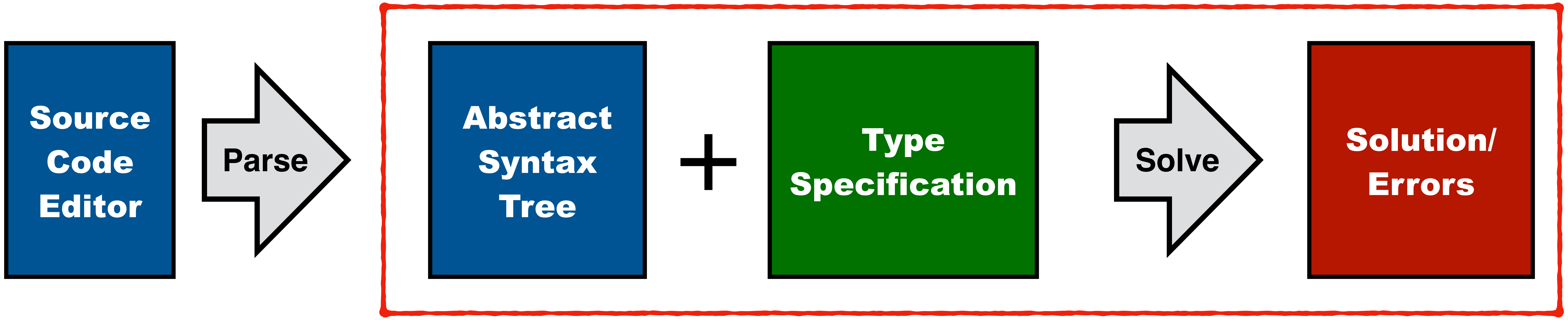
Constraint Semantics and Constraint Resolution

Hendrik van Antwerpen
Eelco Visser

TU Delft

CS4200 | Compiler Construction | September 30, 2021

This lecture



- Type checking with type specifications
- Semantics of a type specification
- Type checking algorithms
- Constraint solving for type specifications
- Term equality and unification

Reading Material

The following papers add background, conceptual exposition, and examples to the material from the slides. Some notation and technical details have been changed; check the documentation.

This paper introduces the Statix DSL for definition of type systems.

Shows how to use scope graphs for structural type and generic types

Explains the need for scheduling in type checkers

OOPSLA 2018

https://doi.org/10.1145/3276484

Scopes as Types

HENDRIK VAN ANTWERPEN, Delft University of Technology, Netherlands
CASPER BACH POULSEN, Delft University of Technology, Netherlands
ARJEN ROUVOET, Delft University of Technology, Netherlands
EELCO VISSER, Delft University of Technology, Netherlands

Scope graphs are a promising generic framework to model the binding structures of programming languages, bridging formalization and implementation, supporting the definition of type checkers and the automation of type safety proofs. However, previous work on scope graphs has been limited to simple, nominal type systems. In this paper, we show that viewing *scopes as types* enables us to model the internal structure of types in a range of non-simple type systems (including structural records and generic classes) using the generic representation of scopes. Further, we show that relations between such types can be expressed in terms of generalized scope graph queries. We extend scope graphs with scoped relations and queries. We introduce Statix, a new domain-specific meta-language for the specification of static semantics, based on scope graphs and constraints. We evaluate the scopes as types approach and the Statix design in case studies of the simply-typed lambda calculus with records, System F, and Featherweight Generic Java.

CCS Concepts: • **Software and its engineering** → **Semantics**; **Domain specific languages**;

Additional Key Words and Phrases: static semantics, type system, type checker, name resolution, scope graphs, domain-specific language

ACM Reference Format:
Hendrik van Antwerpen, Casper Bach Poulsen, Arjen Rouvoet, and Eelco Visser. 2018. Scopes as Types. *Proc. ACM Program. Lang.* 2, OOPSLA, Article 114 (November 2018), 30 pages. https://doi.org/10.1145/3276484

1 INTRODUCTION

The goal of our work is to support high-level specification of type systems that can be used for multiple purposes, including reasoning (about type safety among other things) and the implementation of type checkers [Visser et al. 2014]. Traditional approaches to type system specification do not reflect the commonality underlying the name binding mechanisms for different languages. Furthermore, operationalizing name binding in a type checker requires carefully staging the traversals of the abstract syntax tree in order to collect information before it is needed. In this paper, we introduce an approach to the declarative specification of type systems that is close in abstraction to traditional type system specifications, but can be directly interpreted as type checking rules. The approach is based on scope graphs for name resolution, and constraints to separate traversal order from solving order.

Authors' addresses: Hendrik van Antwerpen, Delft University of Technology, Delft, Netherlands, H.vanAntwerpen@tudelft.nl; Casper Bach Poulsen, Delft University of Technology, Delft, Netherlands, C.B.Poulsen@tudelft.nl; Arjen Rouvoet, Delft University of Technology, Delft, Netherlands, A.J.Rouvoet@tudelft.nl; Eelco Visser, Delft University of Technology, Delft, Netherlands, E.Visser@tudelft.nl.

2475-1421/2018/11-ART114
https://doi.org/10.1145/3276484

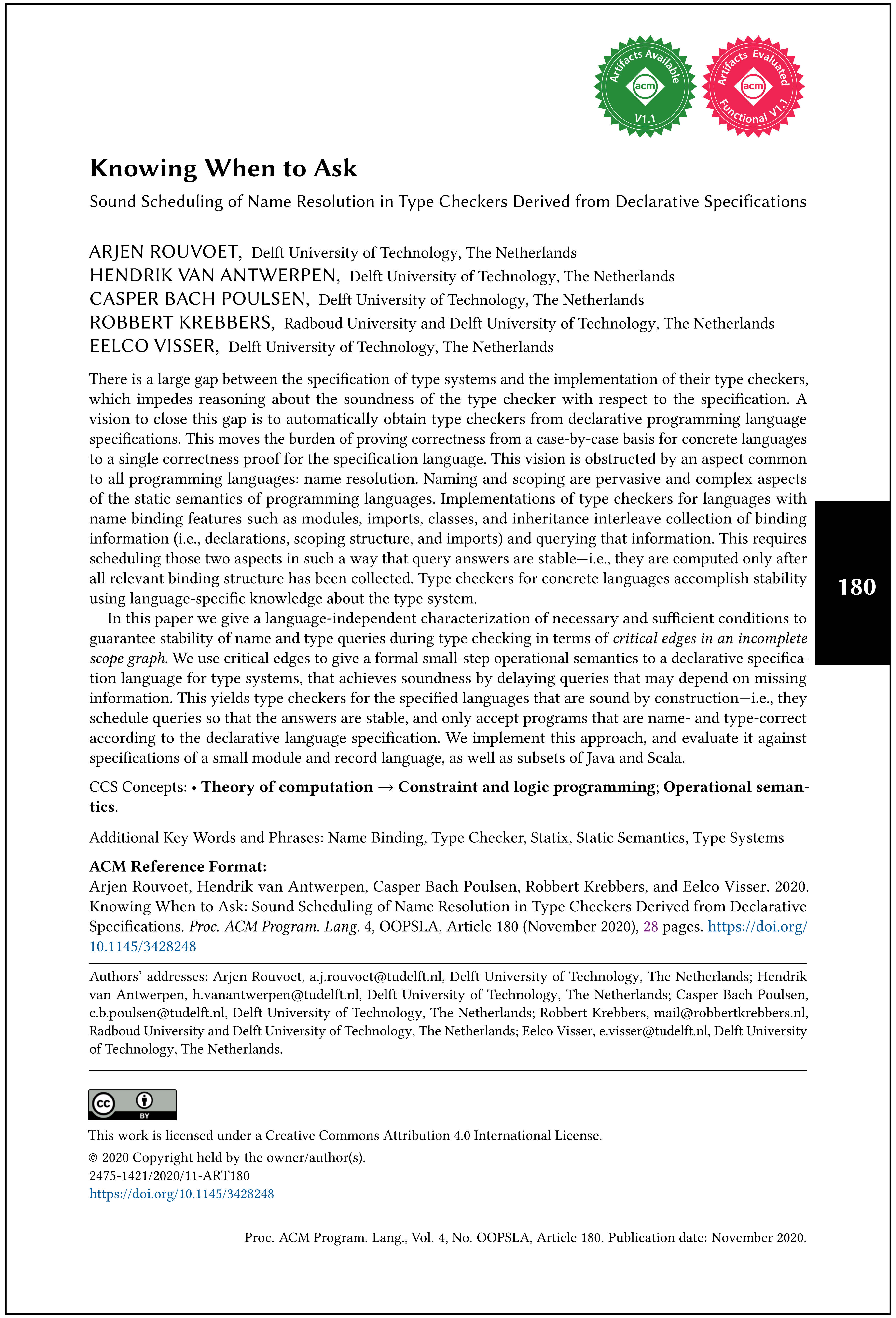
Formalizes the declarative and operational semantics of Statix Core

Introduces concept of critical edges to determine whether a query can be executed

Extends the type system of Statix with ownership in order to statically guarantee that critical edges can be computed

OOPSLA 2020

https://doi.org/10.1145/3428248



Knowing When to Ask

Sound Scheduling of Name Resolution in Type Checkers Derived from Declarative Specifications

ARJEN ROUVOET, Delft University of Technology, The Netherlands
HENDRIK VAN ANTWERPEN, Delft University of Technology, The Netherlands
CASPER BACH POULSEN, Delft University of Technology, The Netherlands
ROBBERT KREBBERS, Radboud University and Delft University of Technology, The Netherlands
EELCO VISSER, Delft University of Technology, The Netherlands

There is a large gap between the specification of type systems and the implementation of their type checkers, which impedes reasoning about the soundness of the type checker with respect to the specification. A vision to close this gap is to automatically obtain type checkers from declarative programming language specifications. This moves the burden of proving correctness from a case-by-case basis for concrete languages to a single correctness proof for the specification language. This vision is obstructed by an aspect common to all programming languages: name resolution. Naming and scoping are pervasive and complex aspects of the static semantics of programming languages. Implementations of type checkers for languages with name binding features such as modules, imports, classes, and inheritance interleave collection of binding information (i.e., declarations, scoping structure, and imports) and querying that information. This requires scheduling those two aspects in such a way that query answers are stable—i.e., they are computed only after all relevant binding structure has been collected. Type checkers for concrete languages accomplish stability using language-specific knowledge about the type system.

In this paper we give a language-independent characterization of necessary and sufficient conditions to guarantee stability of name and type queries during type checking in terms of *critical edges in an incomplete scope graph*. We use critical edges to give a formal small-step operational semantics to a declarative specification language for type systems, that achieves soundness by delaying queries that may depend on missing information. This yields type checkers for the specified languages that are sound by construction—i.e., they schedule queries so that the answers are stable, and only accept programs that are name- and type-correct according to the declarative language specification. We implement this approach, and evaluate it against specifications of a small module and record language, as well as subsets of Java and Scala.

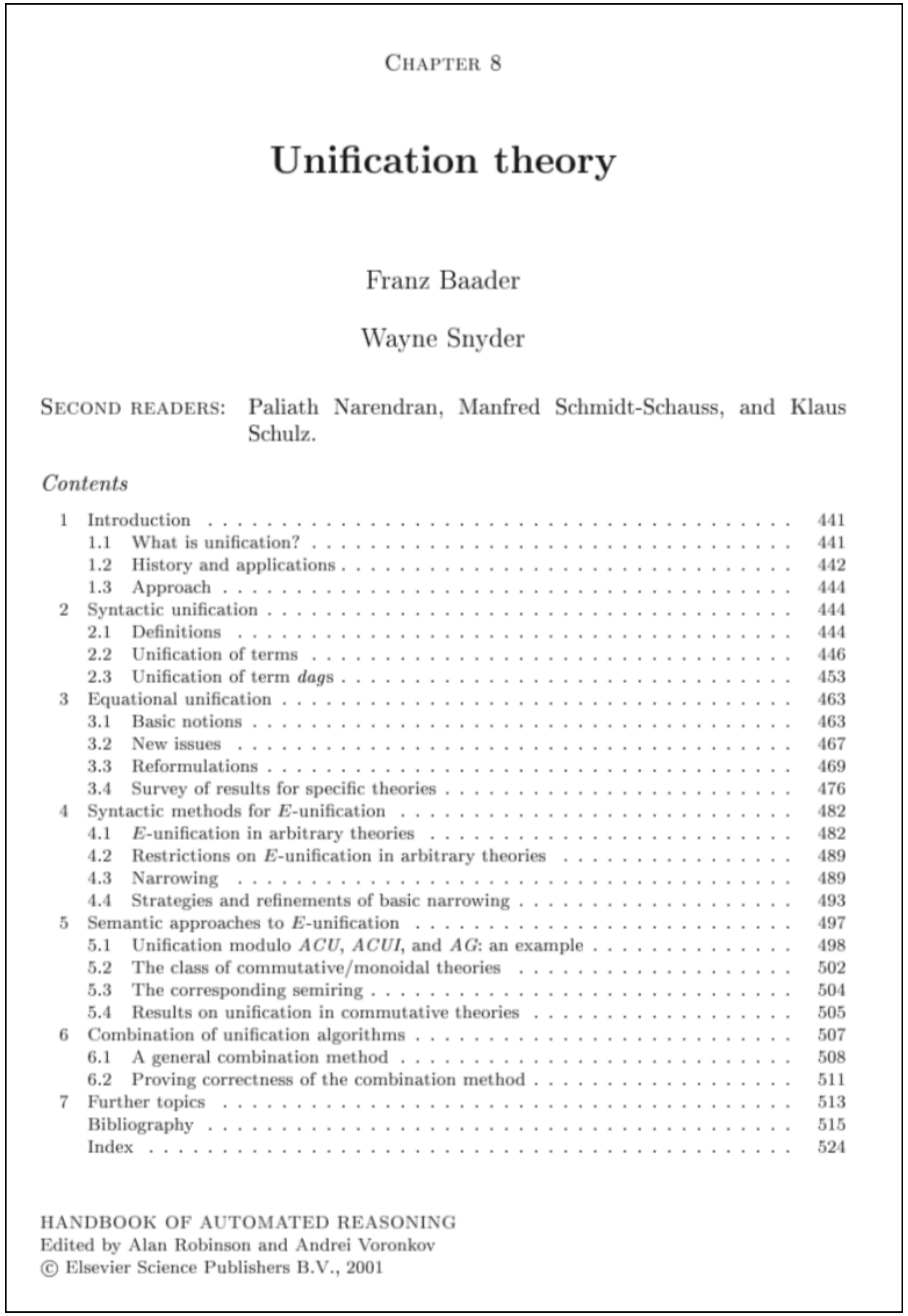
CCS Concepts: • **Theory of computation → Constraint and logic programming**; **Operational semantics**.

Additional Key Words and Phrases: Name Binding, Type Checker, Statix, Static Semantics, Type Systems

ACM Reference Format:
Arjen Rouvoet, Hendrik van Antwerpen, Casper Bach Poulsen, Robbert Krebbers, and Eelco Visser. 2020. Knowing When to Ask: Sound Scheduling of Name Resolution in Type Checkers Derived from Declarative Specifications. *Proc. ACM Program. Lang.* 4, OOPSLA, Article 180 (November 2020), 28 pages. https://doi.org/10.1145/3428248

Authors' addresses: Arjen Rouvoet, a.j.rouvoet@tudelft.nl, Delft University of Technology, The Netherlands; Hendrik van Antwerpen, h.vanantwerpen@tudelft.nl, Delft University of Technology, The Netherlands; Casper Bach Poulsen, c.b.poulsen@tudelft.nl, Delft University of Technology, The Netherlands; Robbert Krebbers, mail@robbertkrebbers.nl, Radboud University and Delft University of Technology, The Netherlands; Eelco Visser, e.visser@tudelft.nl, Delft University of Technology, The Netherlands.

Good introduction to unification, which is the basis of many type inference approaches, constraint languages, and logic programming languages. Read sections 1, and 2.



CHAPTER 8

Unification theory

Franz Baader

Wayne Snyder

SECOND READERS: Paliath Narendran, Manfred Schmidt-Schauss, and Klaus Schulz.

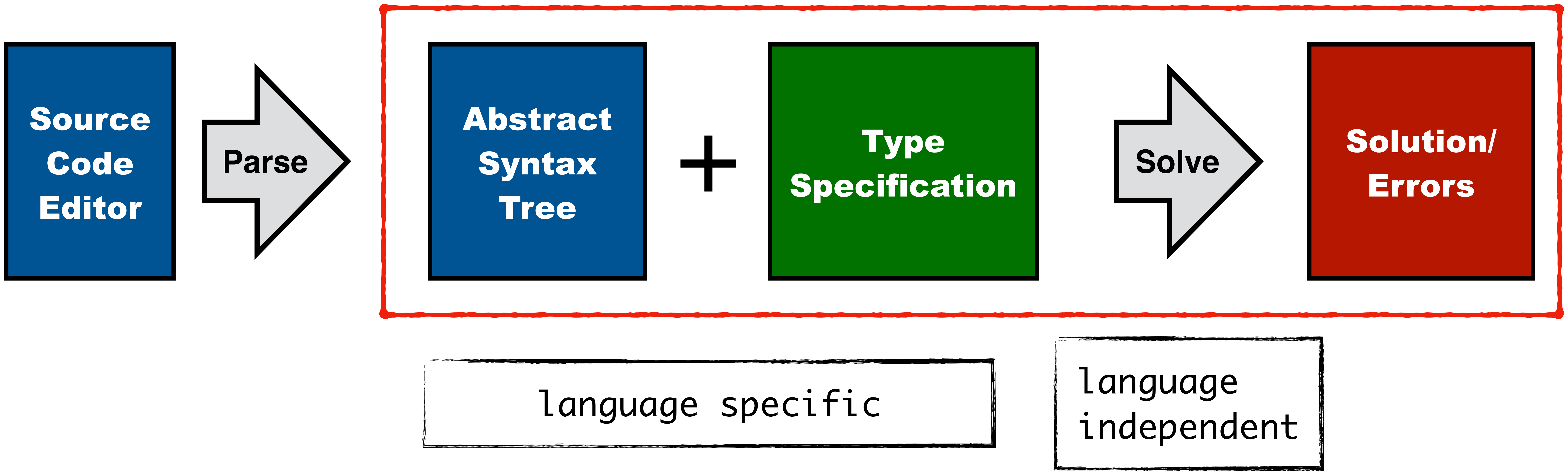
Contents

HANDBOOK OF AUTOMATED REASONING
Edited by Alan Robinson and Andrei Voronkov
© Elsevier Science Publishers B.V., 2001

Baader et al. “Chapter 8 - Unification Theory.” In Handbook of Automated Reasoning, 445–533. Amsterdam: North-Holland, 2001.

https://www.cs.bu.edu/~snyder/publications/UnifChapter.pdf

Type Checking with Specifications


Source Code Editor
Parse
Abstract Syntax Tree
+
Type Specification
Solve
Solution/ Errors
language specific
language independent

Typing Rules

What are typing rules?

- Predicates that specify constraints (rule premises) on their arguments (the program)
- Syntax-directed, match on program constructs (at least in Statix)
- Specification of what it means to be well-typed!

What are the premises?

- Logical assertions that should hold for well-typed programs
- Specification language determines what assertions can be made
  - Type equality and inequality, name resolution, ...
- Determines the expressiveness of the specification!

Solving

- Given an initial predicate that must hold, ...
- find an assignment for all logical variables, such that the predicate is satisfied

Typing Checking

Challenges for type checker implementations?

- Collecting (non-lexical) binding information before use
- Dealing with unknown (type) values

Separation of what from how

- Typing rules says what is a well-typed program
- Solver says how to determine that a program is well-typed

Separation of computation from program structure

- Typing rules follow the structure of the program
- Solver is flexible in order of resolution

Approach: reusable solver for the specification language

- Support logical variables for unknowns and infer their values
- Automatically determine correct resolution order

Constraint Semantics

What gives constraints meaning?

```
ty == FUN(ty1,ty2)
Var{x} in s |-> d
ty1 == INT()
```

What is the meaning of constraints?

- What is a valid solution?
- Or: in which models are the constraints satisfied?
- Can we describe this independent of an algorithm to find a solution?

When are constraints satisfied?

- Formally described by the declarative semantics
- Written as $G,\phi \vDash C$
- Satisfied in a model
  - Substitution ϕ (read: phi)
  - Scope graph G
- Describes for every type of constraint when it is satisfied

Semantics of (a Subset of) Statix Constraints

Syntax

```
C = t == t            // equality
  | r in s |-> d      // name resolution (short for query var … in s |-> [d])
  | C /\ C            // conjunction
```

Declarative semantics

```
G,ϕ ⊨ t == u                 if ϕ(t) = ϕ(u)

G,ϕ ⊨ r in s |-> d           if  ϕ(r) = x
                             and ϕ(d) = x
                             and ϕ(s) = #i
                             and x resolves to x from #i in G

G,ϕ ⊨ C1 /\ C2               if G,ϕ ⊨ C1 and G,ϕ ⊨ C2
```

Using the Semantics

Program

```
let
  function f₁(i₂ : int) : int =
    i₃ + 1
in
  f₄(14)
end
```

Program constraints

```
ty1 == INT()
INT() == INT()
"i" in #s1 |-> d1
ty2 == INT()
"f" in #s0 |-> d2
ty3 == FUN(ty4,ty5)
ty4 == INT()
…
```

Unifier ϕ (model)

```
ϕ = { ty1 -> INT(),
      ty2 -> INT(),
      ty3 -> FUN(INT(),ty5),
      ty4 -> INT(),
      d1  -> "i",
      d2  -> "f"
    }
```

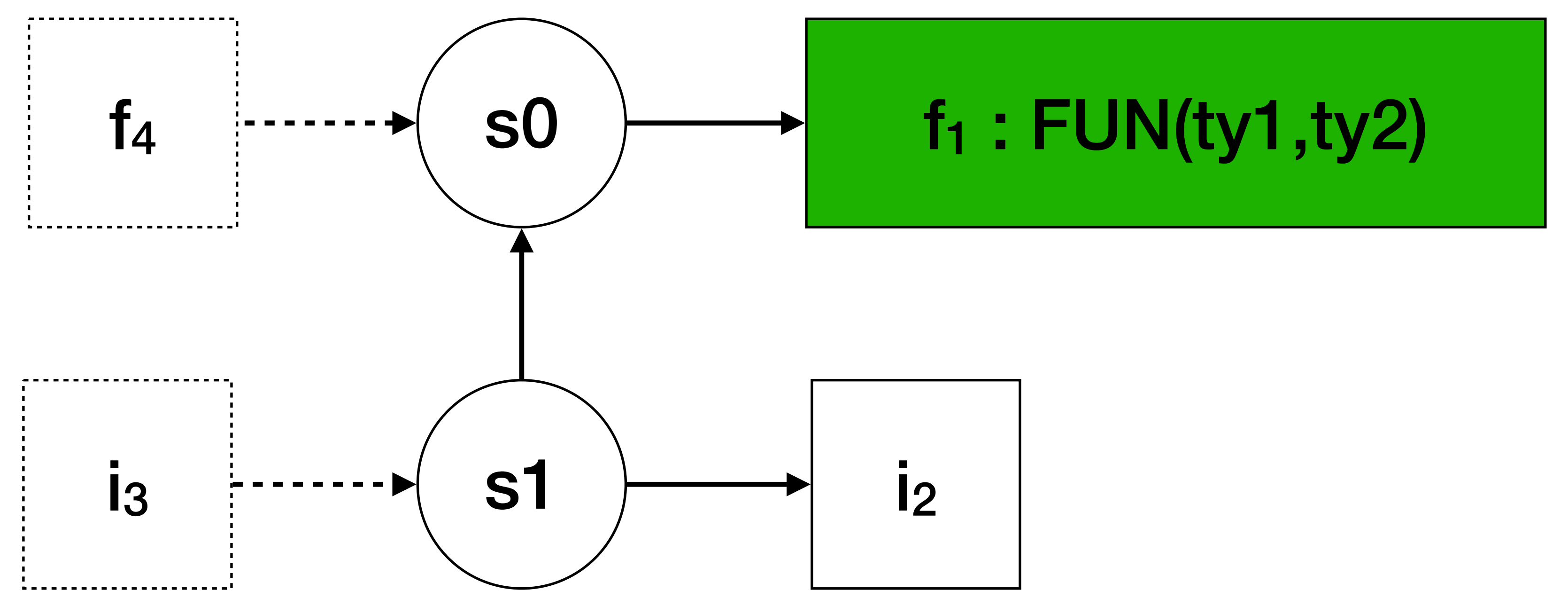
Constraint semantics

```
G,ϕ ⊨ t == u
    if ϕ(t) = ϕ(u)

G,ϕ ⊨ r in s |-> d
    if  ϕ(r) = x
    and ϕ(d) = x
    and ϕ(s) = #i
    and x resolves to x from #i in G

G,ϕ ⊨ C₁ /\ C₂
    if  G,ϕ ⊨ C₁
    and G,ϕ ⊨ C₂
```

Scope graph G (model)



Different Kinds of Variables

Program

```
let
  function f₁(i₂ : int) : int =
    i₃ + 1
in
  f₄(14)
end
```

Program constraints

```
ty1 == INT()
INT() == INT()
"i" in #s1 |-> d1
ty2 == INT()
"f" in #s0 |-> d2
ty3 == FUN(ty4,ty5)
ty4 == INT()
…
```

Unifier ϕ (model)

```
ϕ = { ty1 -> INT(),
      ty2 -> INT(),
      ty3 -> FUN(INT(),ty5),
      ty4 -> INT(),
      d1  -> "i",
      d2  -> "f"
    }
```

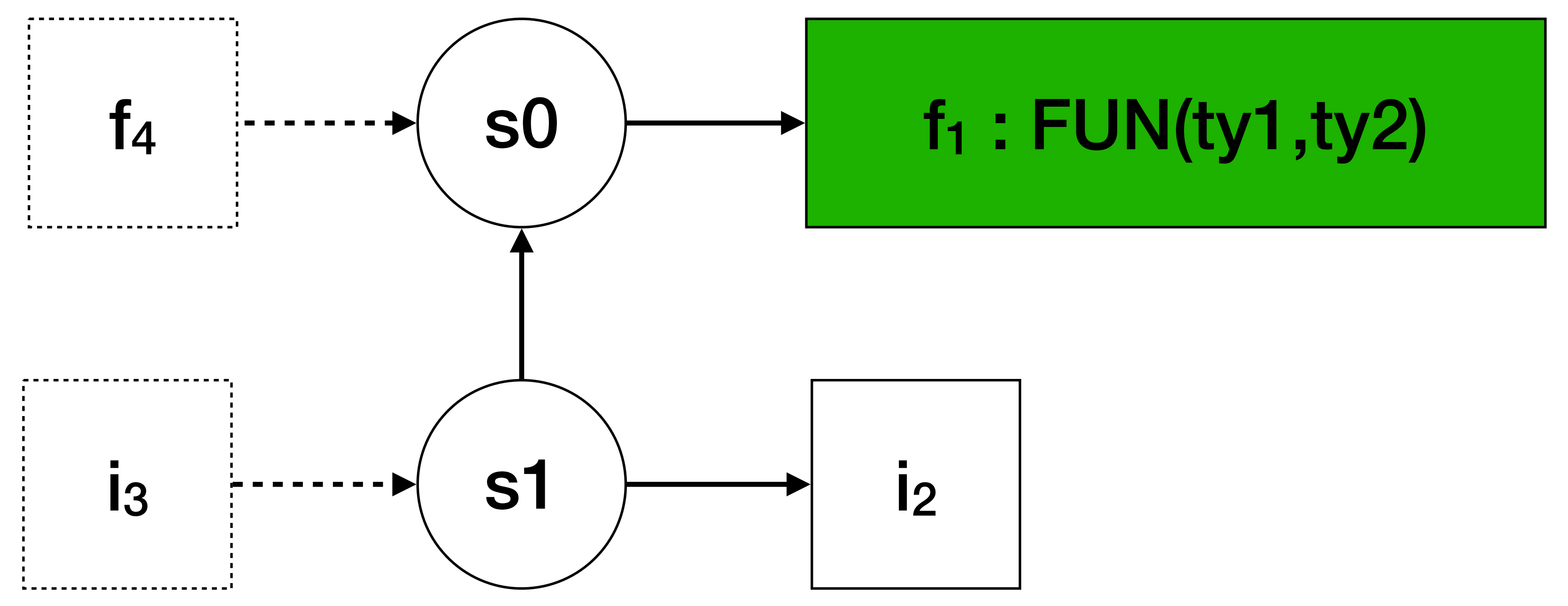
Constraint semantics

```
G,ϕ ⊨ t == u
    if ϕ(t) = ϕ(u)

G,ϕ ⊨ r in s |-> d
    if  ϕ(r) = x
    and ϕ(d) = x
    and ϕ(s) = #i
    and x resolves to x from #i in G

G,ϕ ⊨ C₁ /\ C₂
    if  G,ϕ ⊨ C₁
    and G,ϕ ⊨ C₂
```

Scope graph G (model)



Different Kinds of Variables

Program

```
let
  function f1(i2 : int) : int =
    i3 + 1
in
  f4(14)
end
```

Program constraints

```
ty1 == INT()
INT() == INT()
"i" in #s1 |-> d1
ty2 == INT()
"f" in #s0 |-> d2
ty3 == FUN(ty4,ty5)
ty4 == INT()
```

Unifier ϕ (model)

```
ϕ = { ty1 -> INT(),
      ty2 -> INT(),
      ty3 -> FUN(INT(),ty5),
      ty4 -> INT(),
      d1  -> "i",
      d2  -> "f"
    }
```

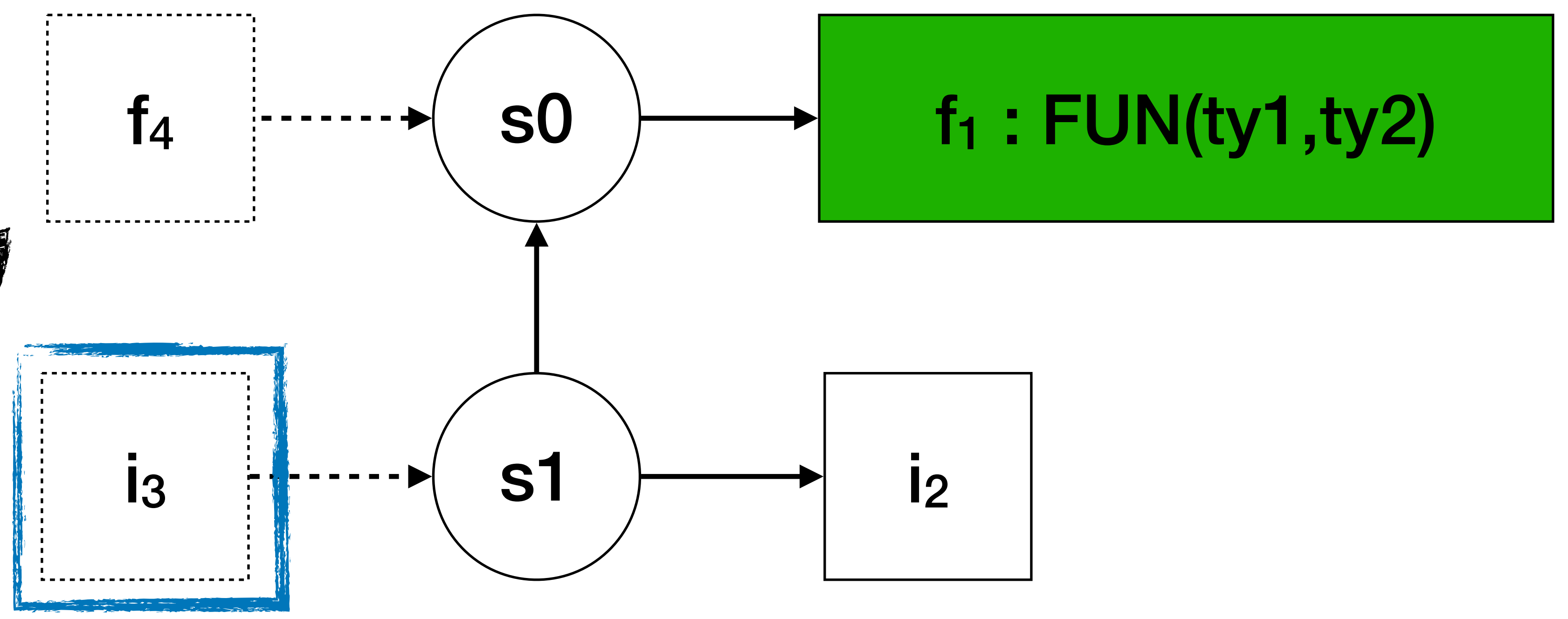
Constraint semantics

```
G,ϕ ⊨ t == u
    if ϕ(t) = ϕ(u)

G,ϕ ⊨ r in s |-> d
    if  ϕ(r) = x
    and ϕ(d) = x
    and ϕ(s) = #i
    and x resolves to x from #i in G

G,ϕ ⊨ C1 /\ C2
    if  G,ϕ ⊨ C1
    and G,ϕ ⊨ C2
```

Object language variables



Different Kinds of Variables

Program

```
let
  function f₁(i₂ : int) : int =
    i₃ + 1
in
  f₄(14)
end
```

Program constraints

```
ty1 == INT()
INT() == INT()
"i" in #s1 |-> d1
ty2 == INT()
"f" in #s0 |-> d2
ty3 == FUN(ty4,ty5)
ty4 == INT()
…
```

Unifier ϕ (model)

```
ϕ = { ty1 -> INT(),
      ty2 -> INT(),
      ty3 -> FUN(INT(),ty5),
      ty4 -> INT(),
      d1  -> "i",
      d2  -> "f"
    }
```

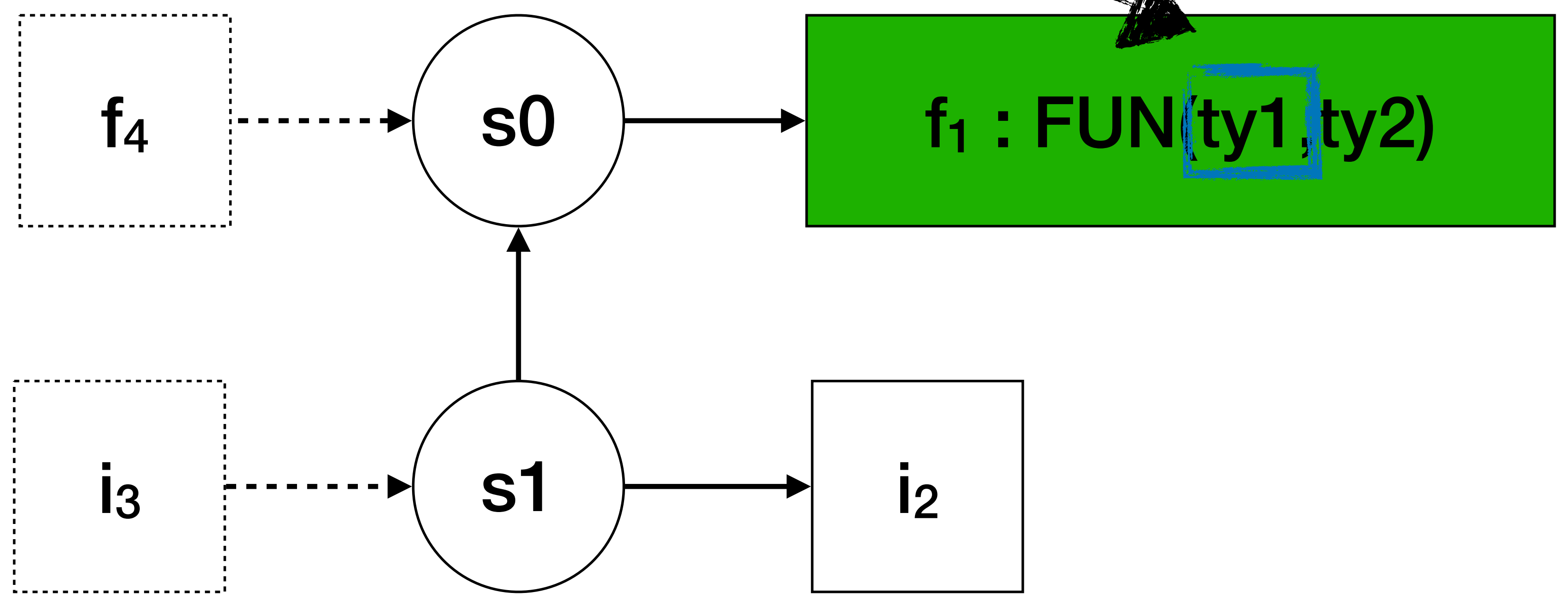
Constraint semantics

```
G,ϕ ⊨ t == u
    if ϕ(t) = ϕ(u)

G,ϕ ⊨ r in s |-> d
    if  ϕ(r) = x
    and ϕ(d) = x
    and ϕ(s) = #i
    and x resolves to x from #i in G

G,ϕ ⊨ C₁ /\ C₂
    if  G,ϕ ⊨ C₁
    and G,ϕ ⊨ C₂
```

Constraint / logic variables



Different Kinds of Variables

Program

```
let
  function f₁(i₂ : int) : int =
    i₃ + 1
in
  f₄(14)
end
```

Program constraints

```
ty1 == INT()
INT() == INT()
"i" in #s1 |-> d1
ty2 == INT()
"f" in #s0 |-> d2
ty3 == FUN(ty4,ty5)
ty4 == INT()
…
```

Unifier ϕ (model)

```
ϕ = { ty1 -> INT(),
      ty2 -> INT(),
      ty3 -> FUN(INT(),ty5),
      ty4 -> INT(),
      d1  -> "i",
      d2  -> "f"
    }
```

Semantics meta-variables

Constraint semantics

$G,\phi \vDash t == \boxed{u}$

  if $\phi(t) = \phi(u)$

$G,\phi \vDash r \text{ in } s \;|\!\!\to d$

  if $\phi(r) = \boxed{x}$

  and $\phi(d) = x$

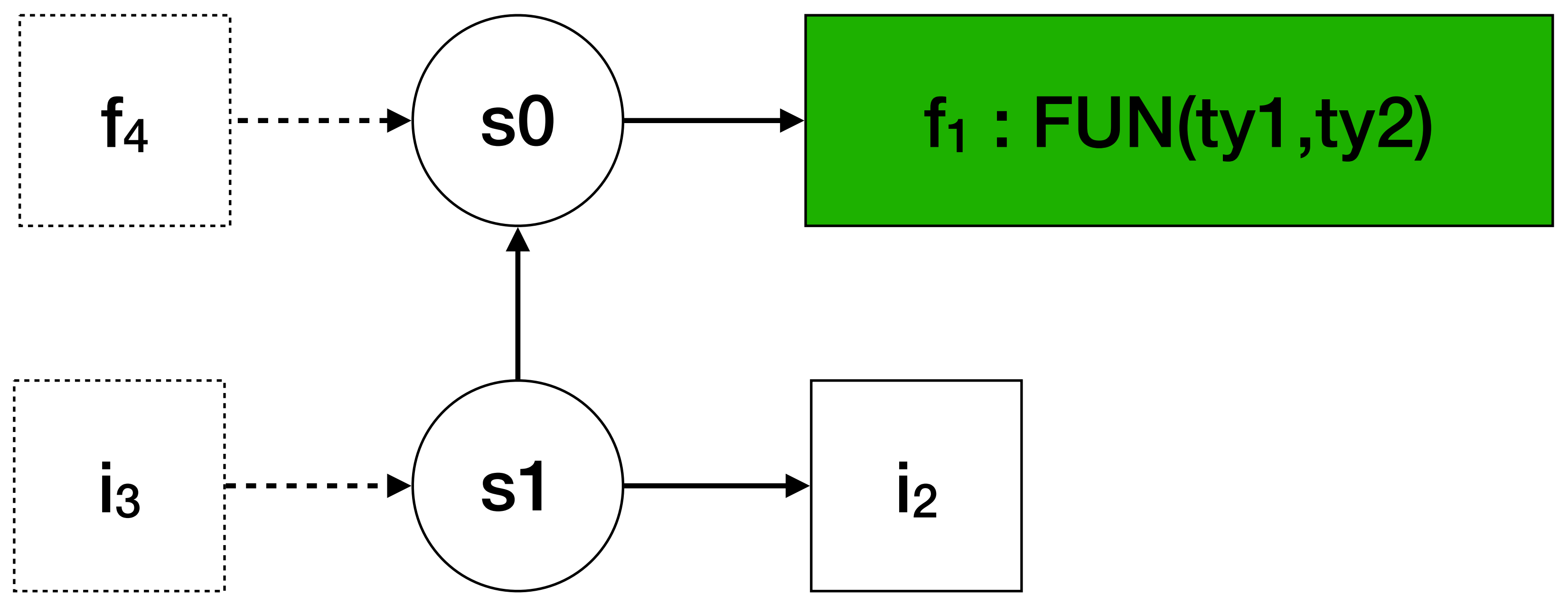
  and $\phi(s) = \#i$

  and x resolves to x from $\boxed{\#i}$ in G

$G,\phi \vDash C_1 \;/\backslash\; C_2$

  if $G,\phi \vDash C_1$

  and $G,\phi \vDash C_2$



Type Checking

How to check types?

What should a type checker do?

- Check that a program is well-typed!
- Resolve names, and check or compute types
- Report useful error messages
- Provide a representation of name and type information
    - Type annotated AST

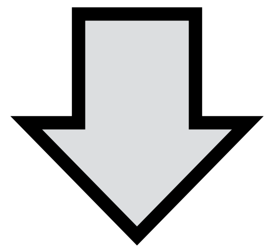
This information is used for

- Next compiler steps (optimization, code generation, …)
- IDE (error reporting, code completion, refactoring, …)
- Other tools (API documentation, …)

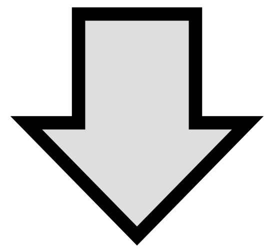
How are type checkers implemented?

Computing Type of Expression (recap)

```
function (a : int) = a + 1
```



```
Fun("a", INT(),
    Plus(Var("a"), Int(1)))
```



```
FUN(INT(), INT())
```

```
typeOfExp(s, Int(_)) = INT().

typeOfExp(s, Plus(e1, e2)) = INT() :-
  typeOfExp(s, e1) == INT(),
  typeOfExp(s, e2) == INT().

typeOfExp(s, Fun(x, te, e)) = FUN(S, T) :- {s_fun}
  typeOfTypeExp(s, te) == S,
  new s_fun, s_fun -P-> s,
  s_fun -> Var{x} with typeOfDecl S,
  typeOfExp(s_fun, e) == T.

typeOfExp(s, Var(x)) = T :-
  typeOfDecl of Var{x} in s |-> [(_, (_, T))].
```

- Can be executed top down, in premise order
- Could be written almost like this in a functional language

Inferring the Type of a Parameter

```
function (a ) = a + 1
```

```
Fun("a", 
     Plus(Var("a"), Int(1)))
```

```
FUN(INT(), INT())
```

Unknown S!

```
typeOfExp(s, Int(_)) = INT().

typeOfExp(s, Plus(e1, e2)) = INT() :-
  typeOfExp(s, e1) == INT(),
  typeOfExp(s, e2) == INT().

typeOfExp(s, Fun(x,    e)) = FUN(S, T) :- {s_fun}

  new s_fun, s_fun -P-> s,
  s_fun -> Var{x} with typeOfDecl S,
  typeOfExp(s_fun, e) == T.

typeOfExp(s, Var(x)) = T :-
  typeOfDecl of Var{x} in s |-> [(_, (_, T))].
```

- What are the consequences for our typing rules?
- Types are not known from the start, but learned gradually
- A simple top-down traversal is insufficient

Checking classes

```
class A {
    B m() {
        return new C();
    }
}

class B {
    int i;
}

class C extends B {
   int m(A a) {
        return a.m().i;
    }
}
```

How can we type check this program?

- Is there a possible single traversal strategy here?
- Why are the type annotations not enough?
- What strategy could be used?

Two-pass approach

- The first pass builds a class table
- The second pass checks expressions using the class table

Question

- Does this still work if we introduce nested classes?

Variables and Constraints

```
function (a         ) = a + 1
```

```
Fun("a",
    Plus(Var("a"), Int(1)))
```

```
FUN(?S, INT()) + ?S == INT()
```

```
?S := INT()
```

```
typeOfExp(s, Int(_)) = INT().

typeOfExp(s, Plus(e1, e2)) = INT() :-
  typeOfExp(s, e1) == INT(),
  typeOfExp(s, e2) == INT().

typeOfExp(s, Fun(x,      e)) = FUN(S, T) :- {s_fun}

  new s_fun, s_fun -P-> s,
  s_fun -> Var{x} with typeOfDecl S,
  typeOfExp(s_fun, e) == T.

typeOfExp(s, Var(x)) = T :-
  typeOfDecl of Var{x} in s |-> [(_, (_, T))].
```

How to check types?

What are challenges when implementing a type checker?

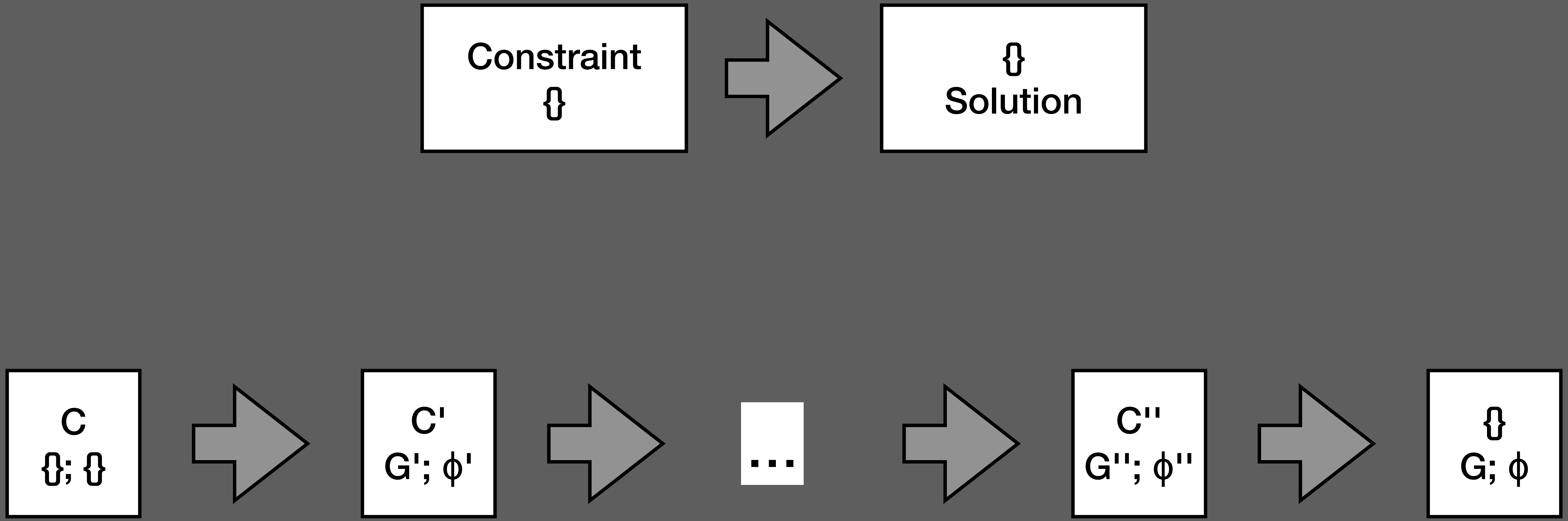
- Collecting necessary binding information before using it
- Gradually learning type information

What are the consequences of these challenges?

- The order of computation needs to be more flexible than the AST traversal
- Support explicit logical variables during solving

Solving Constraints

Solving by Rewriting



Solving by Rewriting

Non-deterministic constraint selection

```
<C; G, ϕ> ⟶ <C; G, ϕ>
```

```
          <t ═ u, C; G, ϕ> ⟶ <C; G, ϕ'> where unify(ϕ,t,u) = ϕ'

      <s1 -L⟶ s2, C; G, ϕ> ⟶ <C; G', ϕ> where ϕ(s1) = #i, ϕ(s2) = #j,
                                                 G + {#i -L⟶ #j} = G'

<r in s ⟼ t, C; G, ϕ> ⟶ <t ═ d, C; G, ϕ> where ϕ(r) = x, ϕ(s) = #i,
                                                 resolve(G, #i, x) = d
```

```
def solve(C):
  if <C; {}, {}> ⟶* <{}; G, ϕ>:
    return <G, ϕ>
  else:
    fail
```

Scope graph and name resolution algorithm don't have to know about logical variables

Solving by Rewriting

Solver = rewrite system

- Rewrite a constraint set + solution
- Simplifying and eliminating constraints
  - Constraint selecting is non-deterministic
  - Resolution order is controlled by side conditions on rewrite rules
- Rely on (other) solvers and algorithms for base cases
  - Unification for term equality
  - Scope graph resolution
- The solution is final if all constraints are eliminated

Does the order matter for the outcome?

- Confluence: the output is the same for any solving order
- Partly true for Statix
  - Up to variable and scope names
  - Only if all constraints are reduced

Semantics vs Algorithm

What is the difference?

- Algorithm computes a solution (= model)
- Semantics describes when a constraint is satisfied by a model

How are these related?

- Soundness
  - If the solver returns $<G, \phi>$, then $G,\phi \vDash C$
- Completeness:
  - If a G and ϕ exists such that $G,\phi \vDash C$, then the solver returns it
  - If no such G or ϕ exists, the solver fails
- Principality
  - The solver finds the most general ϕ

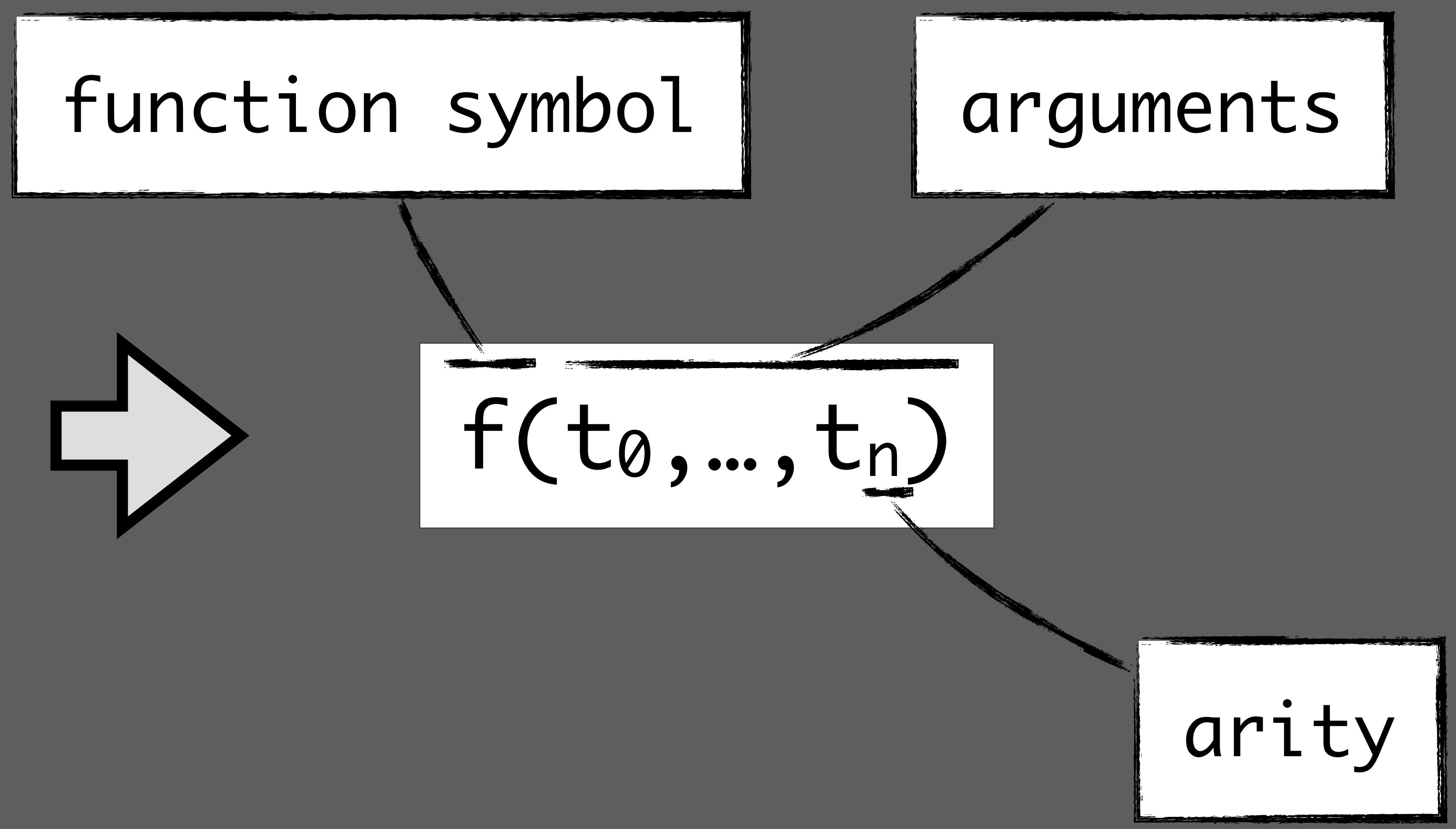
Term Equality & Unification

Syntactic Terms

terms	t, u
functions	f, g, h

Generic Terms

```
INT()
FUN(INT(),INT())
```

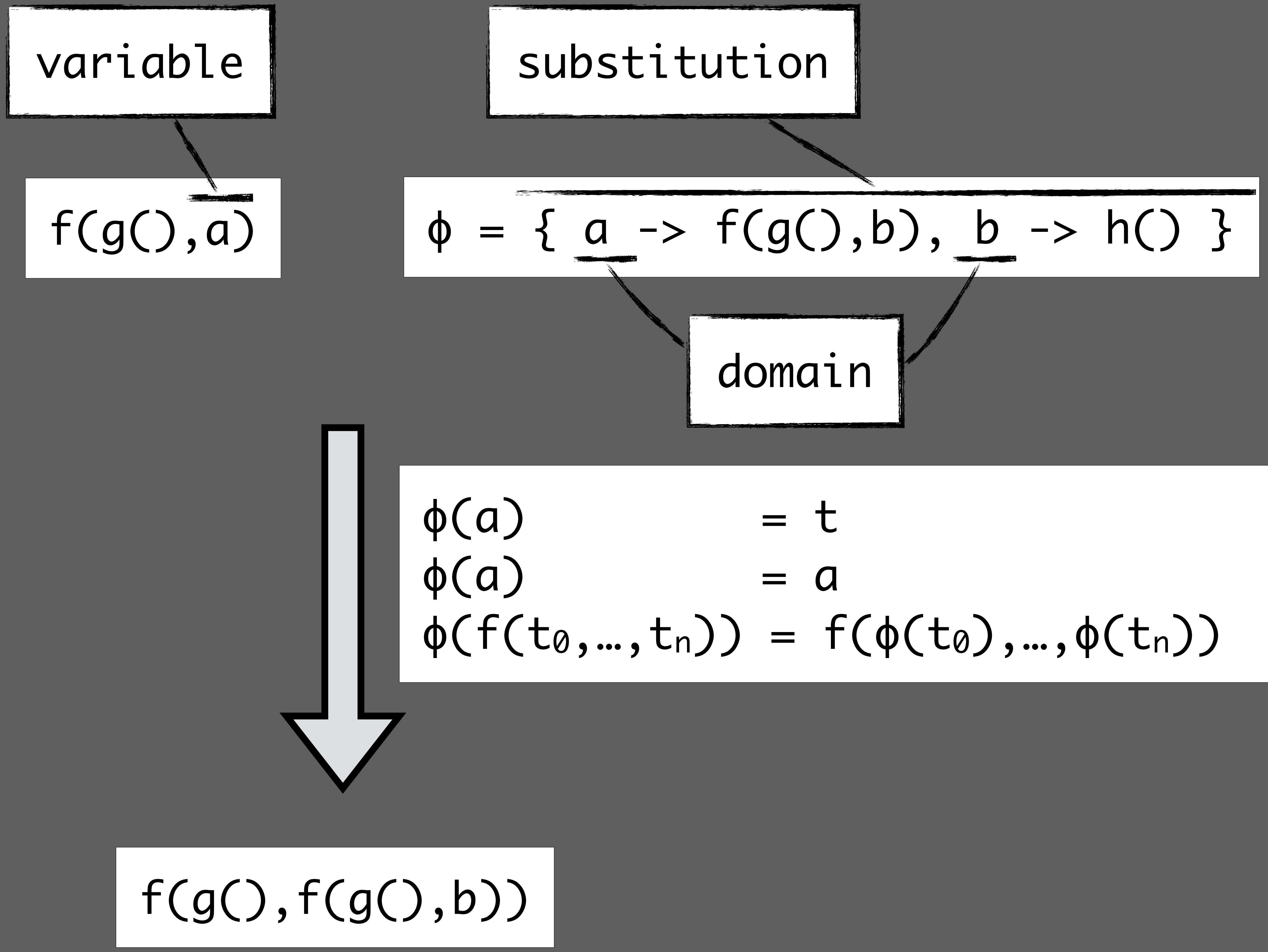


Syntactic Equality

$f(t_0,\ldots,t_n) == g(u_0,\ldots,u_m)$ if
- $f = g$, and $n = m$
- $t_i == u_i$ for every i

Variables and Substitution

terms	t, u
functions	f, g, h
variables	a, b, c
substitution	ϕ



```
f(g(),a)

ϕ = { a -> f(g(),b), b -> h() }
```

```
ϕ(a)            = t                    if { a -> t } in ϕ
ϕ(a)            = a                    otherwise
```

$\phi(f(t_0,\ldots,t_n)) = f(\phi(t_0),\ldots,\phi(t_n))$

```
f(g(),f(g(),b))
```

<u>ground term</u>: a term without variables

Unifiers

terms	t, u
functions	f, g, h
variables	a, b, c
substitution	ϕ

<u>unifier</u>: a substitution that makes terms equal

`f(a,g()) == f(h(),b)` $\Rightarrow$ `a -> h()`, `b -> g()` $\Rightarrow$ `f(h(),g()) == f(h(),g())`

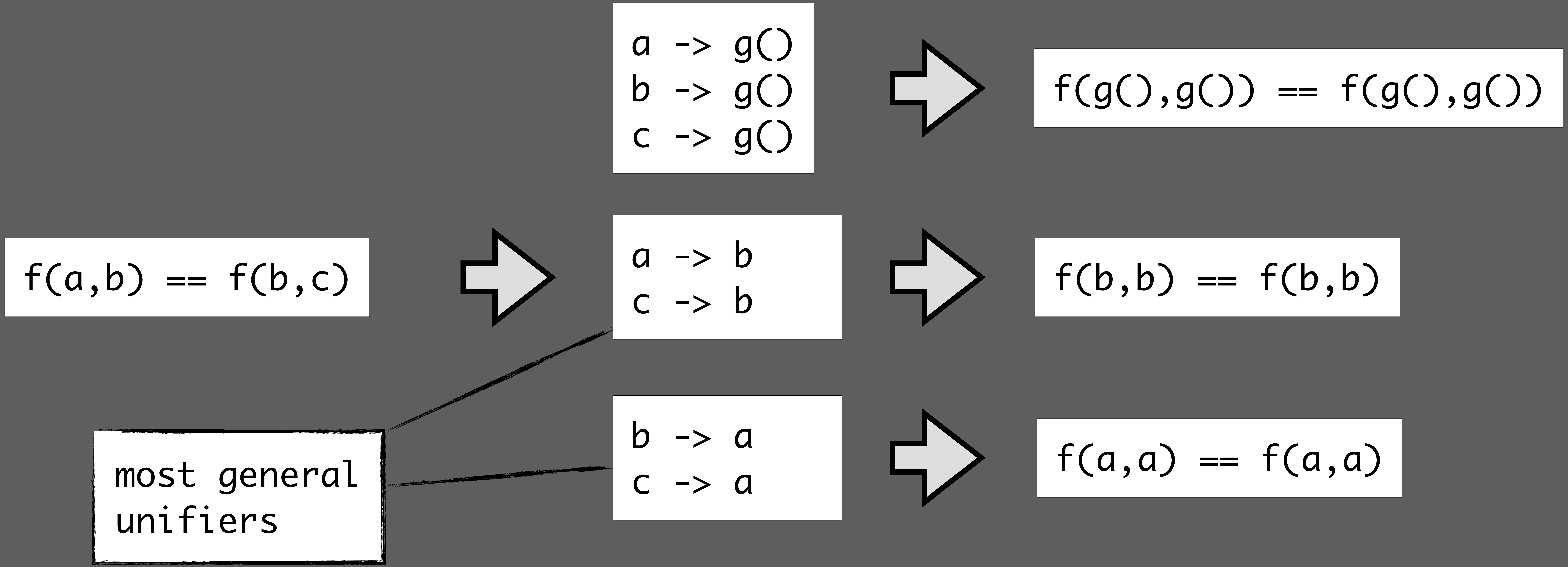
`g(a,f(b)) == g(f(h()),a)` $\Rightarrow$ `a -> f(h())`, `b -> h()` $\Rightarrow$ `g(f(h()),f(h())) == g(f(h()),f(h()))`

`f(a,h()) == g(h(),b)` $\Rightarrow$ no unifier, f != g

`f(b,b) == b` $\Rightarrow$ `b -> f(b,b)` $\leftarrow$ not idempotent

Most General Unifiers

terms	t, u
functions	f, g, h
variables	a, b, c
substitution	ϕ



```
f(a,b) == f(b,c)
```

```
a -> g()
b -> g()
c -> g()
```

```
f(g(),g()) == f(g(),g())
```

```
a -> b
c -> b
```

```
f(b,b) == f(b,b)
```

```
b -> a
c -> a
```

```
f(a,a) == f(a,a)
```

Most General Unifiers

terms	t, u
functions	f, g, h
variables	a, b, c
substitution	ϕ

every unifier is an instance of a most general unifier

(implicit) identity case

$$\begin{tikzcd} \begin{array}{l} a \texttt{ -> } b \\ b \texttt{ -> } b \\ c \texttt{ -> } b \end{array} \arrow[r, "b \texttt{ -> } g()"] & \begin{array}{l} a \texttt{ -> } g() \\ b \texttt{ -> } g() \\ c \texttt{ -> } g() \end{array} \end{tikzcd}$$

most general unifiers are related by renaming substitutions

$$\begin{tikzcd} \begin{array}{l} a \texttt{ -> } b \\ b \texttt{ -> } b \\ c \texttt{ -> } b \end{array} \arrow[r, "b \texttt{ -> } a"] & \begin{array}{l} a \texttt{ -> } a \\ b \texttt{ -> } a \\ c \texttt{ -> } a \end{array} \end{tikzcd}$$

$$\begin{tikzcd} \begin{array}{l} a \texttt{ -> } a \\ b \texttt{ -> } a \\ c \texttt{ -> } a \end{array} \arrow[r, "a \texttt{ -> } b"] & \begin{array}{l} a \texttt{ -> } b \\ b \texttt{ -> } b \\ c \texttt{ -> } b \end{array} \end{tikzcd}$$

Unification

terms	t, u
functions	f, g, h
variables	a, b, c
substitution	ϕ

```
global ϕ
def unify(t, u):
  if t is a variable:
    t := ϕ(t)
  if u is a variable:
    u := ϕ(u)
  if t is a variable and t == u:
    pass
  else if t == f($t_1$,...,$t_n$) and u == g($u_1$,...,$u_m$):
    if f == g and n == m:
      for i := 1 to n:
        unify($t_i$, $u_i$)
    else:
      fail "different function symbols"
  else if t is not a variable:
    unify(u, t)
  else if t occurs in u:
    fail "recursive term"
  else:
    ϕ += { t -> u }
```

t == a
instantiate variable

u == b
instantiate variable

b == b
equal variables

$t == f(t_1,\ldots,t_5)$, $u == f(u_1,\ldots,u_5)$
matching terms

$t == f(t_0,\ldots,t_5)$, $u == g(u_0,\ldots,u_3)$
mismatching terms

$t == f(t_0,\ldots,t_5)$, u == b
swap terms

t == a, u == k(g(a,f()))
recursive terms

t == a, $u == k(u_0,\ldots,u_5)$
extend unifier

Properties of Unification

Soundness

- If the algorithm returns a unifier, it makes the terms equal

Completeness

- If a unifier exists, the algorithm will return it

Principality

- If the algorithm returns a unifier, it is a most general unifier

Termination

- The algorithm always returns a unifier or fails

Efficient Unification with Union-Find

Complexity of Unification

Space complexity

- Exponential
- Representation of unifier

Time complexity

- Exponential
- Recursive calls on terms

Solution

- Union-Find algorithm
- Complexity growth can be considered constant

terms	t, u
functions	f, g, h
variables	a, b, c
substitution	ϕ

$h(a_1, \dots, a_n, f(b_0,b_0), \dots, f(b_{n-1},b_{n-1}), a_n) ==$
$h(f(a_0,a_0), \dots, f(a_{n-1},a_{n-1}), b_1, \dots, b_{n-1}, b_n)$

$a_1 \to f(a_0,a_0)$
$a_2 \to f(f(a_0,a_0), f(a_0,a_0))$
$a_i \to \dots\ 2^{i+1}-1$ subterms …
$b_1 \to f(a_0,a_0)$
$b_2 \to f(f(a_0,a_0), f(a_0,a_0))$
$b_i \to \dots\ 2^{i+1}-1$ subterms …

fully applied

$a_1 \to f(a_0,a_0)$
$a_2 \to f(a_1,a_1)$
$a_i \to \dots$ 3 subterms …
$b_1 \to f(a_0,a_0)$
$b_2 \to f(a_1,a_1)$
$b_i \to \dots$ 3 subterms …

triangular

Set Representatives

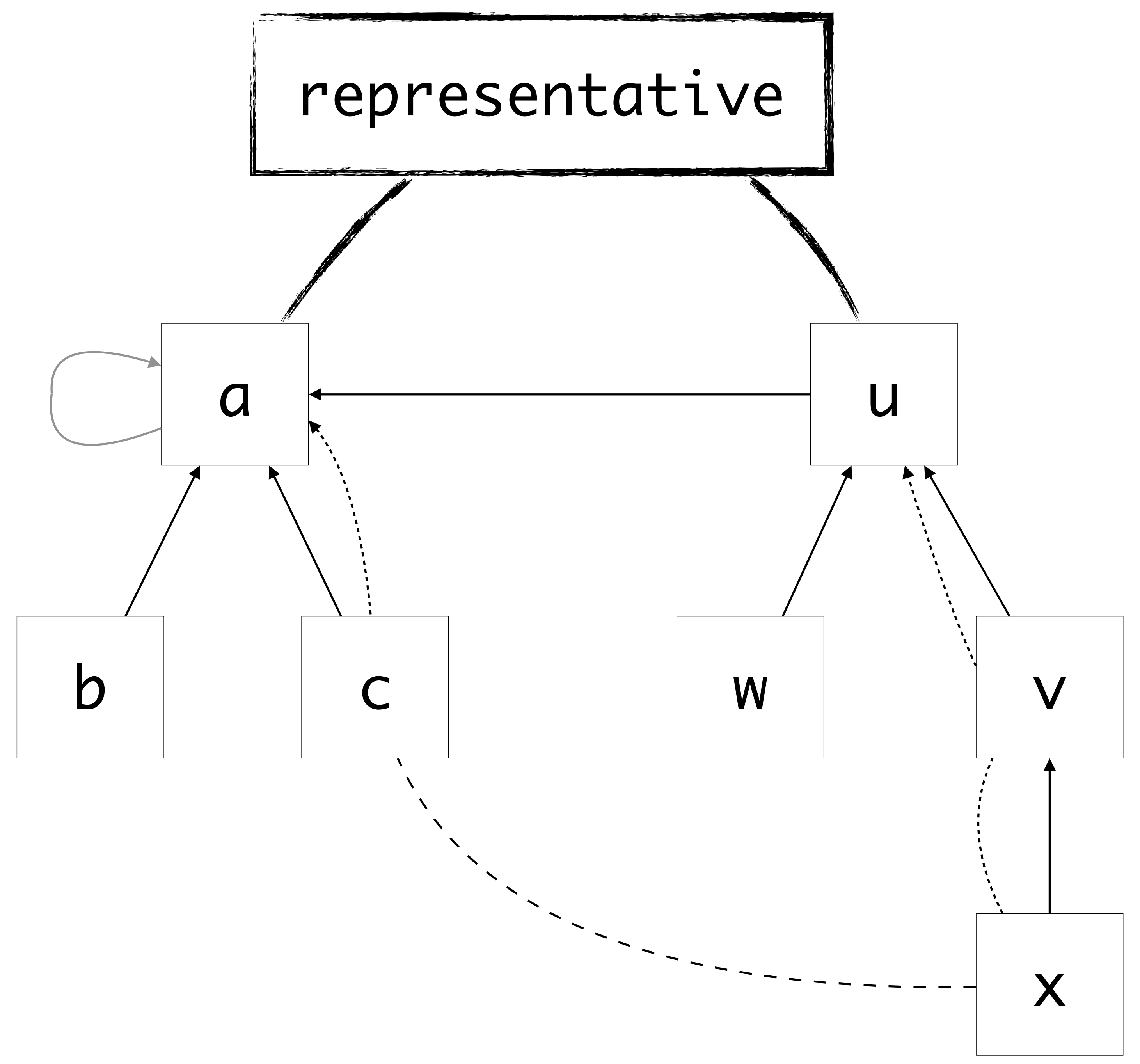
```
FIND(a):
  b := rep(a)
  if b == a:
     return a
  else
     return FIND(b)



UNION(a1,a2):
  b1 := FIND(a1)
  b2 := FIND(a2)
  LINK(b1,b2)

LINK(a1,a2):
  rep(a1) := a2
```

```
a == b
c == a
u == w
v == u
x == v
x == c
```



Path Compression

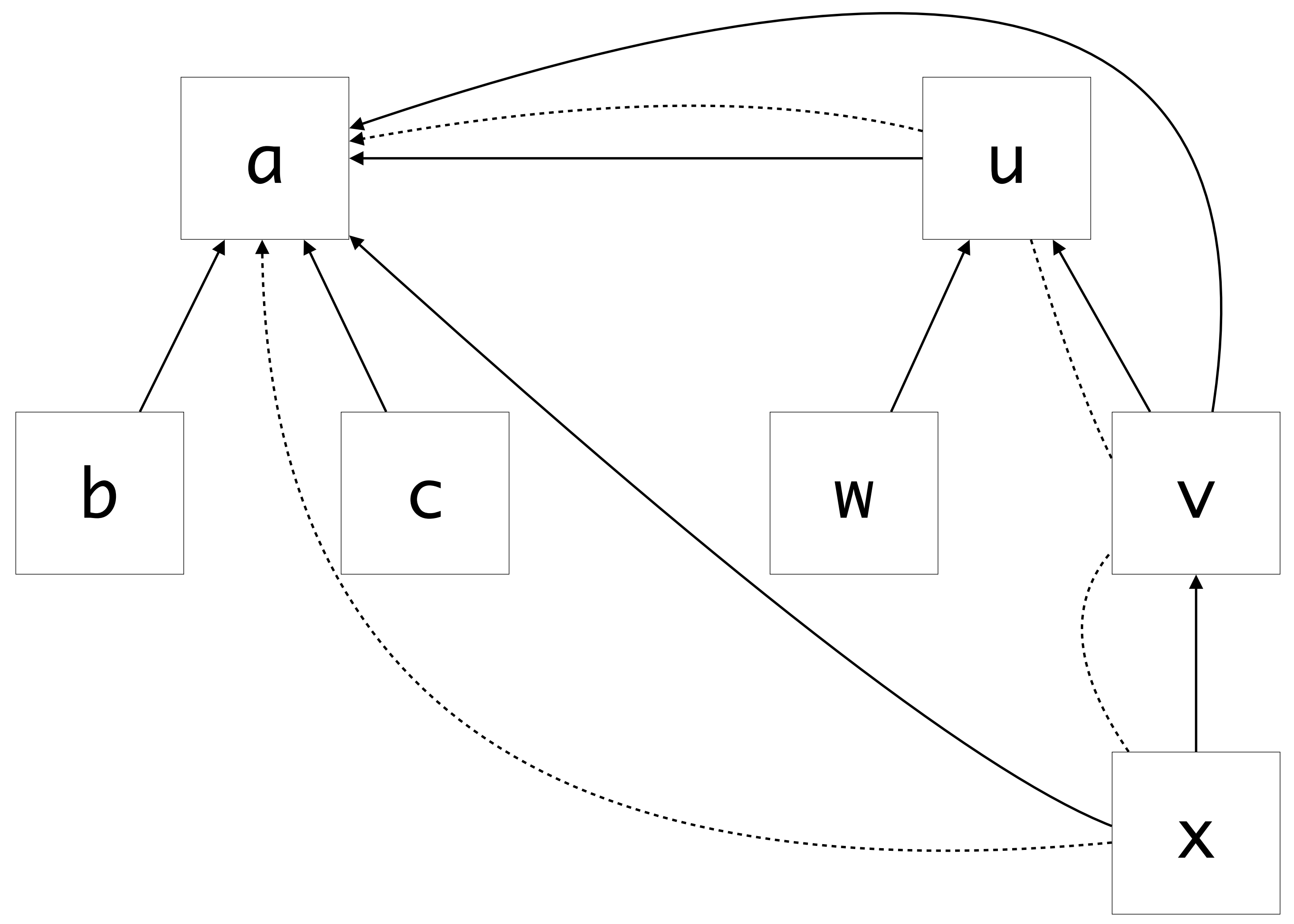
```
FIND(a):
  b := rep(a)
  if b == a:
     return a
  else
     return FIND(b)



UNION(a1,a2):
  b1 := FIND(a1)
  b2 := FIND(a2)
  LINK(b1,b2)

LINK(a1,a2):
  rep(a1) := a2
```

…
x == b
x == c
x == w
x == v



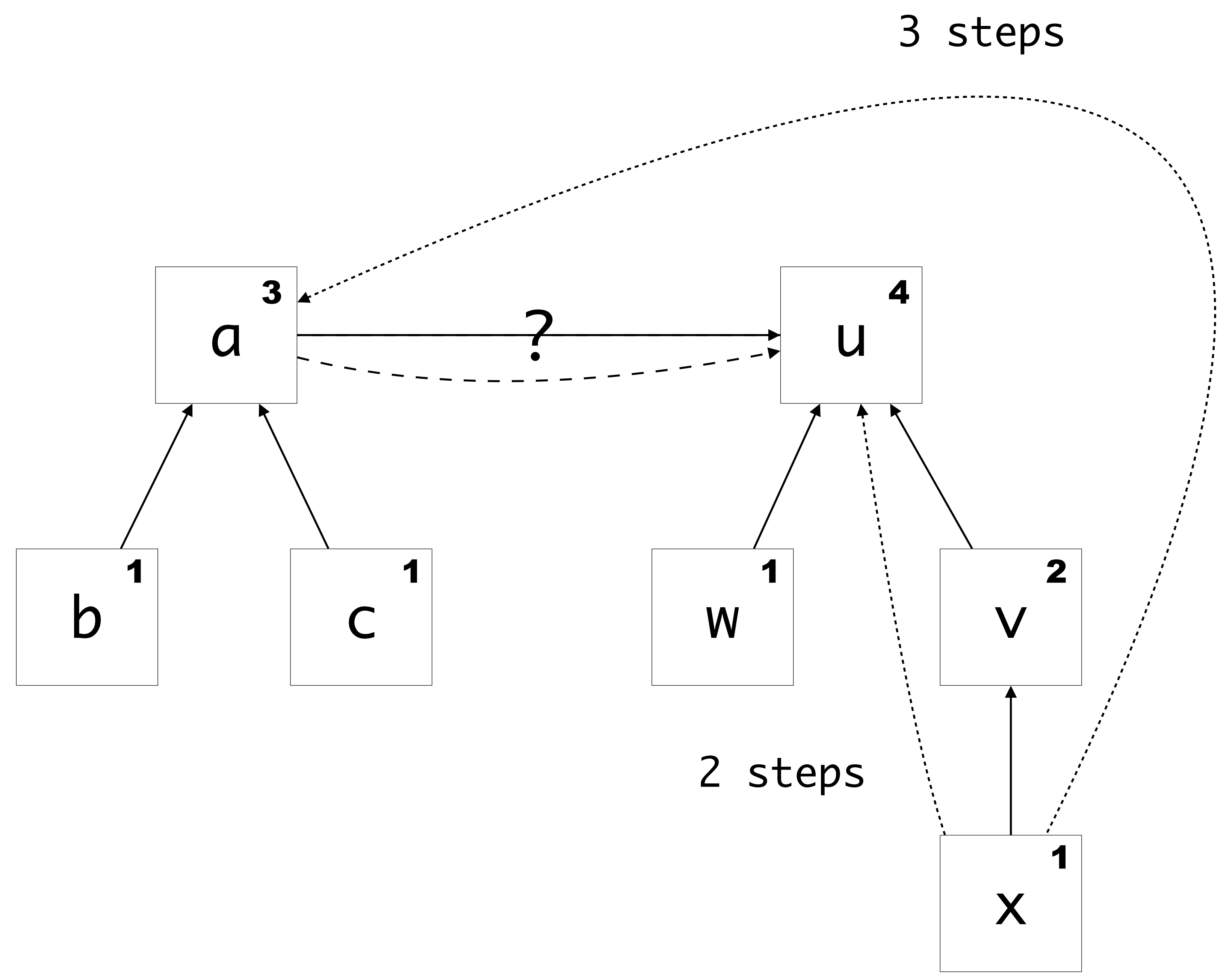
Tree Balancing

```
FIND(a):
  b := rep(a)
  if b == a:
     return a
  else
     b := FIND(b)
     rep(a) := b
     return b

UNION(a1,a2):
  b1 := FIND(a1)
  b2 := FIND(a2)
  LINK(b1,b2)

LINK(a1,a2):
  rep(a1) := a2
```

…
x == c



The Complex Case

$$\begin{array}{l} h(a_1\qquad,\ \ldots, a_n\qquad\qquad,\ f(b_0,b_0),\ \ldots,\ f(b_{n-1},b_{n-1}),\ a_n)\ == \\ h(f(a_0,a_0),\ \ldots, f(a_{n-1},a_{n-1}),\ b_1,\qquad\qquad \ldots,\ b_{n-1}\qquad\qquad,\ b_n) \end{array}$$

$$\begin{tikzcd}
 & a_0 \arrow[r] & b_0 & \\
f(a_0,a_0) & a_1 \arrow[l, dotted] & b_1 \arrow[l] \arrow[r, dotted] & f(b_0,b_0) \\
 & \vdots & \vdots & \\
f(a_{n-2},a_{n-2}) & a_{n-1} \arrow[l, dotted] & b_{n-1} \arrow[l] \arrow[r, dotted] & f(b_{n-2},b_{n-2}) \\
f(a_{n-1},a_{n-1}) & a_n \arrow[l, dotted] \arrow[r] & b_n \arrow[r, dotted] & f(b_{n-1},b_{n-1})
\end{tikzcd}$$

$$\begin{array}{c}
a_n == b_n \\
f(a_{n-1},a_{n-1}) == f(b_{n-1},b_{n-1}) \\
a_{n-1} == b_{n-1} \qquad a_{n-1} == b_{n-1} \\
f(a_{n-2},a_{n-2}) == f(b_{n-2},b_{n-2}) \\
\vdots \\
a_1 == b_1 \qquad a_1 == b_1 \\
f(a_0,a_0) == f(b_0,b_0) \\
a_0 == b_0 \qquad a_0 == b_0
\end{array}$$

How about occurrence checks? Postpone!

Union-Find

`Martelli, Montanari. An Efficient Unification Algorithm. TOPLAS, 1982`

Main idea

- Represent unifier as graph
- One variable represent equivalence class
- Replace substitution by union & find operations
- Testing equality becomes testing node identity

Optimizations

- Path compression make recurring lookups fast
- Tree balancing keeps paths short

Complexity

- Linear in space and almost linear (inverse Ackermann) in time
- Easy to extract triangular unifier from graph
- Postpone occurrence checks to prevent traversing (potentially) large terms

Conclusion

Summary

What is the meaning of constraints?

- Formally described by constraint semantics
- Semantics classifies solutions, but do not compute them
- Semantics is expressed in terms of other theories
  - Syntactic equality
  - Scope graph resolution

What techniques can we use to implement solvers?

- Constraint simplification
  - Simplification rules
  - Depends on built-in procedures to unify or resolve names
- Unification
  - Unifiers make terms with variables equal
  - Unification computes most general unifiers

What is the relation between solver and semantics?

- Soundness: any solution satisfies the semantics
- Completeness: if a solution exists, the solver finds it
- Principality: the solver computes most general solutions