

Eberhard Karls Universität Tübingen
Mathematisch-Naturwissenschaftliche Fakultät
Wilhelm-Schickard-Institut für Informatik

Bachelor Thesis Computer Science

Higher-Order Unification for Data and Codata Types

Julia Wegendt

Date

Reviewer

Prof. Dr. Klaus Ostermann
Department of Computer Science
University of Tübingen

Wegendt, Julia

Higher-Order Unification for Data and Codata Types

Bachelor Thesis Computer Science

Eberhard Karls Universität Tübingen

Period: from-till

Abstract

Write here your abstract.

Acknowledgements

Write here your acknowledgements.

Contents

1	Introduction	1
2	The Untyped Calculus ND	1
2.1	Syntax of the Untyped Calculus ND	1
2.2	Free Variables, Substitutions, Contexts	2
2.3	Conversion	4
3	Simple Types	5
3.1	Typing Rules	5
4	First-Order Unification	6
5	Higher-Order Unification	7
6	Pattern Unification	9
7	The Algorithm For Higher-Order Unification	11
7.1	Decomposing Constraints	11
7.2	Unification	13

List of Theorems

2.1	Definition (Terms of the Calculus ND)	1
2.2	Definition (Free Variables)	2
2.3	Definition (Substitution)	2
2.4	Definition (Domain and Range of a Substitution)	3
2.5	Definition (Action of a Substitution)	3
2.6	Definition (Composition of Substitutions)	3
2.7	Definition (Idempotency)	3
2.8	Definition (More General)	4
2.9	Definition (Beta-Conversion)	4
2.10	Definition (Eta-Conversion for Codata)	4
4.1	Definition (Solution)	6

4.2	Definition (Most General)	6
4.3	Definition (First-Order unification)	6
4.1	Theorem (Decidability of First-Order Unification)	7
4.4	Definition (Unification algorithm for First-Order Unification)	7
5.1	Definition (Higher-Order Unification)	7
5.2	Definition (Constraint)	8
5.1	Theorem (Decidability of Higher-Order Unification)	9
6.1	Definition (Pattern)	9
6.1	Theorem (Decidability of Pattern Unification)	9
6.2	Definition (Normal Form)	10
6.2	Theorem	11
7.1	Example (Decomposing constraints-redundancy and contradiction)	11
7.2	Example (Decomposing constraints-splitting into smaller parts)	12
7.1	Definition (Decomposing Constraints)	12
7.2	Definition (Unification)	14

1 Introduction

Most people probably first encounter unification problems in school, when solving simple math problems. It is also necessary in a few important applications in computer science: Type checking and type inference, in proof assistants, as well as more particular fields like logic programming and computational linguistics. While unification means solving equations with unknown variables, there are two major types of unification: First-order unification and higher-order unification.

For the type systems in most typed programming languages, first-order unification is enough. It is only when more complex types are introduced, like in the interactive theorem prover Coq or in the programming language Agda, higher-order unification is required.

...

While data is a well-known concept and computer scientist have spent a considerable amount thinking about it, its brother codata is less talked about. Codata is dual to data, meaning any concept expressed using data may also be expressed through codata. While data is concerned with how values are constructed or stored, codata is concerned with how values are destructured or used.

$5 \equiv \alpha^?$ and `True` \equiv `False` are examples for first-order unification.

In higher-order unification, functions may appear: ...

2 The Untyped Calculus ND

I will be introducing the Untyped Calculus ND, based on ...

2.1 Syntax of the Untyped Calculus ND

Some knowledge of notation is necessary to familiarize oneself with the syntax of the Untyped Calculus. X represents a (possibly empty) sequence $X_1, \dots, X_i, \dots, X_n$.

A pattern match $e.\mathbf{case}\{\overline{K(\bar{x})} \Rightarrow e\}$ matches a term e against a sequence of clauses, each clause consisting of a constructor and an expression. The expression associated with first constructor that matches the term is the result of the pattern match. For a copattern match $\mathbf{cocase}\{\overline{d(\bar{x})} \Rightarrow e\}$ the same rules apply, but instead of constructors, the term is matched against destructors.

Definition 2.1 (Terms of the Calculus ND).

$e, r, s, t ::= x, y$	Variable
$ K(\bar{e})$	Constructor
$ e.d(\bar{e})$	Destructor
$ e.\mathbf{case}\{\overline{K(\bar{x}) \Rightarrow e}\}$	Pattern match
$ \mathbf{cocase}\{\overline{d(\bar{x}) \Rightarrow e}\}$	Copattern match

In pattern and copattern matches, every con- or destructor may occur no more than once.

Let's look at some examples to ... All rudimentary datatypes can be constructed through constructors: The Booleans **True** and **False** are constructors on an empty sequence. We can of course represent integers as peano numbers using constructors.

Abstract data types like lists, arrays, records etc. can similarly be defined through constructors: **Cons**(**True**, **Cons**(**False**, **Nil**)) and **Date**(27, 08, 2005).

We can use Pattern matching to represent conditionals: Like if statements: if e_1 e_2 else e_3 which is analogous to: $e_1.\mathbf{case}\{\mathbf{True} \Rightarrow e_2, \mathbf{False} \Rightarrow e_3\}$ Or the expression which tests whether a given list starts with **True**: $e.\mathbf{case}\{\mathbf{Cons}(\mathbf{True}, x) \Rightarrow \mathbf{True}, \mathbf{Nil} \Rightarrow \mathbf{False}, \mathbf{Cons}(x, y) \Rightarrow \mathbf{False}\}$

2.2 Free Variables, Substitutions, Contexts

Definition 2.2 (Free Variables). The set of free variables of a term e is $\text{FV}(e)$. A term is closed if this set is empty. Free Variables are defined recursively over the structure of terms as follows:

$$\begin{aligned}
 \text{FV}(x) &:= \{x\} \\
 \text{FV}(K(e_1, \dots e_n)) &:= \text{FV}(e_1) \cup \dots \cup \text{FV}(e_n) \\
 \text{FV}(e.d(e_1, \dots e_n)) &:= \text{FV}(e) \cup \text{FV}(e_1) \cup \dots \cup \text{FV}(e_n) \\
 \text{FV}(e.\mathbf{case}\{\overline{K(\bar{x}) \Rightarrow e}\}) &:= \text{FV}(e) \cup (\text{FV}(e_1) \setminus \bar{x}) \cup \dots \cup (\text{FV}(e_n) \setminus \bar{x}) \\
 \text{FV}(\mathbf{cocase}\{\overline{d(\bar{x}) \Rightarrow e}\}) &:= (\text{FV}(e_1) \setminus \bar{x}) \cup \dots \cup (\text{FV}(e_n) \setminus \bar{x})
 \end{aligned}$$

Definition 2.3 (Substitution). A simultaneous substitution σ of the terms $e_1, \dots e_n$ for the distinct variables $x_1, \dots x_n$ is defined as follows:

$$\sigma ::= [e_1, \dots e_n \setminus x_1, \dots x_n]$$

The set of variables for which the substitution is defined is called the domain. The set of free variables which appear in the substitution is called the range.

Definition 2.4 (Domain and Range of a Substitution). The definitions of Domain and Range of a Substitution are as follows:

$$\begin{aligned}\text{dom}([e_1, \dots, e_n/x_1, \dots, x_n]) &:= \{x_1, \dots, x_n\} \\ \text{rng}([e_1, \dots, e_n/x_1, \dots, x_n]) &:= \text{FV}(e_1) \cup \dots \cup \text{FV}(e_n)\end{aligned}$$

What is actually interesting is what happens when we apply a substitution to an expression

Definition 2.5 (Action of a Substitution). The action of a substitution σ on a term e , written as $e\sigma$ and is defined as follows:

$$\begin{aligned}x[e_1, \dots, e_n/x_1, \dots, x_n] &:= e_i \quad (\text{if } x = x_i) \\ y\sigma &:= y \quad (\text{if } y \notin \text{dom}(\sigma)) \\ (K(e_1, \dots, e_n))\sigma &:= K(e_1\sigma, \dots, e_n\sigma) \\ (e.d(e_1, \dots, e_n))\sigma &:= (e\sigma).d(e_1\sigma, \dots, e_n\sigma) \\ (e.\text{case}\{\overline{K(\bar{x})} \Rightarrow e\})\sigma &:= (e\sigma).\text{case}\{\overline{K(\bar{y})} \Rightarrow (e\sigma')\sigma\} \\ (\text{ccase}\{\overline{d(\bar{x})} \Rightarrow e\})\sigma &:= \text{ccase}\{\overline{d(\bar{y})} \Rightarrow (e\sigma')\sigma\}\end{aligned}$$

Where σ' is a substitution that ensures that we don't bind new variables: σ' has the form $[y_1, \dots, y_n/x_1, \dots, x_n]$ and all y_i are fresh for both the domain and the range of σ .

The composition of two substitutions $\sigma_2 \circ \sigma_1$ which is equivalent to first applying the substitution σ_1 , then the substitution σ_2 .

Definition 2.6 (Composition of Substitutions). Given two substitutions

$$\sigma_1 := [e_1, \dots, e_n/x_1, \dots, x_n], \quad \sigma_2 := [t_1, \dots, t_m/y_1, \dots, y_m]$$

Composition is defined as:

$$\sigma_2 \circ \sigma_1 := [e_1\sigma_2, \dots, e_n\sigma_2, t_j, \dots, t_k/x_1, \dots, x_n, y_j, \dots, y_k]$$

Where j, \dots, k is the greatest sub-range of indices $1, \dots, m$ such that none of the variables y_j to y_k is in the domain of σ_1

Definition 2.7 (Idempotency). A substitution σ is idempotent, iff. $\sigma \circ \sigma = \sigma$. Concretely, this means that it doesn't matter how often we apply a substitution to a given problem.

For example, $[\text{ccase}\{\text{Ap}(x) \Rightarrow x\}/y]$ is idempotent, since:

$$\begin{aligned}& [\text{ccase}\{\text{Ap}(x) \Rightarrow x\}/y] \circ [\text{ccase}\{\text{Ap}(x) \Rightarrow x\}/y] \\ &= [\text{ccase}\{\text{Ap}(x) \Rightarrow x\}[\text{ccase}\{\text{Ap}(x) \Rightarrow x\}/y]/y] \\ &= [\text{ccase}\{\text{Ap}(x) \Rightarrow x\}/y]\end{aligned}$$

On the other hand, the substitution $[\mathbf{cocode}\{\mathbf{Ap}(y) \Rightarrow x\}/x]$ is not idempotent, since:

$$\begin{aligned} & [\mathbf{cocode}\{\mathbf{Ap}(y) \Rightarrow x\}/x] \circ [\mathbf{cocode}\{\mathbf{Ap}(y) \Rightarrow x\}/x] \\ &= [\mathbf{cocode}\{\mathbf{Ap}(y) \Rightarrow x\}[\mathbf{cocode}\{\mathbf{Ap}(y) \Rightarrow x\}/x]/x] \\ &= \mathbf{cocode}\{\mathbf{Ap}(y) \Rightarrow (\mathbf{Ap}(y) \Rightarrow x)\} \neq [\mathbf{cocode}\{\mathbf{Ap}(y) \Rightarrow x\}/x] \end{aligned}$$

Definition 2.8 (More General). A substitution σ is more general than a substitution θ , iff. there exists a mapping τ , such that: $\theta = \tau \circ \sigma$.

For example, look at the following unification problem where we are trying to substitute types for two unification variables:

$$\begin{aligned} \text{List}(\alpha^?) &\equiv \text{List}(\beta^?) \\ \alpha^? &\equiv \text{Int} \end{aligned}$$

One solution might be: $\theta = [\text{Int}, \text{Int}/\alpha^?, \beta^?]$, so substituting Int for both unification variables. The more general solution is $\sigma = [\text{Int}, \alpha^?/\alpha^?, \beta^?]$ (substituting $\alpha^?$ for $\beta^?$, and substituting Int for $\alpha^?$), however. This is because there exists a mapping $\tau = [\text{Int}/\alpha^?]$, such that:

$$\tau \circ \sigma = [\text{Int}[\text{Int}/\alpha^?], \alpha^?[\text{Int}/\alpha^?]/\alpha^?, \beta^?] = [\text{Int}, \text{Int}/\alpha^?, \beta^?] = \theta$$

2.3 Conversion

Definition 2.9 (Beta-Conversion). A single step of beta-conversion $e_1 \equiv_\beta^1 e_2$ is defined as follows:

$$\begin{aligned} K(\bar{e}).\mathbf{case}\{\dots, K(\bar{x}) \Rightarrow e, \dots\} &\equiv_\beta^1 e[\bar{e}/\bar{x}] & (\beta\text{-Data}) \\ \mathbf{cocode}\{\dots, d(\bar{x}) \Rightarrow e, \dots\}.d(\bar{e}) &\equiv_\beta^1 e[\bar{e}/\bar{x}] & (\beta\text{-Codata}) \end{aligned}$$

We require that the constructor $K(\bar{e})$ and the constructor $K(\bar{x})$ have the same number of arguments. This, in short ensures that we don't generate stuck terms, i.e. terms that can't be evaluated.

Some examples:

$$\begin{aligned} \text{True}.\mathbf{case}\{\text{False} \Rightarrow \text{True}, \text{True} \Rightarrow \text{False}\} &\equiv_\beta^1 \text{False} \\ \mathbf{cocode}\{\mathbf{Ap}(x) \Rightarrow \text{True}\}.\mathbf{Ap}(x) &\equiv_\beta^1 \text{True}[x/x] = \text{True} \\ \mathbf{cocode}\{\mathbf{Ap}(y) \Rightarrow y\}.\mathbf{Ap}(x) &\equiv_\beta^1 y[x/y] = x \end{aligned}$$

Intuitively, beta-conversion means function application or the reduction under pattern or copattern matching.

Definition 2.10 (Eta-Conversion for Codata). A single step of eta-conversion $e_1 \equiv_\eta^1 e_2$ is defined as follows:

$$\mathbf{cocode}\{\overline{d(\bar{x}) \Rightarrow e.d(\bar{x})}\} \equiv_\eta^1 e \quad (\text{if } \bar{x} \notin \text{FV}(e)) \quad (\eta\text{-Codata})$$

3 Simple Types

We want to be able to use the unification algorithm to discern types for given terms. To start, let's look at some examples terms and their types:

```

5 : Int
False : Bool
Tup(1, True) : Pair(Int, Bool)
cocase{fst ⇒ 1, snd ⇒ True} : LPair(Int, Bool)
Cons(1, Cons(2, Nil)) : List(Int)
cocase{Ap(x) ⇒ x.case{True ⇒ False, False ⇒ True}} : Bool → Bool
Trues = cocase{hd ⇒ True, tl ⇒ Trues} : Stream(Bool)

```

3.1 Typing Rules

To be able to give our examples a formal basis, we will introduce typing rules. These will not cover all the types one could construct using our calculus, but instead all the basic composite types. This will be enough to construct examples covering each case we have to consider, and hopefully give an idea how to construct any type.

When writing $\Gamma \vdash t : \tau$, we mean that from the variables and their types in Γ , we can deduce that t has the type τ .

$$\begin{array}{c}
\frac{x : \tau \in \Gamma}{\Gamma \vdash x : \tau} \text{VAR} \quad \frac{}{\Gamma \vdash \text{True} : \text{Bool}} \text{TRUE} \quad \frac{}{\Gamma \vdash \text{False} : \text{Bool}} \text{FALSE} \\
\\
\frac{\Gamma \vdash t_1 : \tau_1 \quad \Gamma \vdash t_2 : \tau_2}{\Gamma \vdash \text{Tup}(t_1, t_2) : \text{Pair}(\tau_1, \tau_2)} \text{TUP} \\
\\
\frac{}{\Gamma \vdash \text{Nil} : \text{List}(\tau)} \text{NIL} \quad \frac{\Gamma \vdash t_1 : \tau \quad \Gamma \vdash t_2 : \text{List}(\tau)}{\Gamma \vdash \text{Cons}(t_1, t_2) : \text{List}(\tau)} \text{CONS} \\
\\
\frac{\Gamma \vdash t : \text{List}(\tau') \quad \Gamma \vdash t_1 : \tau \quad \Gamma, y : \tau', z : \text{List}(\tau') \vdash t_2 : \tau}{\Gamma \vdash t.\text{case}\{\text{Nil} \Rightarrow t_1, \text{Cons}(y, z) \Rightarrow t_2\} : \tau} \text{CASE-LIST} \\
\\
\frac{\Gamma \vdash t : \text{Pair}(t_1, t_2) \quad \Gamma, x : \tau_1, y : \tau_2, t : \tau}{\Gamma \vdash t.\text{case}\{\text{Tup}(t_1, t_2) \Rightarrow t\} : \tau} \text{CASE-PAIR} \\
\\
\frac{\Gamma \vdash t : \text{Stream}(\tau)}{\Gamma \vdash t.\text{hd} : \tau} \text{HD} \quad \frac{\Gamma \vdash t : \text{Stream}(\tau)}{\Gamma \vdash t.\text{tl} : \text{Stream}(\tau)} \text{TL}
\end{array}$$

$$\begin{array}{c}
\frac{\Gamma \vdash t_1 : \tau \quad \Gamma \vdash t_2 : \text{Stream}(\tau)}{\Gamma \vdash \mathbf{cocase}\{\mathbf{hd} \Rightarrow t_1, \mathbf{tl} \Rightarrow t_2\} : \text{Stream}(\tau)} \text{STREAM} \\
\\
\frac{\Gamma \vdash t : \text{Lpair}(\tau_1, \tau_2)}{\Gamma \vdash t.\mathbf{fst} : \tau_1} \text{FST} \qquad \frac{\Gamma \vdash t : \text{Lpair}(\tau_1, \tau_2)}{\Gamma \vdash t.\mathbf{snd} : \tau_2} \text{SND} \\
\\
\frac{\Gamma \vdash t_1 : \tau_1 \quad \Gamma \vdash t_2 : \tau_2}{\Gamma \vdash \mathbf{cocase}\{\mathbf{fst} \Rightarrow t_1, \mathbf{snd} \Rightarrow t_2\} : \text{LPair}(\tau_1, \tau_2)} \text{LPAIR} \\
\\
\frac{\Gamma \vdash t_1 : \tau_1 \rightarrow \tau_2 \quad \Gamma \vdash t_2 : \tau_1}{\Gamma \vdash t_1.\mathbf{Ap}(t_2) : \tau_2} \text{APP} \\
\\
\frac{\Gamma, x : \tau_1 \vdash t : \tau_2}{\Gamma \vdash \mathbf{cocase}\{\mathbf{Ap}(x) \Rightarrow t\} : \tau_1 \rightarrow \tau_2} \text{FUN}
\end{array}$$

4 First-Order Unification

We want to slowly make our way to higher-order unification, and thus touch on simpler problems first. Furthermore, we need a couple concepts more to be able to talk about unification problems and describe our algorithm.

The Unification Problem is described by a set of equations with expressions on each side $\bar{e} \equiv \bar{e}$ containing unknown unification variables $\alpha_1^?, \alpha_2^?, \dots$, where our goal is to find a simultaneous substitution $[e_1, \dots, e_n / \alpha_1^?, \dots, \alpha_n^?]$ which substitutes expressions for unification variables, such that the sides of the given equations are the same (respectively).

Definition 4.1 (Solution). A solution to a given unification problem is described by a simultaneous substitution $[e_1, \dots, e_n / \alpha_1^?, \dots, \alpha_n^?]$ which when applied to the problem solves it, i.e. makes the sides of the equations equal

Definition 4.2 (Most General). A solution is the most general unifier (mgu), iff. it is more general than all other solutions.

Now let's take a look at first-order unification, which is a pretty limited subproblem, but in many applications all we need, as in most type checking.

Definition 4.3 (First-Order unification).

$$\begin{array}{ll}
e, r, s, t ::= \alpha^?, \beta^? & \text{Unification variable} \\
\quad \mid x & \text{Variable} \\
\quad \mid K(\bar{e}) & \text{Constructor}
\end{array}$$

Some examples: $\alpha^? \equiv \text{True}$ has the solution $[\text{True}/\alpha^?]$. $\text{True} \equiv \text{False}$ doesn't have a solution.

$\text{Int} \rightarrow \alpha^? \equiv \text{Int} \rightarrow \text{Bool}$ has the solution $[\text{Bool}/\alpha^?]$. On the other hand, $\alpha^? \equiv \text{List}(\alpha^?)$ should not have a solution. This is the negative example for the occur check rule below.

Theorem 4.1 (Decidability of First-Order Unification). For first-order unification, there exists an algorithm on equations $\bar{e} \equiv \bar{e}$, which always terminates, and returns the solution if there exists one. In particular, this solution is always a mgu (i.e. if there is a solution, then there always exists a most general one).

Definition 4.4 (Unification algorithm for First-Order Unification). \perp is the symbol for fail. The algorithm is defined by non-deterministically applying the below rules:

$$\begin{aligned}
E \cup \{e \equiv e\} &\Rightarrow E && \text{(delete)} \\
E \cup \{K(e_1 \dots e_n) \equiv K(t_1 \dots t_n)\} &\Rightarrow E \cup \{e_1 \equiv t_1, \dots, e_n \equiv t_n\} && \text{(decompose)} \\
E \cup \{K_1(e_1, \dots, e_n) \equiv K_2(t_1, \dots, t_m)\} &\Rightarrow \perp && \text{if } K_1 \neq K_2 \text{ or if } n \neq m \text{ (conflict)} \\
E \cup \{e \equiv \alpha^?\} &\Rightarrow E \cup \{\alpha^? \equiv e\} && \text{(swap)} \\
E \cup \{\alpha^? \equiv e\} &\Rightarrow E[e/\alpha^?] \cup \{\alpha^? \equiv e\} && \text{if } \alpha^? \in E \text{ and } \alpha^? \notin e \text{ (eliminate)} \\
E \cup \{\alpha^? \equiv K(e_1, \dots, e_n)\} &\Rightarrow \perp && \text{if } \alpha^? \in e_1, \dots, e_n \text{ (occurs check)}
\end{aligned}$$

This algorithm is based on the version presented by Martelli and Montanari in [3], adapted to our syntax.

5 Higher-Order Unification

Definition 5.1 (Higher-Order Unification).

$$\begin{array}{ll}
e, r, s, t ::= \alpha^? \sigma, \beta^? \sigma & \text{Unification Variables with substitution} \\
| x & \text{Variable} \\
| K(\bar{e}) & \text{Constructor} \\
| e.d(\bar{e}) & \text{Destructor} \\
| e.\text{case}\{\overline{K(\bar{x}) \Rightarrow e}\} & \text{Pattern match} \\
| \text{cocase}\{\overline{d(\bar{x}) \Rightarrow e}\} & \text{Copattern match}
\end{array}$$

Note that this encompasses our syntax described in Section 2, but with the addition of unification variables with substitutions. To illustrate the need for this substitution, look at what problem arises when omitting the substitution: Take the following example: $\text{cocase}\{\text{Ap}(x) \Rightarrow \alpha^?\}. \text{Ap}(y) \equiv \beta^?$. First

focus on the left side and notice that there is a redex. What happens if we reduce it?

$$\mathbf{cocase}\{\mathbf{Ap}(x) \Rightarrow \alpha^?\}. \mathbf{Ap}(y) \equiv_{\beta}^1 \alpha^?[y/x]$$

This motivates our need for substitutions: We may need to apply substitutions to unification variables. Note that this is *not* possible in first-order unification, since we don't create substitutions through redexes!

When the substitution is trivial, we may write $\alpha^?, \beta^?$ instead.

In higher-order unification in contrast to in first-order unification, we are not interested in syntactic equality, but want a broader set of terms to be equal to one another. Depending on the type of unification problem one wants to solve, they may want to only include beta-equality or both beta- and eta-equality.

This further motivates our use of the symbol \equiv so far. Whereas in first-order unification it just stands for syntactic equality, in higher-order unification, I use it to mean syntactically equality, beta-equality or eta-equality. This essentially means that two terms are equivalent if they are equivalent after function application and/or are equivalent externally.

Let's next consider a few examples: The problem $\alpha^?.\mathbf{Ap}(5) \equiv 5$ has multiple solutions: $[\mathbf{cocase}\{\mathbf{Ap}(x) \Rightarrow x\}/\alpha^?]$ and $[\mathbf{cocase}\{\mathbf{Ap}(x) \Rightarrow 5\}/\alpha^?]$, where \mathbf{Ap} is a function applicator. Thus, the two given solutions are the identity function and the constant function 5, which when consuming the argument 5, both give back 5. In this case there also doesn't exist an mgu.

To be able to discuss unification equations in more depth, we need one more concept:

Definition 5.2 (Constraint).

$$\begin{aligned} C &::= \top \mid \perp \mid \Psi \vdash e \equiv t \\ \mathcal{C} &::= C \wedge \mathcal{C} \end{aligned}$$

Ψ , called context is just a list of distinct variables x_1, \dots, x_n and may be empty.

$\Psi \vdash e \equiv t$ means that given the variables Ψ , we deduce that $e \equiv t$. Ψ may contain variables that occur in or are even bound in e, t . Ψ contains those variables we have seen before and want to remember. This motivates the naming of Ψ as context, as well.

Why do we need a formal definition here? We don't solve our unification problem in one huge step, but work on it incrementally, solving parts of terms and remembering the information we have learned from these parts. We want to be able to talk about these processes formally.

We formulate our constraints from a given unification problem as follows: We take each given equation and formulate a constraint K with empty context Ψ . We join them using ands: $\overline{e \equiv t}$ becomes: $\mathcal{C} = C_1 \wedge \dots \wedge C_n = \vdash e_1 \equiv t_1 \wedge \dots \wedge \vdash e_n \equiv t_n$

For clarification, $C \wedge \mathcal{C}$ is the regular logical and thus, and $\top \wedge \mathcal{C} = \mathcal{C}$ as well as $\perp \wedge \mathcal{C} = \perp$

We can also apply substitutions on a set of constraints, which just means applying the substitution to the equation part of all the constraints in the set: $\mathcal{C}\sigma = (C \wedge \mathcal{C}')\sigma = C\sigma \wedge \mathcal{C}'\sigma = \Psi \vdash e\sigma \equiv t\sigma \wedge \mathcal{C}'$. Applying a substitution to \top or \perp changes nothing.

Theorem 5.1 (Decidability of Higher-Order Unification). Higher-order unification includes unification problems containing higher-order terms (equivalent to lambda abstractions), and is covered by our introduced syntax. Higher-order unification is not decidable. This can be proven through reducing Hilbert's tenth problem to the unification problem.

6 Pattern Unification

Pattern unification, also sometimes called the pattern fragment is a subsection of Higher-Order Unification, with its solution being similarly simple as the one to first-order unification. It was described first by Miller in [4]. Since we are dealing with what amounts to an extension to the lambda calculus (as our syntax also contains constructors), we need to extend our definition to more than just function applications. This means that (in practice,) the pattern fragment described by Miller is a subset of our definition.

Definition 6.1 (Pattern). A pattern is any term p

$$p ::= \alpha^?, \beta^? \mid p.d(x_1, \dots x_n)$$

where it holds that all $x_1, \dots x_n$ are distinct variables.

If You are familiar with other definitions of patterns, You might have noticed that we have omitted the part about the variables being bound. We require this later on when looking at patterns as subterms. Some examples: $\alpha^?.\mathbf{Ap}(x).\mathbf{Ap}(y) \equiv x$ is a pattern and has the solution $[\mathbf{cocode}\{\mathbf{Ap}(x) \Rightarrow \mathbf{cocode}\{\mathbf{Ap}(y) \Rightarrow x\}\}/\alpha^?]$. $\alpha^?.fst \equiv 2$ is a pattern and has the solution $[pair(2, x)/\alpha^?]$.

Theorem 6.1 (Decidability of Pattern Unification). Pattern Unification is decidable. If there exists a solution, there also exists a mgu.

Note that first-order unification is not a subset of pattern unification. Equations containing first-order terms that don't contain patterns still remain solvable.

The reason there always exists an mgu lies in the constraint we put on our definition: All the variables must be distinct.

To illustrate this, take the problem $\alpha^?.\mathbf{Ap}(x).\mathbf{Ap}(x) \equiv x$ (where the variables are **not** distinct). We can name two solutions:

$$\begin{aligned}\sigma_1 &= [\mathbf{cocase}\{\mathbf{Ap}(x) \Rightarrow \mathbf{cocase}\{\mathbf{Ap}(y) \Rightarrow x\}\}/\alpha^?] \\ \sigma_2 &= [\mathbf{cocase}\{\mathbf{Ap}(x) \Rightarrow \mathbf{cocase}\{\mathbf{Ap}(y) \Rightarrow y\}\}/\alpha^?]\end{aligned}$$

(Intuitively, the solutions say to select the first or second argument of the function applications, respectively.) These solutions are equivalent, in that no solution is more general than the other. There exists no mgu for this problem. The solutions aren't unique because the variables aren't unique.

To be able to talk about the algorithms for solving unification problems, we need another definition:

Definition 6.2 (Normal Form). The normal form **NF** is defined as follows:

$$\begin{aligned}n &::= x \mid \alpha^? \mid n.d(\bar{v}) \mid n.\mathbf{case}\{\overline{K(\bar{x}) \Rightarrow v}\} \\ v &::= n \mid K(\bar{v}) \mid \mathbf{cocase}\{\overline{d(\bar{x}) \Rightarrow v}\}\end{aligned}$$

Terms that satisfy the n -definition are called neutral terms, v -terms are called values.

Note that these are the terms that do not contain beta-redexes. A beta-redex is a term that can be transformed using a beta-conversion.

This is apparent when one tries to construct terms containing beta-redexes in normal form: To construct the first kind of beta-redex: $K(\bar{e}).\mathbf{case}\{\dots, K(\bar{x}) \Rightarrow e\}$, we start with the term $n.\mathbf{case}\{\overline{K(\bar{x}) \Rightarrow v}\}$, now wanting to substitute $K(\bar{e})$ for n . This is not possible because we are limited to neutral terms, which constructors are not part of. Similarly with the second kind of beta-redex: $\mathbf{cocase}\{\dots, d(\bar{x}) \Rightarrow e, \dots\}.d(\bar{e})$, where we could not substitute the cocase in $n.d(\bar{e})$ because we are limited to neutral terms.

This underlines the intuition that neutral terms are terms that cannot be reduced because they contain an term we can't further evaluate (either a variable or a unification variable) in the front. Values, where we don't have this assurance cannot contain the building blocks for a beta-redex.

Some examples:

$$\begin{aligned}r &= \alpha^?.\mathbf{Ap}(\mathbf{cocase}\{\mathbf{Ap}(x) \Rightarrow x\}), \\ s &= \mathbf{cocase}\{\mathbf{Ap}(x) \Rightarrow \mathbf{Cons}(x, \mathbf{Cons}(y, \mathbf{Nil}))\}, \\ t &= \alpha^?.\mathbf{Ap}(x_1, x, y, z)\end{aligned}$$

r and s are in normal form and t is a pattern in normal form.

Theorem 6.2. If a unification problem has a solution, that solution is the same for the normal form of that same problem. No normal form of a problem that doesn't have a solution has a solution either.

From this point on, we will only be looking at terms that have a normal form. This is enough in most applications.

This is helpful for us, since we only have to consider normal forms in our algorithm, as in: Met with a term, we first reduce it to its normal form, and then solve for our solution.

As an example, the problem $\text{True.case}\{\text{True} \Rightarrow \alpha^?, \text{False} \Rightarrow 2\} \equiv 3$ has the solution $[3/\alpha^?]$, but this is more obvious after using a beta-reduction on the left-hand side bringing it into normal form:

$$\begin{aligned} \text{True.case}\{\text{True} \Rightarrow \alpha^?, \text{False} \Rightarrow 2\} &\equiv_{\beta}^1 \alpha^? \\ \implies \alpha^? &\equiv 3 \end{aligned}$$

Let's take a look at another example:

$$\begin{aligned} \alpha^? &\equiv \text{True} \\ \alpha^?.\text{case}\{\text{True} \Rightarrow 2, \text{False} \Rightarrow 3\} &\equiv \beta^? \end{aligned}$$

To find out that $[2/\beta^?]$ is the solution to the second equation, we first need to find out that $[\text{True}/\alpha^?]$ is the solution to the first equation and substitute it in the second. This is what is called *dynamic* pattern unification, where we hold off on solving some equations we don't have all the information for yet until we know more.

7 The Algorithm For Higher-Order Unification

7.1 Decomposing Constraints

It is helpful to simplify our equations a bit before starting the unification process. We do this by taking out redundant equations, spotting clearly contradictory equations or splitting our equations into smaller parts which we can further simplify and unify.

Let's look at some examples. We would like the following to be true:

Example 7.1 (Decomposing constraints-redundancy and contradiction).

$$x \vdash x.\mathbf{fst} \equiv x.\mathbf{fst} \quad \mapsto \top \quad (1)$$

$$x, y \vdash x.\mathbf{fst} \equiv y.\mathbf{fst} \quad \mapsto \perp \quad (2)$$

$$x \vdash x.\mathbf{fst} \equiv x.\mathbf{snd} \quad \mapsto \perp \quad (3)$$

$$\vdash \mathbf{Cons}(x, \mathbf{Nil}) \equiv \mathbf{Cons}(y, \mathbf{Nil}) \quad \mapsto \perp \quad (4)$$

These example might be confusing at first. Looking at the third example, one might argue that there exists a pair, say $x = \mathbf{Tup}(2, 2)$, such that $x.\mathbf{fst} = x.\mathbf{snd}$. This is where it is important to remember that we are not looking for solutions to variables like x . Whereas to our unification variables $\alpha^?$ we want to assign any term such that our equations hold, variables x add *constraints* to our equations. The equation $x \vdash x.\mathbf{fst} \equiv x.\mathbf{snd}$ must hold for *any* variable x , since we cannot choose x !

Since for $x = (2, 3)$, the equation does not hold, we can simplify to \perp .

Example 7.2 (Decomposing constraints-splitting into smaller parts).

$$\vdash \mathbf{Cons}(\alpha^?, \mathbf{Nil}) \equiv \mathbf{Cons}(\alpha^?, \mathbf{Nil}) \quad \mapsto \alpha^? \equiv \beta^? \quad (5)$$

$$x \vdash x.\mathbf{Ap}(e_1) \equiv x.\mathbf{Ap}(e_2) \quad \mapsto x \vdash e_1 \equiv e_2 \quad (6)$$

$$\vdash \mathbf{cocase}\{\mathbf{Ap}(x) \Rightarrow \alpha^?\} \equiv \mathbf{cocase}\{\mathbf{Ap}(x) \Rightarrow \beta^?\} \quad \mapsto x \vdash \alpha^? \equiv \beta^? \quad (7)$$

$$\begin{aligned} x \vdash x.\mathbf{case}\{\mathbf{T} \Rightarrow e_2, \mathbf{F} \Rightarrow e_2\} &\equiv x.\mathbf{case}\{\mathbf{T} \Rightarrow t_1, \mathbf{F} \Rightarrow t_2\}^* \\ \mapsto x \vdash e_1 &\equiv t_1 \wedge x \vdash e_2 \equiv t_2 \end{aligned} \quad (8)$$

Note that none of these examples contain redexes, meaning the only way for the terms on each side of the equations to be equivalent, is for them to be equivalent *syntactically*.

We want to formulate rules which help us simplify equations like these.

*T and F are stand-ins for True and False.

Definition 7.1 (Decomposing Constraints).

$$\Psi \vdash x \equiv x \quad \mapsto_r \top \quad (1)$$

$$\Psi \vdash \alpha^? \equiv \alpha^? \quad \mapsto_r \top \quad (2)$$

$$\begin{aligned} \circ \Psi \vdash e_1.d(\bar{e}) &\equiv e_2.d(\bar{t}) \\ \mapsto_d \Psi \vdash e_1 &\equiv e_2 \wedge \overline{\Psi \vdash e \equiv t} \end{aligned} \quad (3)$$

$$\begin{aligned} * \Psi \vdash e_1.\mathbf{case}\{\overline{K(\bar{x}) \Rightarrow e}\} &\equiv e_2.\mathbf{case}\{\overline{K(\bar{x}) \Rightarrow t}\} \\ \mapsto_d \Psi \vdash e_1 &\equiv e_2 \wedge \overline{\Psi, \bar{x} \vdash e \equiv t} \end{aligned} \quad (4)$$

$$\circ \Psi \vdash K(\bar{e}) \equiv K(\bar{t}) \quad \mapsto_d \overline{\Psi \vdash e \equiv t} \quad (5)$$

$$\Psi \vdash \mathbf{ccase}\{\overline{d(\bar{x}) \Rightarrow e.d(\bar{x})}\} \equiv t \quad \mapsto_e \Psi \vdash e \equiv t \quad (6)$$

$$* \Psi \vdash \mathbf{ccase}\{\overline{d(\bar{x}) \Rightarrow e}\} \equiv \mathbf{ccase}\{\overline{d(\bar{x}) \Rightarrow t}\} \quad \mapsto_d \overline{\Psi, \bar{x} \vdash e \equiv t} \quad (7)$$

$$\Psi \vdash \mathbf{ccase}\{\overline{d(\bar{x}) \Rightarrow e}\} \equiv t \quad \mapsto_d \overline{\Psi, \bar{x} \vdash e \equiv t.d(\bar{x})} \quad (8)$$

$$\Psi \vdash t \equiv \mathbf{ccase}\{\overline{d(\bar{x}) \Rightarrow e}\} \quad \mapsto_d \overline{\Psi, \bar{x} \vdash t.d(\bar{x}) \equiv e} \quad (9)$$

$$\text{non-matching } * \text{- or } \circ \text{-equation} \quad \mapsto_c \perp \quad (10)$$

Rules 7-9 are taken from [1], adapted to our syntax.

For equations marked with $*$, we require the constructors (or destructors) to be equal to one another in each equation. We also require them to have the same list of variables as arguments, respectively (i.e. full syntactic equality).

For equations marked with \circ , we only require the constructors (or destructors) to be equal to one another in each equation. (i.e. no syntactic equality among arguments required).

(The reason for this discrepancy lies in the fact that we are only expecting terms in normal form!) If any of this does not hold in a given equation, rule 9 applies and we simplify to \perp .

In the special case of rule 5 where the constructors have no arguments, e.g. $\mathbf{True} \equiv \mathbf{True}$, we can simplify to \top . Note that 7 (as well as 8 with being just the mirror of 7) are possible through eta-conversion:

$$\begin{aligned} \mathbf{ccase}\{\overline{d(\bar{x}) \Rightarrow e}\} &\equiv t && \equiv_\eta \\ \mathbf{ccase}\{\overline{d(\bar{x}) \Rightarrow e}\} &\equiv \mathbf{ccase}\{\overline{d(\bar{x}) \Rightarrow t.d(\bar{x})}\} && 6 \\ &\mapsto_e \overline{e \equiv t.d(\bar{x})} \end{aligned}$$

(Annotations on the right are supposed to show what rule is being used to get to the statement below.)

7.2 Unification

What do we do when we have a solution? ...

Take a look at the following unification problem:

$$\begin{aligned} \text{List}(\alpha^?) &\equiv \text{List}(\text{Int}) \\ \beta^? &\equiv \alpha^?.\text{case}\{\text{Int} \Rightarrow \text{True}\} \end{aligned}$$

I will demonstrate how we want to solve this, introducing what to do when we found a solution.

$$\begin{array}{lll} \mathcal{C} = & \vdash \text{List}(\alpha^?) \equiv \text{List}(\text{Int}) & \wedge \vdash \beta^? \equiv \alpha^?.\text{case}\{\text{Int} \Rightarrow \text{True}\} \\ \xrightarrow{(5)_d} & \vdash \alpha^? \equiv \text{Int} & \wedge \vdash \beta^? \equiv \alpha^?.\text{case}\{\text{Int} \Rightarrow \text{True}\} \\ \mapsto_s & \vdash \alpha^? \equiv \text{Int} & \wedge \vdash \beta^? \equiv \text{Int}.\text{case}\{\text{Int} \Rightarrow \text{True}\} \\ \stackrel{1}{\equiv}_{\beta} & \vdash \alpha^? \equiv \text{Int} & \wedge \vdash \beta^? \equiv \text{True} \end{array}$$

In this example, several things are expressed: When we found a solution for a unification variable, we want to keep it in our constraints, since we sometimes have to substitute already found unification variables in other equations (constraints). Doing so might introduce redexes.

Definition 7.2 (Unification).

$$e \equiv \alpha^? \qquad \mapsto_s \alpha^? \equiv e \qquad (1)$$

$$\mathcal{C} \wedge \Psi \vdash \alpha^? \equiv e \qquad \mapsto_s \mathcal{C}[e/\alpha^?] \wedge \Psi \vdash \alpha^? \equiv e \qquad (\alpha^? \notin e) \qquad (2)$$

Since substituting a solution for a unification variable in other constraints might yield a beta-redex or another simplifiable constraint, we need to continually apply decompositions and unifications to our equations.

In [2], Huet’s algorithm is described.

References

- [1] A. Abel and B. Pientka. Higher-order dynamic pattern unification for dependent types and records. In *Proceedings of the 10th International Conference on Typed Lambda Calculi and Applications*, TLCA’11, page 10–26, Berlin, Heidelberg, 2011. Springer-Verlag.
- [2] G. Dowek. Higher-order unification and matching. In J. A. Robinson and A. Voronkov, editors, *Handbook of Automated Reasoning (in 2 volumes)*, pages 1009–1062. Elsevier and MIT Press, 2001.
- [3] A. Martelli and U. Montanari. An efficient unification algorithm. *ACM Trans. Program. Lang. Syst.*, 4(2):258–282, Apr. 1982.
- [4] D. MILLER. A Logic Programming Language with Lambda-Abstraction, Function Variables, and Simple Unification. *Journal of Logic and Computation*, 1(4):497–536, 09 1991.

Selbständigkeitserklärung

Hiermit versichere ich, dass ich die vorliegende Bachelorarbeit selbständig und nur mit den angegebenen Hilfsmitteln angefertigt habe und dass alle Stellen, die dem Wortlaut oder dem Sinne nach anderen Werken entnommen sind, durch Angaben von Quellen als Entlehnung kenntlich gemacht worden sind. Diese Bachelorarbeit wurde in gleicher oder ähnlicher Form in keinem anderen Studiengang als Prüfungsleistung vorgelegt.

Ort, Datum

Unterschrift