( C^T \), which specifies a scope graph which defines the binding structures of the program. Resolution constraints \( C^{Res} \) describe requirements for all program names to be properly resolved and, where appropriate, to be unique or complete. Typing constraints \( C^{Ty} \) describe requirements for the program to be well-typed. The informal meaning of each constraint form was described by a bulleted definition in Section 2. Constraints can be combined using conjunction (\( C \land C \)) and disjunction (\( C \lor C \)). True represents the trivially satisfiable constraint.

A ground constraint is one having no variables. A scope graph is ground if it is specified by a set of ground scope graph constraints; otherwise it is incomplete.

The constraint language is parameterized by a family of type constructors \( c \in C^{T} \) and a set of labels \( l \in L \). We describe the former here and the latter in Section 3.4.

3. Type Constructors

Types in \( T \) are either type variables \( \tau \) or type constructor applications \( c(\tau, \ldots, \tau) \) with \( c \in C^{T} \), a set of language-specific type constructors. Each constructor \( c \) has an associated arity \( c :: n \). For example, \( Int \) and \( Bool \) are type constructors with arity 0 and \( Fun \) is a type constructor with arity 2. Well-formed constraints respect the arity of the type constructors.

To represent user-defined types, such as classes in object-oriented languages or algebraic data types in functional languages, a type constructor can also include the scope graph declaration corresponding to the type definition. For example, record types in LMR are represented by \( Rec(d) \) with \( d \) a type name declaration in
For simplicity, we describe the algorithm as operating over LMR’s concrete syntax. The algorithm is defined by a family of functions indexed by syntactic category (decl, exp, etc.). Each function takes a syntactic component and possibly one or more auxiliary parameters, and returns a constraint, possibly involving one or more fresh variables or new scope identifiers. Functions are defined by a set of rules, one for each possible syntactic form in the category. For example, \([\cdot]\) has twelve rules, and is parameterized by the scope \(s\) in which identifier references within the expression are to go and the expected type \(t\) of the expression. We use the notation \([\cdot]^s_t\) on sequences of items of syntactic category \(c\) to mean the result of applying \([\cdot]\) to each item and returning the conjunction of the resulting constraints, or True for the empty sequence.

For our basic approach to defining satisfaction is as follows. First assume that we have only ground constraints. Then we can interpret scope graph constraints \(C^G\) directly as a ground scope graph. We next define a satisfiability relation \(\models\) by cases on ground resolution constraints \(C^G\) and typing constraints \(C^Ty\) relative to a context \((G, \psi)\), where \(G\) is a ground scope graph and \(\psi\) is a typing environment mapping declarations in \(D(G)\) to unique ground types in \(T\). In particular, resolution constraints are checked against \(G\) using the parameterized by the scope \(s\) and type \(t\) of the type variable \(\tau\).
The scope graph resolution calculus (described in Section 3.3). Finally, we apply $\models$ with $G$ set to $G'$. To lift this approach to constraints with variables, we simply apply a multi-sorted substitution $\phi$, mapping type variables $\tau$ to ground terms, declaration variables $\delta$ to ground declarations and scope variables $\varsigma$ to ground scopes. Thus, our overall definition of satisfaction for a program $p$ is:

$$\phi(C_R^\varsigma), \psi \models \phi(C_R^{\text{Res}}) \land \phi(C_T^\varsigma) \quad (\phi)$$

where $\phi(E)$ denotes the application of the substitution $\phi$ to all the variables appearing in $E$ that are in the domain of $\phi$. When the proposition $\phi$ holds, we say that $\psi$ and $\phi$ resolve $p$.

### Resolution and Typing Constraints

The $\models$ relation is given by the inductive rules in Fig. 8, where $=\models$ is the syntactic equality on terms and $\vdash_G x_i \rightarrow x_i'$ is the resolution relation for graph $G$. The interpretation of a name collection $[\pi]$ is the multiset defined as follows: $[\mathcal{V}(S)]_G = \pi(\mathcal{D}_G(S))$, $[\mathcal{T}(S)]_G = \pi(\mathcal{R}_G(S))$, and $[\pi(X)]_G = \pi((x_1^{\pi} \mid \exists \pi \cdot \vdash_G p : S \rightarrow x_2^{\pi}))$ where $\pi(A)$ is the multiset produced by projecting the identifiers from a set $A$ of references or declarations. Given a multiset $M$, $1_M(x)$ denotes the multiplicity of $x$ in $M$.

#### 3.3 Resolution Calculus

The resolution calculus defines the resolution of a reference to a declaration in a scope graph as a most specific, well-formed path from reference to declaration through a sequence of edges. A path $p$ is a list of steps representing the atomic scope transitions in the graph. There are three kinds of steps:

- A (direct) edge step $E(I, S_2)$ is a direct transition from the current scope to the scope $S_2$. This step records the label of the scope transition that is used.
- A nominal edge step $N(l, y^\varsigma, S)$ requires the resolution of reference $y^\varsigma$ to a declaration with associated scope $S$ to allow a transition between the current scope and scope $S$.
- A complete path always ends with a declaration step $D(x_2^{\pi})$ that stores the declaration the path is leading to.

A path $p$ is a valid resolution in the graph from reference $x_i^{\pi}$ to declaration $x_2^{\pi}$, such that $\vdash_G p : x_i^{\pi} \rightarrow x_2^{\pi}$ according to the calculus rules in Fig. 9. These rules all implicitly apply to a fixed graph $G$, which we omit to avoid clutter. The calculus defines the resolution relation in terms of edges in the scope graph, reachable declarations, and visible declarations. Here $\text{is}$ is the set of seen imports, a technical device needed to avoid “out of thin air” anomalies in resolution of nominal imports. We often drop $\text{is}$ from a resolution when it is empty. The $\mathcal{S}$ component that appears in the transitive closure rules is the set of seen scopes that are used to prevent cycles in the resolution path of a given reference.

**Figure 7. Syntax of constraints**

| $C$ | $\models C_G \mid C_T \mid C_{\text{Res}} \mid C \land C \mid \text{True}$ |
| $C_G$ | $R \rightarrow S \mid S \rightarrow D \mid S \rightarrow S \mid D \rightarrow S \mid S \rightarrow R$ |
| $C_{\text{Res}}$ | $R \rightarrow D \mid D \rightarrow S \mid !N \mid N \nsubseteq N$ |
| $C_T$ | $T \equiv T \mid D : T$ |

**Figure 8. Interpretation of resolution and typing constraints**

| Resolutions | $s$ | $D(x_2^{\pi}) \mid E(l, S) \mid N(l, x_2^{\pi}, S)$ |
| $p$ | $[] \mid s \mid p \cdot p$ (inductively generated) |
| $\vdash_G p : S \rightarrow x_2^{\pi}$ |

Well-formed paths

$WF(p) \Leftrightarrow labels(p) \in E$

Visibility ordering on paths

$label(s_1) < label(s_2)$

$$\frac{s_1 \cdot p_1 < s_2 \cdot p_2}{p_1 < p_2}$$

Edges in scope graph

$$\frac{S_1 \rightarrow S_2}{1 \vdash E(I, S_2) : S_1 \rightarrow S_2}$$

**Transitive closure**

$$\frac{1 \vdash s : A \rightarrow A}{B \nsubseteq S \vdash s : A \rightarrow B \mid \{B\} \cup s \vdash B \rightarrow C}$$

Reachable declarations

$$\frac{1 \vdash p : S \rightarrow S' \mid WF(p)}{1 \vdash p : S \rightarrow x_i^{\pi}}$$

Visible declarations

$$\frac{1 \vdash p : S \rightarrow x_i^{\pi}}{\forall j, p'(1 \vdash p' : S \rightarrow x_j^{\pi} \rightarrow (p' < p))}$$

Reference resolution

$$\frac{x_2^{\pi} \rightarrow S \mid \{x_2^{\pi}\} \cup 1 \vdash p : S \rightarrow x_2^{\pi}}{1 \vdash p : S \rightarrow x_2^{\pi}}$$

**Figure 9. Resolution calculus from [14] extended for arbitrary edge labels and parameterized with well-formedness predicate $WF$ and visibility ordering $<$. Here $label$ projects the label from a step and $labels$ projects the sequence of labels from a path.**
Lexical scope
\[ L := \{P\} \quad E := P^* \quad D < P \]
Non-transitive imports
\[ L := \{P, I\} \quad E := P^* \cdot I? \quad D < P, D < I, I < P \]
Transitive imports
\[ L := \{P, TI\} \quad E := P^* \cdot TI^* \quad D < P, D < TI, TI < P \]
Transitive Includes
\[ L := \{P, Inc\} \quad E := P^* \cdot Inc^* \quad D < P, Inc < P \]

\[ D < P, D < TI, TI < P, Inc < P, D < I, I < P, \]

\[ \text{Fig. 10. Example reachability and visibility policies by instantiation of path well-formedness and visibility.} \]

3.4 Parameterization

In order to model the name binding features and resolution policies from different programming languages, the scope graph and resolution calculus are parameterized with a set of labels \( L \), a regular expression \( E \) that defines the scope reachability policy, and an order \(<\) on the \( L \) (extended with the built-in \( D \) label) that defines the scope visibility policy. Fig. 9 defines generic predicates derived from these parameters and used in the calculus. The regular expression \( E \) entails a well-formedness predicate \( WF \) on paths obtained by projecting the sequence of labels from the path and testing it for membership in the language of \( E \). The ordering relation on labels entails an ordering relation on paths using the lexicographic order on the projected label sequences.

Fig. 10 presents several example instantiations for these parameters, encoding different policies. The first policy defines lexical scope in which scopes are transitively linked through parent edges (\( P \)) and local declarations shadow declarations in parents. The next policy extends lexical scope with non-transitive imports (\( I \)). The well-formedness predicate allows an optional import at the end of a lexical scope chain, ruling out access to the parents of an imported scope. Further, the policy states that imported declarations are not shadowed included (\( Inc \)) declarations. The final policy combines three import policies, not providing rules to disambiguate between paths through different kinds of import edges. Thus, a reference that can be resolved through an import and an include edge is ambiguous and can be flagged as an error.

4. Resolution Algorithm

In this section, we describe an algorithm for solving constraints in the sense of Section 3.2, i.e. finding \( \phi \) and \( \Psi \) that satisfy \( \phi \). Our algorithm works only for a restricted class of generated constraints: all constraints in \( C^{\phi \Psi} \) must be ground, except that scope variables \( z \) can appear as targets in direct edge constraints (e.g. \( S \rightarrow z \)). This restriction is met by the constraints generated by the LMR collection algorithm in Section 2. Broader classes of constraints might be useful for other languages; we defer exploration of algorithms that could handle these to future work.

4.1 Variables in Scope Graph Constraints

The basic approach of the algorithm is to interpret the scope graph constraints as a scope graph \( G \) and then use it to resolve resolution and typing constraints using a conventional unification-based algorithm. However, since scope graph constraints can contain variables, we cannot fully define the scope graph before starting constraint resolution, because we do not fully know \( \phi \). Thus, our algorithm builds \( \phi \) and \( \Psi \) incrementally. The key idea is that we can solve some resolution and typing constraints even when \( \phi \) is not yet fully defined, in such a way that the solution remains valid as it becomes more defined.

4.2 Name Resolution Algorithm

In order to solve resolution constraints (e.g. \( x^R \rightarrow \delta \)) or to compute the set of visible elements from a scope \( \psi(S) \) we need an algorithm that computes the name resolution relation \( x^R \rightarrow x^P \) as specified by the calculus presented in Section 3.3. We introduced such an algorithm in our prior work [14], but it was specific to a particular set of labels, visibility order, and well-formedness predicate. In this section, we present a generic version of the algorithm that is parameterized by \( L \), \( E \) and \(<\) as described in Section 3.4.

Incomplete Scope Graphs

A further new requirement on the algorithm is that it can operate on an incomplete scope graph, specified by a set of constraints that may still contains variables as the targets of direct edges. The non-strictly positive premise of the \( V \) rule of the resolution calculus makes the derivation of a resolution relation from a graph non-monotonic with respect to additions to the graph. For example, suppose that in some graph \( G \), a reference \( x^R \) in a scope \( S \) resolves to \( x^P \) in the parent scope \( S' \). In a bigger graph \( G' \) that also has a declaration \( x^P \) in \( S' \) itself, \( x^R \) will resolve to \( x^P \), and the old resolution to \( x^P \) will be shadowed. Thus we cannot simply restrict resolution to the complete part of the graph, and expect the results to remain valid as the graph becomes more completely known. Instead, we modify the original algorithm to signal when a result is preliminary.

The Algorithm

Fig. 11 defines a resolution algorithm that works on such incomplete scope graphs. The function for resolving a single reference, \( R[[x^R]](x^P) \), returns either a set of declarations or \( U \) (unknown) if the reference cannot be resolved in the current graph. Similarly, the environment functions \( Env_{\rightarrow}[[l, S]](S) \) return a pair consisting of:

- a result flag, \( T \) (total) if all declarations visible from \( S \) can be computed or \( P \) (partial) if there are still possible additional resolutions (some scope variables are accessible)
• a set of declarations corresponding to resolutions from scope \( S \) that are already certain in this incomplete graph.

When a scope graph contains no variables (i.e. when no partial or unknown flags are raised) the intended behavior of the different functions is the following:

- \( R[[x]](x^R) \) returns the set of declarations to which the reference resolves.
- \( Env_r[[x]](S) \) returns the set of declarations that are reachable from scope \( S \) with a minimal path satisfying the regular expression \( x \).
- \( Env^i_r[[x]](S) \) returns the set of declarations visible from \( S \) through labels in set \( I \) after application of the shadowing policy. Using the labeling order, the declarations accessible through smaller labels shadow the declarations accessible through larger ones.
- \( Env^p_r[[x]](S) \) returns the set of declarations accessible from \( S \) with a \( D \) step, i.e. the set of declarations in \( S \).
- \( Env^l_r[[x]](S) \) returns the set of declarations accessible from \( S \) with an \( l \)-labeled step.
- \( IS^l[[x]](S) \) returns the set of scopes that are accessible through a nominal edge by resolving the reference and returning its associated scope.

The algorithm uses the following auxiliary notation and definitions:

- \( \emptyset \) denotes the empty regular expression and given a path \( p \) and a regular expression \( x \), \( p \in re \) denotes that labels \( (p) \) is in the language of \( x \). The shadowing operator \( \lhd \) on sets of declarations is defined by: \( D_1 \lhd D_2 \triangleq \{ x^D \mid x^D \in D_1 \lor (x^D \in D_2 \land \exists j, x^D \in D_1) \} \).

The shadowing operators on pairs with result flag are defined by:
\[
(f_1, D_1) \lhd (f_2, D_2) \triangleq \begin{cases} (f_2, D_1 \lhd D_2) & \text{if } f_1 = T \\ (P, D_1) & \text{otherwise} \end{cases}
\]

The union \( \cup \) operator over pairs with result flag is defined as:
\[
\bigcup_{i \in I} (f_i, D_i) \triangleq \begin{cases} (T, D) & \text{if } \forall i \in I, f_i = T \\ (P, D) & \text{otherwise} \end{cases}
\]

where \( D = \{ x^D \in \cup_{i \in I} D_i \mid \forall j \in I, f_j = T \lor \exists x^D_i \in D_j \} \). Given a regular expression over labels \( re \) and a label \( l \), \( l ^{\rightarrow} re \) denotes the Brzozowski derivative[2] of \( re \) by \( l \). Given a partially ordered set \( L \), \( Max(L) \) denotes the set of maximal elements of \( L \), i.e. \( \{ l \in L \mid \nexists l' \in L, l < l' \} \). Given a scope \( S \) and a label \( l \), we define:
\[
S^l = \{ x^S \mid S \xrightarrow{\cdot} x^S \} \quad S^l = \{ S' \mid S \xrightarrow{\cdot} S' \}
\]

### 4.3 Correctness

We want to prove the correctness of this algorithm with respect to the calculus introduced in Section 3.3. Details of the proofs can be found in the appendix of the extended version [17].

**Termination** First notice that the algorithm terminates using the lexicographic ordering \#(\( R(G) \)), \#(\( S(G) \)), \#(A), where \#(A) denotes the cardinality of set \( A \) and \( \triangleq \) denotes the following well founded order among the different functions:
\[
Env_r > Env^i_r > Env^p_r > IS > R
\]

This termination order is used as the induction principle in most of the proofs.

**Correctness on ground scope graphs** We want to prove that when this algorithm operates on a ground scope graph, it is sound and complete with respect to the calculus presented in Fig. 9. First, it is trivial to prove that on a ground scope graph, the return flag can never be \( \emptyset \) or \( U \), therefore in this section we forget about the flag and assume that the \( Env \) functions return a set of declarations.

To prove the correctness of the algorithm, we consider the set of paths that corresponds to the set of declarations returned by the different functions. Given two sets of scopes \( I \) and \( S \) and a scope \( S \), we define \( P[I,S]((S)) \) as:
\[
\{ p \cdot D(d) \mid \exists S', I, S \cup \{ S \} \vdash p : S \rightarrow S' \land Sc(d) = S' \}
\]

and given a path \( p \) such that \( p = p' \cdot D(d), \Delta(p) \) denotes the declaration \( d \). For a set of paths \( S, \Delta(S) \) denotes its corresponding set of declarations \( \{ \Delta(p) \mid p \in S \} \) and
\[
\lll S \triangleq \{ p \cdot D(x^D) \in S \mid \forall (p' \cdot D(x^D')) \in S, \lnot p' < p \}
\]

Given these definitions, we can state the correctness of the algorithm:

**Lemma 1** (Resolution algorithm correctness). On a ground scope graph, we have the following equivalences:
\[
R[[x]](x^R) = \Delta(\{ p \mid \exists l, \lll p \rightarrow x^R \})
\]

\[
 Env^l_r[[x]](S) = \{ \emptyset \mid S \in S \}
\]

\[
 Env_r[[x]](S) = \{ \Delta(\{ p \mid p \in P, \lll l \rightarrow x^R \}) \}
\]

\[
 Env^p_r[[x]](S) = \{ \Delta(\{ D(d) \mid d \in D \land \lll l \rightarrow x^R \}) \}
\]

\[
 IS^l[[x]](S) = \{ S' \mid \exists y^R, \lll l \rightarrow N(l, y^R, S') \}
\]

**Proof.** The proof is by induction on the termination order of the algorithm. Key observations are that all the considered sets of paths are finite since all the paths are acyclic and if there is a minimal path \( s \cdot p \) from scope \( S \) with \( l \rightarrow x^R \) then its tail \( p \) is also minimal from \( S' \), due to the lexicographic ordering.

**Correctness on incomplete scope graphs** We now want to state the general correctness of the algorithm that can operate on incomplete scope graphs. We first extend this definition of resolution as follows. Given an incomplete scope graph \( G \), a reference \( x^R \) is said to resolve to a declaration \( x^D \) if and only if this resolution is valid in all ground instances of \( G \):
\[
\vdash_G x^R \rightarrow x^D \triangleq \forall \phi, \vdash_{G(\phi)} x^R \rightarrow x^D
\]

where we write \( \vdash \) for the resolution relation for graph \( G \) and \( \phi(G) \) is the ground scope graph corresponding to the application of substitution \( \phi \) to variables in \( G \). Similarly a declaration \( x^D \) is visible from scope \( S \) in an incomplete scope graph \( G \) if and only if it is visible in all the ground instances.

In order to be able to resolve uniqueness constraints for a program we also want to ensure that an incomplete graph provides all the possible resolutions of a given reference. In particular, if a resolution is unique in an incomplete graph, we want to be sure it is unique in all its ground instances. An incomplete graph \( G \) is stable for a reference or a scope \( \alpha \), denoted \( G \vdash_{\alpha} \), if all the resolutions in all its ground instances are the same:
\[
G \vdash_{\alpha} \triangleq \forall \phi, \phi', \vdash_{G(\phi)} x^R \rightarrow x^D \Rightarrow \vdash_{G(\phi')} x^R \rightarrow x^D
\]

**Soundness** Given this definition, we can prove that the algorithm on incomplete graphs is correct with respect to the calculus:

**Lemma 2.** For any incomplete graph \( G \):
\[
x^D \in R_G(x^R) \Rightarrow \vdash_G x^R \rightarrow x^D \land G \vdash_{x^R}
\]

where \( R_G(x^R) \) denotes the top-level resolution function \( R[\emptyset](x^R) \) for the graph \( G \).
Lemma 1 states that this property holds when the graph $G$ is ground. We next prove that if the resolution on an incomplete graph $G'$ terminates with a total flag $T$ then for any graph $G'$ that is an instance of $G$, the result is the same.

$$\text{Env}_{\pi}[I,S][x^n]_{G'} = (T, D) \implies \text{Env}_{\pi}[I,S][x^n]_{G} = (T, D)$$  \hspace{1cm} (i)

**Proof.** We prove this result along with similar result for all the other functions by induction on the termination order of the algorithm. The fact that the result is total implies that the results of all the recursive calls are also total and this allows us to apply the desired induction hypothesis (when a $P$ or $U$ flag is raised it is always propagated).

Now we show that the resolution is also correct in the partial case. Let $G$ be an incomplete scope graph and $G'$ one of its instances. If a resolution on $G$ contains a set of declarations for a given name then the resolution on $G'$ contains the same declarations for this name:

$$\text{Env}_{\pi}[I,S](S)_{G} = (\lambda, D) \implies \text{Env}_{\pi}[I,S](S)_{G'} = (\lambda, D') \implies \forall x, \{x^D \in D\} \neq \emptyset \implies \{x^D \in D\} = \{x^{D'} \in D'\} \hspace{1cm} (ii)$$

**Proof.** We prove this result along with similar result for all the other functions by induction on the termination order of the algorithm, using (i).

Finally, we can prove Lemma 2:

**Proof.** Let $S_x = R_G(x^n)$ and pick $x^D \in S_x$. To prove that $x^n$ resolves to $x^D$ in $G$, let $G'$ be an arbitrary ground instance of $G$. Using (ii) we have $x^D \in R_G(x^n)$ and by Lemma 1 we have $\vdash_{G'} x^n \rightarrow x^D$. By $\phi$, we get that $\vdash_{G} x^n \rightarrow x^D$.

To prove stability, let $G_1$ and $G_2$ be ground instances of $G$. Then using (ii), we have $R_{G_1}(x^n) = R_{G_2}(x^n) = S_x$, so by definition we have $G \downarrow x^n$.

### 4.4 Name Collection Computation

This resolution algorithm on partial graphs is used to compute not only resolution of references but also the set of names visible from a given scope. Given an incomplete graph $G$ and a scope $S$, we compute name collections as:

$$N_G(S) = \pi(D_G(S)) \hspace{1cm} N_G(\pi(S)) = \pi(R_G(S))$$

$$N_G(\pi(S)) = \pi(x^D \in \exists E, \text{Env}_{\pi}[I,\emptyset,\emptyset][S]_{G'} \land x^D \in E)$$

**Lemma 3** (Name computation soundness). If the computation of a name collection $E$ terminates on an incomplete graph $G$, its results is the semantics of the name collection for any graph $G'$ that is an instance of $G$:

$$N_G(E) = M \implies [E]_{G'} = M.$$  \hspace{1cm} (i)

### 4.5 Constraint Solving Algorithm

With this name resolution algorithm in hand, Fig. 12 gives an algorithm to solve the constraint system from Section 3. The algorithm is a non-deterministic rewrite system working over tuples $(C, G, \psi)$ of a constraint, a scope graph, and a typing environment. It is non-deterministic in the sense that rules may be applied to any atomic constraint in any order considering that $\land$ is associative and commutative.

Name resolution introduces ambiguity, since a reference $x^n$ may resolve to multiple definitions. If this happens the solver branches, picking a different resolution for $x^n$ in every branch. The returned solution is a set of all the $(C, G, \psi)$ tuples the solver was able to construct. The initial state of the solver is the collected constraint, the (incomplete) scope graph built from the scope graph constraints and an empty typing environment. The algorithm will eliminate clauses from $C$ while instantiating $G$ and filling $\psi$.

The algorithm terminates when the constraint is empty or no more clauses can be solved. Each rule solves one constraint, possibly updating components of the tuple or applying a substitution to it.

- **Rule S-Resolve** solves resolution constraints $x^n \rightarrow \delta$ using the resolution algorithm from Fig. 11. If a resolution is found, it is substituted for the variable $\delta$. If the scope graph is incomplete, the algorithm might return $U$, in which case the constraint is left to be solved later.
- **Rule S-ASSOC** solves scope association constraints $x^D \sim \varsigma$ by looking up the scope $S$ associated with ground declaration $x^D$ in the scope graph. By substituting $S$ for $\varsigma$, the scope graph becomes more complete, possibly allowing more references to be resolved.
- **Rule S-EQUAL** solves equality constraints $T_1 \equiv T_2$. It uses first order unification $U(T_1, T_2)$, as described in [1]. The resulting substitution is applied to the tuple.
- **Rule S-Unique** solves $\forall N$ constraints by checking that the identifier collection $N$ can be computed and all identifiers in it are distinct. ($\mu(x)$ is the multiplicity of $x$ in $A$).
- **Rule S-SubName** solves $N_1 \subseteq N_2$ constraints by checking that the identifier collections $N_1$ and $N_2$ can be computed and that every identifier in $N_1$ is also in $N_2$.
- **Rule S-TypeOf** solves type assignment constraints $x^D : T$. The rule considers two cases. When no type assignment is declared for $x^D$ in $\psi$ (i.e. the first time that it is encountered) the assignment is added to the typing environment $\psi$. When a type assignment is declared (i.e. for subsequent encounters), the type $T$ from the constraint is unified with the type $\psi(x^D)$ from the typing environment.

The constraint resolution algorithm is sound with respect to the constraints semantics.

**Lemma 4** (Constraint Solver correctness). If the algorithm produces a solution to a resolution problem then the solution is valid: for all $C, G, G', \psi$:

$$(C, G, \emptyset) \rightarrow^* (\text{True}, G', \psi') \implies \exists \phi, \phi(G) = G' \land \forall \sigma, \sigma G', \sigma \psi' \models \sigma(\phi(C)).$$

**Proof.** To prove this result we first state some results on the auxiliary unification.

**Unification**: If $U(t_1, t_2) = \sigma$ then $\sigma t_1 = \sigma t_2 \land \sigma = \sigma$. See [1] for a survey on unification problem and unification algorithms for first order terms.

**Resolution Soundness**: Now we can prove the Lemma 4 of the constraint resolution algorithm. We first prove that for each reduction step, if the output is satisfiable, the input is also satisfiable in the same definition-to-type environment:

$$\forall (C_1, G_1, \psi_1), (C_2, G_2, \psi_2) \rightarrow (C_2, G_2, \psi_2) \implies$$

$$\exists \sigma', \sigma'(G_1) = G_2 \land$$

$$\forall \sigma, (\sigma(G_2), \sigma \psi_2) \models \sigma(C_2) \Rightarrow$$

$$\sigma(G_2, \sigma \psi_2) \models \sigma \sigma'(C_1)$$

(1)

The proof of this property is by case analysis on the reduction step. From it, we can prove Lemma 4 by a simple induction on the number of reduction steps.
5. Related Work and Discussion

In this section, we discuss the relation of this paper with previous and other related work, and discuss limitations and ideas for future work.

Previous Work The work in this paper is based closely on our previous theory of name resolution [14], which we extend and generalize here as follows: (i) a scope graph is now defined directly by a set of constraints; (ii) we generalize the parent relation to an arbitrary labeled direct edge between pairs of scopes, and the named import relation to an arbitrary labeled nominal edge between scopes and references; (iii) we extend the resolution algorithm to handle arbitrary well-formedness conditions expressed as regular expressions over arbitrary sets of path labels and arbitrary visibility orderings on labels; (iv) we support partial resolution over incomplete scope graphs; (v) we add the seen-scopes component, previously an artifact of the resolution algorithm, to the resolution calculus to prevent cyclic resolution paths.

The development of the scope graph framework fits in an ongoing line of research to provide high-level domain-specific support for name binding and type analysis in the Spoofax Language Workbench [10] using the NaBL and TS meta-DSLs [12, 19, 18]. NaBL is a DSL for defining the name binding rules of programming languages by identifying the references, definitions, scopes, and imports in an abstract syntax tree without recourse to environments or symbol tables [12]. TS is a complementary DSL for defining type analysis rules. (The design of TS is not formally published, but it is sketched in [18].) Rules in TS are similar to traditional typing judgments, relating an expression to a type. However, type rules do not have to propagate context information, since that is taken care of by the separate binding rules. TS rules refer to the results of name analysis produced by NaBL (e.g. definition of x has type t), and NaBL rules refer to the results of type analysis to achieve type-dependent name resolution. NaBL and TS are implemented by generation of (1) a language-specific AST traversal that generates ‘tasks’, and (2) a language-independent task engine that evaluates tasks in order to (incrementally) compute a name and type assignment [19]. The resulting name and type analysis engines produce Eclipse IDE support for editor services such as name and type error checking, reference resolution, and code completion.

While NaBL and TS are used in practice to build language definitions with Spoofax, the lack of a solid theoretical foundation was a problem for further development. The aim to verify properties of language definitions [18] requires a semantics that can be explained to a proof assistant such as Coq. In particular, the semantics of notions such as imports and ‘subsequent scope’ were hard to capture. NaBL has some limitations in its coverage of name binding patterns. For example, it cannot express variations on let bindings such as sequential and parallel let. While the task engine is constraint-like, its type resolution is not based on unification, which entails that TS cannot be used to express languages requiring type inference. The constraint language developed in this paper provides a solid formal basis for developing a new generation of name binding and type specification languages.

Prototype Implementation We have developed a prototype implementation of the constraint solver and applied it in the IDE generated with the Spoofax Language Workbench [10] for the LMR model language used in this paper. However, the prototype does not yet implement the parameterized name resolution algorithm developed in this paper, but uses the fixed policy from [14]. In the prototype implementation, sets of constraints for erroneous programs lead to partial solutions with unsolvable residual constraints that can be translated into error messages in an IDE. However, we have not formalized this; we have only proven the soundness of the solver for successful reductions. Furthermore, the implementation is not optimized, nor does it support incremental evaluation of constraints in the sense of the NaBL/TS task engine [19].

Constraints The use of constraints to abstract out type inference problems from the abstract syntax tree is a common approach in implementations and extensions of the Hindley/Milner type system [13] and has been applied to a huge variety of typing features. However, these approaches do not address name resolution using constraints, but rather perform name resolution during constraint collection. For example, in the work of Palsberg et al. [15, 16] on object-oriented type systems, constraints are associated with identifiers, which requires these to be resolved before constraint collection. We believe that our use of constraints to define static name resolution is novel. Instead of performing name resolution during constraint collection, we provide a reusable set of constraints to express name resolution problems, including name resolution for ‘remote’ names through imports and the interaction between name and type resolution in type-dependent name resolution.

A variation on traditional type system definitions using inference rules is the co-contextual approach of Erdweg et al. [5]. Instead of propagating an environment to the sub-terms, environments are ‘synthesized’ along with type constraints, and the constraints and environments for sub-terms are merged. This allows for compositional and incremental processing of name and type constraints. Name resolution is expressed using operations on environments. It would be interesting to consider a bottom-up collection of constraints in our approach. The extraction algorithm of Fig. 6 can be reformulated as a bottom-up collector, using scope variables as placeholders for as yet unknown scopes. However, a key difference with our approach is the support for imports (and nominal instead of structural record types, which requires inspecting the AST associated with a type declaration), which precludes a representation of context information using a flat environment. A general challenge lies in the convergence of these approaches: how to realize incremental name and type analysis in the face of imports?

Attribute Grammars Another common approach to the implementation of static semantic analysis is by means of attribute gram-

---

**Figure 12. Constraint solving algorithm**

\[
\begin{align*}
(x^N \mapsto \sigma \land C, G, \psi) & \rightarrow (\sigma \mapsto \rho \{C, G, \psi\}) & \text{where }\rho \in R_\sigma(x^N) & \text{(S-RESOLVE)} \\
(x^N \mapsto \sigma \land C, G, \psi) & \rightarrow (\sigma \mapsto \rho \{C, G, \psi\}) & \text{where }\rho \in R_\sigma(x^N) & \text{(S-ASSOC)} \\
(T_1 \equiv T_2 \land C, G, \psi) & \rightarrow (T_1 \equiv T_2 \land C, G, \psi) & \text{where }U(T_1, T_2) = \sigma & \text{(S-EQUAL)} \\
((N \land C, G, \psi) & \rightarrow (C, G, \psi) & \text{where }\forall x \in N_G(N), 1_{N_G(N)}(x) = 1 & \text{(S-UNIQUE)} \\
(N_1 \subset N_2 \land C, G, \psi) & \rightarrow (C, G, \psi) & \text{where }N_G(N_1) \subset N_G(N_2) & \text{(S-SUBNAME)} \\
(x^O : T \land C, G, \psi) & \rightarrow \{ (C, G, \psi \mapsto \rho) \cup \psi(x^O) \mapsto T \land C, G, \psi \} & \text{if }x^O \not\in \text{dom}(\psi) & \text{(S-TYPEOF)} \\
(\text{True} \land C, G, \psi) & \rightarrow (C, G, \psi) & \text{(S-TRUE)}
\end{align*}
\]


mats [11]. In traditional attribute grammars all ‘semantic’ operations are carried out in the value domain. Thus, name resolution is expressed by propagating a type environment or symbol table through attribute values. Kastens and Waite [9] provide a reusable ADT for the definition of name analysis that bears some resemblance to our scope graph framework, although the treatment of modules and imports is only discussed at the implementation level. Such attribute grammars would be a suitable mechanism for the definition of constraint collection. The extraction algorithm in Fig. 6 could easily be rephrased as an attribute grammar with scopes and type variables as inherited attributes and constraints as synthesized attribute. In reference attribute grammars [7], attributes can get references to tree nodes as values. Thus, attributes can be used to link references (in the scope graph sense) to their declarations. For example, Ekman and Hedin [3] provide a generic framework for name resolution based on generic reference attributes. Though this framework is part of the JastAdd Java compiler, it can be reused for other languages as well. The framework needs to be instantiated with language-specific lookup functions to resolve names. These can be specified modularly per language construct, making it possible to echo the structure of the Java language specification of name binding closely. However, these lookup functions programatically encode name binding idioms such as lexical scoping, shadowing, and hiding. Reference attributes can also be used in the specification of type analysis. Similar to our approach, name binding and typing rules can be specified mostly separately. In a generic framework, Ekman and Hedin [4] use reference attributes to link language constructs to their types and to represent type relations such as subtyping. Similar to name resolution, instantiations of the framework need to be encoded programatically. Modularity and extensibility require particular encoding patterns such as double dispatch.

The distinctive feature of our approach is that we treat name resolution using a largely separate mechanism, the scope graph, rather than integrating it into type resolution. Since some language constructs require type-dependent name resolution, there is inevitably some interaction between naming and typing, but we are still able to reuse most of our existing name resolution theory, which gives us the ability to handle a very rich variety of name binding schemes.

Future Work There are many directions for future work. One important goal is to extend our theory to handle languages with more sophisticated typing features, including subtyping, type-parameterized classes and functions, and modules with type signatures. To support popular OO language idioms, we also need to add support for multiple independent name spaces (and disambiguation across them) and type-based overloading resolution. As we make such extensions, we would also like to address the completeness of the constraint resolution algorithm (on suitably restricted sets of constraints). In particular, it would be interesting to integrate approaches to type error recovery [8, 20, 21] in order to generate good quality type error messages automatically.

On a pragmatic front, more analysis and implementation experiments are needed to determine if our approach will scale to real-world tools. In particular, we need to assess the theoretical and actual efficiency of our constraint solving algorithm. In addition, many applications for semantic analysis (e.g. in IDEs) require efficient incremental computation of name and type resolution.

On the usability front, we are interested in evaluating the expressivity and understandability of our constraint language and of higher-level name and type specification languages that we express in terms of it. Is there a payoff to the use of high-level, but perhaps more abstract concepts, in contrast to a direct implementation?

Finally, we are interested in extending the application of our building block approach to other tasks where constraint-based methods have proved useful, such as pointer analysis.

Acknowledgments We thank the anonymous reviewers for their feedback on previous versions of this paper. This research was partially funded by the NWO VICI Language Designer’s Workbench project (639.023.206). Andrew Tolmach was partly supported by a Digiteo Chair at Laboratoire de Recherche en Informatique, Université Paris-Sud.

References

A. Proofs
A.1 Proof of Lemma 1
Lemma 5. Given ≃ an equivalence relation, let Min≃(A) = {x ∈ A | ∀y ∈ A, x ≃ y ⇒ ¬y < x} in (A ∪ B).

Proof. Let (H) be the definition of ≃. Assume x ∈ Min≃(A), by definition we have x ≃ y and then (1) x ∈ A ∪ B and (2) ∀y ∈ A, x ≃ y ⇒ ¬y < x.

We want to prove ∀y ∈ A ∪ B, x ≃ y ⇒ ¬y < x. Assume y ≃ x and contraction with (2) if y < x then (H) we have z ≃ x, x ≃ y ⇒ ¬y < x. If y ∈ A then using (H) we have z ≃ x, x ≃ y ⇒ ¬y < x. Assume y /∈ A then contradiction (2).

Thus x ∈ Min≃(A ∪ B).

Lemma 6. We have a similar result with the shadowing operator on path sets:

∀AB, A ⊆ B ⇒

(proof similar to Lemma 5).

Proof. Let N(p, p′) = (Name(p) = Name(p′)) and ∀S, (∀(p, p′) ∈ S).

Lemma 7 (Termination). The name resolution algorithm presented in Fig. 11 terminates.

Proof. In Fig. 13, we associate to each function call c its measure M(c) as a 4-tuple of integers, S(G) and R(G) respectively denotes the set of scopes and of references of the graph G and #A the cardinality of a set A. We can easily prove that this measure decreases for the lexicographic ordering at each recursive call and therefore that the algorithm terminates.

Now we can proceed for the proof of Lemma 1. Fig. 14 presents the different sets of path and scopes for the different functions. Using these definitions, we now prove the following lemma:

Lemma 8 (Resolution algorithm correctness (Lemma 1)). On a ground scope graph, we have the following equivalences

The proof is done by induction on the termination measure of the algorithm. All cases are described in Figures 15 and 16.

A.2 Proof of Lemma 2
Lemma 9 (Lemma 2). For any incomplete graph G:

where R_G(x^G) denotes the top-level resolution function R(θ)(x^G) for the graph G.

Lemma 1 states that this property holds when the graph G is ground. We next prove that if the resolution on an incomplete graph G terminates with a total flag T then for any graph G' that is an instance of G, the result is the same.

Proof. We prove this result along with similar result for all the other functions by induction on the termination order of the algorithm.

Now let us prove that the resolution is also correct in the partial case. Let G be an incomplete scope graph and G' one of its instances. If a resolution on G contains a set of declarations for a given name then the resolution on G' contains the same declarations for this name:

(ii)∀x, {x^D ∈ D} ⇒ {x^D ∈ D'} (ii)

Proof. We prove this result along with similar result for all the other functions by induction on the termination order of the algorithm.

Finally, we can prove Lemma 2:

Proof. Let S_2 = R_G(x^G) and pick x^D ∈ S_2. To prove that x^G resolves to x^D in G, let G' be an arbitrary ground instance of G. Using (ii) we have x^G ∈ R_G(x^G) and by Lemma 1 we have x^G ∈ R_G(x^G) → x^D. By (i), we get that x^G ∈ R_G(x^G) → x^D.

To prove stability, let G_1 and G_2 be ground instances of G. Then using (ii), we have R_G_1(x^G_1) = R_G_2(x^G_2) = S_2, so by definition we have x^G_1 = x^G_2.
\[
M(R[I](x^R)) = \begin{cases} 
#(R(G)\setminus I), #S(G), 5, 0) \text{ when } x^R \in I \\
#(R(G)\setminus I), #S(G), 0, 0) \text{ when } x^R \notin I 
\end{cases}
\]
\[
M(Env_{re[I,S]}(S)) = \begin{cases} 
#(R(G)\setminus I), #S(G), 5, 0) \text{ when } x^R \in I \\
#(R(G)\setminus I), #S(G), 0, 0) \text{ when } x^R \notin I 
\end{cases}
\]

Assume there is \(\sigma\) such that \(\sigma(\sigma'(G,\psi))M|= \sigma(\sigma'(C)) (H)\)
then we want to prove:

\[
\sigma\sigma'(G,\psi)M|= \sigma\sigma'(x^R \mapsto \delta \land C)
\]

### 13. Functions Measure

\[
F_{R[I]}(x^R) \triangleq \{ p \mid \exists d, I \vdash p : x^R \rightarrow d \}
\]
\[
P_{re[I,S]}(S) \triangleq \{ d \mid \vdash d \in P[I,S](S) \} \text{ otherwise}
\]
\[
P_{re[I,S]}(S) \triangleq \{ d \mid \vdash d \in S \}
\]
\[
P_{I,S}[I,S](S) \triangleq \{ S' \mid \forall y^R, I \vdash N(I,y^R,S') : S \rightarrow S' \}
\]
\[
P_{I,S}[I,S](S) \triangleq \{ p \mid \exists l, p \in P[I,S](S) \}
\]

### 14. Path Sets

#### A.3 Proof of Lemma 4

**Lemma 10** (Lemma 4).

\[
\forall C, G, G', \psi' : (C, G, 0) \rightarrow^* (G', F^\leq C, \psi') \Rightarrow \\
\exists \phi, \phi(G) = (G') \land \\
\forall \sigma, \sigma(G'), \sigma(\psi') = \sigma(\phi(C)) (\phi)
\]

**Proof.** To prove this result we first state some results on the auxiliary unification and least upper bound computations.

**Unification:** If \(U(t_1, t_2) = \sigma\) then \(\sigma_1 = \sigma_2 \land \sigma = \sigma.\) See [1] for a survey on unification problem and unification algorithms for first order terms.

**Resolution Soundness:** Now we can prove the Lemma 4 of the constraint resolution algorithm. We first prove that for each reduction step, if the output is satisfiable, the input is also satisfiable in the same definition-in-type environment. This is stated by the following property:

\[
\forall(C_1, G_1, \psi_1), (C_2, G_2, \psi_2), \\
(C_1, G_1, \psi_1) \rightarrow (C_2, G_2, \psi_2) \Rightarrow \\
\exists \sigma', \sigma'(G_1) = (G_2) \land \\
\forall \sigma, \sigma(G_2), \sigma(\psi_2) = \sigma(C_2) \Rightarrow \\
\sigma'(G_2), \sigma(\psi_2) \approx \sigma' \sigma(C_1) (i)
\]

The proof of this property is by case analysis on the reduction step.

**Proof of property †** In this proof, given a triple \((G, \psi)\), we denote \((G, \psi)^{\mathcal{M}}\) the triple \((G, \leq_{\mathcal{M}}, \psi)\).

We want to prove the following property about the constraint resolution system presented in Figure 12:

\[
\forall(C_1, G_1, \psi_1), (C_2, G_2, \psi_2), \\
(C_1, G_1, \psi_1) \rightarrow (C_2, G_2, \psi_2) \Rightarrow \\
\exists \sigma', \sigma'(G_1) = (G_2, F^\leq C) \land \\
\forall \sigma, \sigma(G_2), \sigma(\psi_2)^{\mathcal{M}} = \sigma(C_2) \Rightarrow \\
\sigma(G_2), \sigma(\psi_2)^{\mathcal{M}} \approx \sigma' \sigma'(C_1) (i)
\]

**Proof.** We prove this property by case analysis on the reduction:

\[
(C_1, G_1, \psi_1) \rightarrow (C_2, G_2, \psi_2)
\]

- **S-RESOLVE** Assume:

\[
(x^R \mapsto \delta \land C, G, \psi) \rightarrow [\delta \mapsto x^D](C, G, \psi)
\]

where \(x^D \in R_D(x^R)\) and let \(\sigma' = [\delta \mapsto x^D].\)

Assume there is \(\sigma\) such that

\[
\sigma(\sigma'(G, \psi))^\mathcal{M} = \sigma(\sigma'(C)) (H)
\]

then we want to prove:

\[
\sigma\sigma'(G, \psi)^\mathcal{M} = \sigma\sigma'(x^R \mapsto \delta \land C)
\]
- **Case** $R[I](x^R)$
  $x^R \in R[I](x^R) \iff \text{(Def)}$

- **Case** $\mathsf{Env}_E[x^R \cup I, \emptyset](S)$ where $\mathsf{Sc}(x^R) = S \iff \text{(IH with #I)}$
  $\exists p, p \cdot D(x^D) \in \mathsf{Env}_E[x^R \cup I, \emptyset](S)$ \text{(IH with #I)}$

- **Case** $\mathsf{Pre}[I,S](S)$
  $x^R \in \mathsf{Env}_E[x^R \cup I, \emptyset](S)$ \text{(Def)}$

Figure 15. Proof of Lemma 1, Pt. 1

- **Case** $\mathsf{Env}_E[x^R \cup I, \emptyset](S)$ where $\mathsf{Sc}(x^R) = S \iff \text{(IH with #I)}$
  $\exists p, p \cdot D(x^D) \in \mathsf{Env}_E[x^R \cup I, \emptyset](S)$ \text{(Def)}$

- **Case** $\mathsf{Pre}[I,S](S)$
  $x^R \in \mathsf{Env}_E[x^R \cup I, \emptyset](S)$ \text{(Def)}$

QED

- **Case** $\mathsf{Env}_E[x^R \cup I, \emptyset](S)$ where $\mathsf{Sc}(x^R) = S \iff \text{(IH with #I)}$
  $\exists p, p \cdot D(x^D) \in \mathsf{Env}_E[x^R \cup I, \emptyset](S)$ \text{(Def)}$

- **Case** $\mathsf{Pre}[I,S](S)$
  $x^R \in \mathsf{Env}_E[x^R \cup I, \emptyset](S)$ \text{(Def)}$

QED

Let $\exists S \cdot p$.

- **Case** $\mathsf{Env}_E[x^R \cup I, \emptyset](S)$ where $\mathsf{Sc}(x^R) = S \iff \text{(IH with #I)}$
  $\exists p, p \cdot D(x^D) \in \mathsf{Env}_E[x^R \cup I, \emptyset](S)$ \text{(Def)}$

- **Case** $\mathsf{Pre}[I,S](S)$
  $x^R \in \mathsf{Env}_E[x^R \cup I, \emptyset](S)$ \text{(Def)}$

QED

Let $\exists S \cdot p$.

- **Case** $\mathsf{Env}_E[x^R \cup I, \emptyset](S)$ where $\mathsf{Sc}(x^R) = S \iff \text{(IH with #I)}$
  $\exists p, p \cdot D(x^D) \in \mathsf{Env}_E[x^R \cup I, \emptyset](S)$ \text{(Def)}$

- **Case** $\mathsf{Pre}[I,S](S)$
  $x^R \in \mathsf{Env}_E[x^R \cup I, \emptyset](S)$ \text{(Def)}$

QED

Let $\exists S \cdot p$.

- **Case** $\mathsf{Env}_E[x^R \cup I, \emptyset](S)$ where $\mathsf{Sc}(x^R) = S \iff \text{(IH with #I)}$
  $\exists p, p \cdot D(x^D) \in \mathsf{Env}_E[x^R \cup I, \emptyset](S)$ \text{(Def)}$

- **Case** $\mathsf{Pre}[I,S](S)$
  $x^R \in \mathsf{Env}_E[x^R \cup I, \emptyset](S)$ \text{(Def)}$

QED

Let $\exists S \cdot p$.

- **Case** $\mathsf{Env}_E[x^R \cup I, \emptyset](S)$ where $\mathsf{Sc}(x^R) = S \iff \text{(IH with #I)}$
  $\exists p, p \cdot D(x^D) \in \mathsf{Env}_E[x^R \cup I, \emptyset](S)$ \text{(Def)}$

- **Case** $\mathsf{Pre}[I,S](S)$
  $x^R \in \mathsf{Env}_E[x^R \cup I, \emptyset](S)$ \text{(Def)}$

QED

Let $\exists S \cdot p$.

- **Case** $\mathsf{Env}_E[x^R \cup I, \emptyset](S)$ where $\mathsf{Sc}(x^R) = S \iff \text{(IH with #I)}$
  $\exists p, p \cdot D(x^D) \in \mathsf{Env}_E[x^R \cup I, \emptyset](S)$ \text{(Def)}$

- **Case** $\mathsf{Pre}[I,S](S)$
  $x^R \in \mathsf{Env}_E[x^R \cup I, \emptyset](S)$ \text{(Def)}$

QED

Let $\exists S \cdot p$.

- **Case** $\mathsf{Env}_E[x^R \cup I, \emptyset](S)$ where $\mathsf{Sc}(x^R) = S \iff \text{(IH with #I)}$
  $\exists p, p \cdot D(x^D) \in \mathsf{Env}_E[x^R \cup I, \emptyset](S)$ \text{(Def)}$

- **Case** $\mathsf{Pre}[I,S](S)$
  $x^R \in \mathsf{Env}_E[x^R \cup I, \emptyset](S)$ \text{(Def)}$

QED
- Case $\text{Env}_{\lambda}(D, I)(S) S$ is trivial
- Case $\text{Env}_{\lambda}(I, I)(S) S$

$x_D \in \text{Env}_{\lambda}(I, I)(S) \iff \text{(Def)}$

$\exists S' \in IS^{[I]}(S) \cup S^\bullet, x_D \in \text{Env}_{\lambda}(I, I)(S) \cup S'(S) \iff \text{(IH on } #S)$

$\exists S' \in IS^{[I]}(S) \cup S^\bullet, \exists p, p \cdot D(x_D) \in P_{\lambda, i-1, r}\{\}, \{\} \cup S(S')$

We split the equivalence to be proved:

$(\Rightarrow)$ By case on $S'$ source

- if $S' \in IS^{[I]}(S)$ by IH on $\text{Env}_{\lambda} > IS$ we have:

$\exists y^k, \exists N(l, y^k, S') : S \rightarrow S'$ and then trivially that $N(l, y^k, S') \cdot p \cdot D(x_D) \in P_{\lambda, i-1, r}\{\}, \{\} \cup S(S)$.

- if $S' \in S^\bullet$ we have:

$\vdash \exists p \cdot D(x_D) \in P_{\lambda, i-1, r}\{\}, \{\} \cup S(S')$

and then trivially that $E(l, S') \cdot p \cdot D(x_D) \in P_{\lambda, i-1, r}\{\}, \{\} \cup S(S)$.

$(\Leftarrow)$ If $s \cdot p \cdot D(x_D) \in P_{\lambda, i-1, r}\{\}, \{\} \cup S(S)$ then first, $\exists S', p \cdot D(x_D) \in P_{\lambda, i-1, r}\{\}, \{\} \cup S(S)$ and $(\ast) \vdash s : S \rightarrow S'$.

By case on $s$:

- if $s = E(l, S')$ then by inversion on $(\ast)$: $S' \in S^\bullet$ which terminates the proof.

- if $s = N(l, y^k, S')$ then by $(\ast)$ we have $S' \in P_{\lambda, i-1, r}\{\}, \{\} \cup S(S)$ and by IH (with $\text{Env}_{\lambda} > IS$) $S' \in IS^{[I]}(S)$.

QED

- Case $\text{Env}_{\lambda}(I, I)(S)$

$x_D \in \text{Env}_{\lambda}(I, I)(S)$ We split the equivalence to be proved:

$(\Rightarrow)$ By case on $x_D$ source:

- if $\exists l \in \text{Max}(L), x_D \in \text{Env}_{\lambda}(l < L)\{\}, \{\} \cup S(S)$ then by induction on $\#L$:

$\exists p, p \cdot D(x_D) \in \text{Env}(l \neq L)\{\}, \{\} \cup S(S)$

and thus $p \cdot D(x_D) \in \text{Env}(l \neq L)\{\}, \{\} \cup S(S)$.

Assume $p \cdot D(x_D)$ is not minimal, let $l_1$ be such that $p \cdot D(x_D) \in \text{Env}(l_1 \neq L)\{\}, \{\} \cup S(S)$, then there is $l_2$ and $p_2 \in \text{Env}(l_2 \neq L)\{\}, \{\} \cup S(S)$ such that $Name(p_2) = x$ and $p_2 < p \cdot D(x_D)$ and $(\ast) l_2 \neq l_1$.

But since $l_1 \neq l_2$ and $p_2 < p \cdot D(x_D)$, we have to have: $l_2 < l_1$ (the order is the lexicographic order), and thus $l_2 < l_1 < l$ which contracts $(\ast)$.

- if $\exists l \in \text{Max}(L)$ such that (1) $\forall y \neq x$ and $x_D \in \text{Env}_{\lambda}(l \neq L)\{\}, \{\} \cup S(S)$ then:

By IH (\text{Env} > IS): $\exists p, p \cdot D(x_D) \in \text{Env}(l \neq L)\{\}, \{\} \cup S(S)$.

Assume $p \cdot D(x_D) \in \text{Env}(l \neq L)\{\}, \{\} \cup S(S)$ then there is a path $p'$ and $l'$ such that $Name(p') = x$ and $p' \in \text{Env}(l' \neq L)\{\}, \{\} \cup S(S)$ and $p' < p$.

- if $l' = l$ then we have $tail(p') < tail(p)$ but they both are in $\text{Env}(l \neq L)\{\}, \{\} \cup S(S)$ which is a contradiction.

- else we have $l' < l$, thus $(\ast) \exists l' \neq l, p \in \text{Env}(l' \neq L)\{\}, \{\} \cup S(S)$ and $Name(p) = x$ is not empty and has a minimal element. Which contradicts (1).

$(\Leftarrow)$ Let $x_D \in \Delta(P_{\lambda, i-1, r}\{\}, \{\})$ then:

$\exists p, p \cdot D(x_D) \in \text{Env}(l \neq L)\{\}, \{\} \cup S(S)$

Let $l_1$ be such that $p \cdot D(x_D) \in P_{\lambda, i-1, r}\{\}, \{\} \cup S(S)$:

- if $l_1 \in \text{Max}(L)$ then $\forall l' < l_1, \forall p' \in \text{Env}(l' \neq L)\{\}, \{\} \cup S(S), Name(p') \neq x \wedge p' < p \cdot D(x_D)$ thus $\forall p' \in \text{Env}(l' \neq L)\{\}, \{\} \cup S(S), Name(p') \neq x$ and by IH (on size $L$), $\forall y \in \text{Env}(l' \neq L)\{\}, \{\} \cup S(S), y \neq x$ and we have $x_D \in \text{Env}(l \neq L)\{\}, \{\} \cup S(S)$.

- if $l_1 < l_2 \in \text{Max}(L)$, then $p \cdot D(x_D) \in \text{Env}(l_2 \neq L)\{\}, \{\} \cup S(S)$ and by IH, $p \cdot D(x_D) \in \text{Env}(l_2 \neq L)\{\}, \{\} \cup S(S)$ which terminates the proof.

QED

Figure 16. Proof of Lemma 1, Pt. 2
We have:

1. \( \vdash x^R \rightarrow x^D \) by correctness of the name resolution algorithm \( R^g() \).
2. \( \vdash \sigma \bigwedge C, G, \psi \rightarrow [t \rightarrow S](C, G, \psi) \)

Assume there is \( \sigma \) such that

\[ \sigma \bigwedge C, G, \psi \models \sigma \bigwedge C \] (H)

then we want to prove:

\[ \sigma \bigwedge C, G, \psi \models \sigma \bigwedge C \]

We have:

1. \( DSc(x^D) = S \) by the rewriting rule condition
2. \( \sigma \bigwedge C, G, \psi \models \sigma \bigwedge x^D \rightarrow \bot \)
3. \( \sigma \bigwedge C, G, \psi \models \sigma \bigwedge C \) using H
4. we conclude by C-AND rule of the constraint interpretation with 2. and 4.

- S-EQUAL Assume:

\( (T_1 \equiv T_2 \land C, G, \psi) \rightarrow \sigma'(C, G, \psi) \)

where \( \sigma' = \mu(T_1, T_2) \).

Assume there is \( \sigma \) such that

\[ \sigma \bigwedge C, G, \psi \models \sigma \bigwedge C \] (H)

then we want to prove:

\[ \sigma \bigwedge C, G, \psi \models \sigma \bigwedge C \]

We have:

1. \( \sigma T_1 = \sigma T_2 \) by unification property
2. \( \sigma \bigwedge C, G, \psi \models \sigma T_1 \equiv T_2 \) by C-EQUAL rule and 1.
3. \( \sigma \bigwedge C, G, \psi \models \sigma \bigwedge C \) using H
4. we conclude by C-AND rule of the constraint interpretation with 2. and 4.

- S-UNIQUE Assume:

\( (\bigwedge E \land C, G, \psi) \rightarrow (C, G, \psi) \)

Assume there is \( \sigma \) such that

\[ \sigma \bigwedge C, G, \psi \models \sigma \bigwedge C \] (H)
then we want to prove:
\[ \sigma(G, \psi)^M \models \sigma(E \land TC) \]

We have:
1. \( N_G(E) = \llbracket E \rrbracket_{\sigma G} \) by Lemma 3
2. \( \forall x \in N_G(E), 1_{N_G(E)}(x) \) \( \approx \) \( 1 \) by reduction rule hypothesis
3. we conclude by C-AND rule of the constraint interpretation with 1. and 2.

**Proof of Lemma 4** Using this result \( \dagger \) we can prove Lemma 4 by a simple induction on the number of reduction steps.

\[ S-T \]

Assume:
\( (E_1 \subseteq E_2 \land C, G, \psi) \rightarrow (C, G, \psi) \)
Assume there is \( \sigma \) such that:
\[ \sigma(G, \psi)^M \models \sigma(C) \] \hspace{1cm} (H)
then we have:
1. \( \sigma(G, \psi)^M \models \sigma(\text{True}) \) by C-True rule
2. we conclude by C-AND rule of the constraint interpretation with 1. and H.

\[ S-\text{DECLTypeFirst} \]
Assume:
\( (x^D : T \land C, G, \psi) \rightarrow (C, G, \{ x^D \rightarrow T \} \cup \psi) \)
Assume there is \( \sigma \) such that
\[ \sigma(G, \{ x^D \rightarrow T \} \cup \psi)^M \models \sigma(C) \] \hspace{1cm} (H)
then we want to prove:
\[ \sigma(G, \{ x^D \rightarrow T \} \cup \psi)^M \models \sigma(x^D : T \land C) \]
We have:
1. \( \sigma(G, \{ x^D \rightarrow T \} \cup \psi)^M \models \sigma(x^D : T) \) by C-TypeOf semantics rule
2. we conclude by C-AND rule of the constraint interpretation with 1. and H

\[ S-\text{DECLTypeNext} \]
Assume:
\( (x^D : T \land C, G, \psi) \rightarrow (\psi(x^D) \equiv T \land C, G, \psi) \)
Assume there is \( \sigma \) such that
\[ \sigma(G, \psi)^M \models \sigma(\psi(x^D) \equiv T \land C) \] \hspace{1cm} (H)
then we want to prove:
\[ \sigma(G, \psi)^M \models \sigma_1(x^D : T \land C) \]
We have:
1. \( \sigma(\psi(x^D)) = \sigma(T) \) by inversion of C-AND and C-Equal semantics rules
2. \( \sigma(G, \psi)^M \models \sigma(x^D : T) \) by C-TypeOf rule
3. \( \sigma(G, \psi)^M \models \sigma(C) \) using H
4. we conclude by C-AND rule of the constraint interpretation with 2. and 3.