Higher-Order unification for free!

Reusing the meta-language unification for the object language

Davide Fissore
davide.fissore@inria.fr
Université Côte d'Azur, Inria
France

Enrico Tassi
enrico.tassi@inria.fr
Université Côte d'Azur, Inria
France

ABSTRACT

Specifying and implementing a proof system from scratch requires significant effort. Logical Frameworks and Higher Order Logic Programming Languages provide dedicated, high-level meta languages to facilitate this task in two ways: 1) variable binding and substitution are for free when meta language binders represent object logic ones; 2) proof construction, and proof search, are greatly simplified by leveraging the unification procedure provided by the meta language. Notable examples of meta languages are Elf [19], Twelf [21], λProlog [14], Beluga [22], Abella [8] and Isabelle [28] which have been used to implement or specify many formal systems such as First Order Logic [5], Set Theory [18], Higher Order Logic [17], and the Calculus of Constructions [4].

The object logic we are interested in is Coq's type theory [26]. We aim to develop a higher-order unification-based proof search procedure using the meta language Elpi [3], a dialect of λProlog. Elpi's equational theory includes $\eta\beta$-equivalence and features a higher-order unification procedure $\simeq_\lambda$ for the pattern fragment [13]. Elpi offers an encoding of Coq terms suitable for meta programming [25, 24, 9, 6] but that restricts $\simeq_\lambda$ to first-order unification problems only. We refer to this basic encoding as $\mathcal{F}$.

In this paper we propose a more well-behaved encoding called $\mathcal{H}$, and show how to translate unification problems from $\mathcal{F}$ to corresponding ones in $\mathcal{H}$. Consequently, we derive $\simeq_o$, the higher-order unification procedure of $\mathcal{F}$ that honours $\eta\beta$-equivalence (for Coq functions), addresses problems within the pattern fragment, and allows for the use of heuristics to deal with problems outside the pattern fragment. Moreover, as $\simeq_o$ delegates most of the work to $\simeq_\lambda$, it can be used to efficiently simulate a logic program in $\mathcal{F}$ by taking advantage of unification-related optimizations of the meta language, such as clause indexing.

KEYWORDS

Logic Programming, Meta-Programming, Higher-Order Unification

ACM Reference Format:
Davide Fissore and Enrico Tassi. 2024. Higher-Order unification for free!: Reusing the meta-language unification for the object language. In . ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

Conference'17, July 2017, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM
https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

We aim to implement a form of proof search known as type-class resolution [27, 23] for the Coq's system [26]. Type-class solvers are unification based proof search procedures reminiscent of Prolog, which back-chain lemmas taken from a database of "type-class instances". Given this analogy with Logic Programming we want to leverage the Elpi meta-programming language [25], a dialect of λProlog, already used to extend Coq in various ways [25, 24, 9, 6].

The use of a meta language facilitates the implementation of a proof system in two key ways. The first and most well-know one is that variable binding and substitution come for free. The second one is that these meta languages come equipped with some form of unification, a cornerstone of proof construction and proof search. In this paper we focus on this last aspect of the implementation of a Prolog-like proof system, precisely *how to reuse the higher-order unification procedure of the meta language in order to simulate a higher-order logic program for the object language.*

We take as an example the `Decision` and `Finite` type classes from the Stdpp library [12]. The class `Decision` identifies predicates equipped with a decision procedure, while `Finite` identifies types whose inhabitants can be enumerated in a (finite) list. The following three type-class instances state that: 1) the type of natural numbers smaller than `n`, called `fin n`, is finite; 2) the predicate `nfact n nf`, relating a natural number `n` to the number of its prime factors `nf`, is decidable; 3) the universal closure of a predicate has a decision procedure if its domain is finite and if the predicate is decidable.

```
Instance fin_fin: ∀n, Finite (fin n).                    (* r1 *)
Instance nfact_dec: ∀n nf, Decision (nfact n nf). (* r2 *)
Instance forall_dec: ∀A P, Finite A →                    (* r3 *)
  ∀x:A, Decision (P x) → Decision (∀x:A, P x).
```

Given this database, a type-class solver is expected to prove the following statement automatically:

```
Decision (∀x: fin 7, nfact x 3)                          (* g *)
```

The proof found by the solver back-chains on rule 3 (the only rule about the ∀ quantifier), and then solves the premises with rules 1 and 2 respectively. Note that rule 3 features a second-order parameter `P` that represents a function of type `A → Prop` (a 1-argument predicate over `A`). The solver has to infer a value for `P` by unifying the conclusion of rule 3 with the goal, and in particular, it has to solve the unification problem `P x = nfact x 3`. This higher-order problem falls in the so-called pattern fragment and admits a unique solution ρ that assigns the term λ`x.nfact x 3` to `P`. In the rest of this paper shall refer to the pattern fragment as $\mathcal{L}$ [13].

In order to implement such a search in Elpi, we shall describe the encoding of Coq terms and then the encoding of instances as rules. Elpi comes equipped with an Higher Order Abstract Syntax

(HOAS [20]) datatype of terms, called `tm`, that includes (among others) the following constructors:

```
type lam  tm -> (tm -> tm) -> tm.     % lambda abstraction
type app  list tm -> tm.              % n-ary application
type all  tm -> (tm -> tm) -> tm.     % forall quantifier
type con  string -> tm.               % constants
```

Following the standard syntax of λProlog [14], the meta-level binding of a variable `x` in an expression `e` is written as «`x\ e`», while square brackets delimit a list of terms separated by comma. For example, the term «`∀y:t, nfact y 3`» is encoded as follows:

```
all (con"t") y\ app [con"nfact", y, con"3"]
```

We now illustrate a naive encoding of the three instances above as higher-order logic programming rules: capital letters denote rule parameters; `:-` separates the rule's head from the premises, and «`pi w\ p`» introduces a fresh nominal constant `w` for the premise `p`.

```
finite   (app [con"fin", N]).                          (r1)
decision (app [con"nfact", N, NF]).                    (r2)
decision (all A x\ app [P, x]) :- finite A,            (r3)
  pi w\ decision (app [P, w]).
```

Unfortunately this encoding of rule ($r3$) does not work since it uses the predicate `P` as a first order term: for the meta language its type is `tm`. If we try to back-chain the rule ($r3$) on the encoding of the goal (g) given below

```
decision (all (app [con"fin", con"7"]) x\              (g)
  app [con"nfact", x, con"3"]).
```

we obtain an unsolvable unification problem (p): the two lists of terms have different lengths!

```
app [con"nfact", x, con"3"] = app [P, x]               (p)
```

The problem above has no solution in a first-order language where `P` can only stand for a predicate symbol, while in a higher-order language `P` can stand for any 1-argument predicate.

In this paper we study a more sophisticated encoding of Coq terms and rules that, on a first approximation, would reshape ($r3$) as follows:

```
decision (all A x\ Pm x) :- link Pm P A, finite A,     (r3′)
  pi x\ decision (app [P, x]).
```

Since `Pm` is a higher-order unification variable of type `tm -> tm`, with `x` in its scope, the unification problem (p') admits one solution:

```
app [con"nfact", x, con"3"] = Pm x                     (p′)
Pm = x\ app [con"nfact", x, con"3"]                    (σ)
```

Once the head of rule ($r3'$) unifies with the goal (g), the premise «`link Pm A P`» brings the assignment (σ) back to the domain `tm` of Coq terms, obtaining the expected solution ρ:

```
P = lam A x\ app [con"nfact", x, con"3"]
```

This simple example is sufficient to show that the encoding we seek is not trivial and does not only concern the head of rules, but the entire sequence of unification problems that constitute the execution of a logic program. In fact the solution for `P` above generates a (Coq) β-redex in the second premise (the predicate under the `pi w\`).

In turn, this redex prevents rule ($r2$) from backchaining properly since the following unification problem has no solution:

```
app [ lam A (a\ app [con"nfact", a, con"3"]) , x] =
app [ con"nfact"                             , N, NF]
```

The root cause of the problems we outlined in this example is a subtle mismatch between the equational theories of the meta language and the object language, which in turn makes the unification procedures of the meta language weak. The equational theory of the meta language Elpi encompasses $\eta\beta$-equivalence and its unification procedure can solve higher-order problems in the pattern fragment. Although the equational theory of Coq is much richer, for efficiency and predictability reasons, automatic proof search procedures typically employ a unification procedure that only captures a $\eta\beta$-equivalence and only operates in $\mathcal{L}$. The similarity is striking, but one needs to exercise some caution in order to simulate a higher-order logic program in Coq using the unification of Elpi.

Contributions. In this paper we identify a minimal language $\mathcal{F}$ in which the problems sketched in the introduction can be formally described. We detail an encoding of a logic program in $\mathcal{F}$ to a strongly related logic program in $\mathcal{H}$ (the language of the meta-language) and we show that the higher-order unification procedure of the meta language $\simeq_\lambda$ can be efficiently used to simulate a higher-order unification procedure $\simeq_o$ for the object language that features $\eta\beta$-conversion. We show how $\simeq_o$ can be extended with heuristics to deal with problems outside the pattern fragment.
Section 2 states the problem formally and gives the intuition behind our solution; section 3 sets up a basic simulation of first-order logic programs, section 4 and section 5 extend it to higher-order logic programs in the pattern fragment while section 7 goes beyond the pattern fragment. Section 8 discusses the implementation in Elpi.
The λProlog code discussed in the paper can be accessed at the address https://github.com/FissoreD/ho-unif-for-free.

2 PROBLEM STATEMENT AND SOLUTION

Even if we encountered the problem working on Coq's Calculus of Inductive Constructions, we devise a minimal setting to ease its study. In this setting, we have a $\mathcal{F}$ language (for first order) with a rich equational theory and a $\mathcal{H}$ meta language with a simpler one.

2.1 Preliminaries: $\mathcal{F}$ and $\mathcal{H}$

To reason about unification, we provide a description of the $\mathcal{F}$ and $\mathcal{H}$ languages where unification variables are first-class terms, i.e. they have a concrete syntax as shown in fig. 1. Unification variables in $\mathcal{F}$ (`fuva` term constructor) have no explicit scope: the arguments of a higher-order variable are given via the `fapp` constructor. For example the term «`P x`» is represented as «`fapp [fuva N, x]`», where `N` is the memory address of `P` and `x` is a bound variable.
In $\mathcal{H}$, the representation of «`P x`» is instead «`uva N [x]`», since unification variables are higher-order and come equipped with an explicit scope.

```
kind fm type.                    kind tm  type.
type fapp list fm -> fm.         type app list tm -> tm.
type flam (fm -> fm) -> fm.      type lam (tm -> tm) -> tm.
type fcon string -> fm.          type con string -> tm.
type fuva addr -> fm.            type uva addr -> list tm -> tm.
```

Figure 1: The $\mathcal{F}$ and $\mathcal{H}$ languages

Notational conventions. When we write $\mathcal{H}$ terms outside code blocks we follow the usual λ-calculus notation, reserving f, g, a, b for constants, x, y, z for bound variables and X, Y, Z, F, G, H for unification variables. However, we need to distinguish between the "application" of a unification variable to its scope and the application of a term to a list of arguments. We write the scope of unification variables in subscript while we use juxtaposition for regular application. Here are few examples:

$f\ a$	`app [con "f", con "a"]`
$\lambda x.\lambda y.F_{x\,y}$	`lam x\ lam y\ uva F [x, y]`
$\lambda x.F_x\ a$	`lam x\ app [uva F [x], con "a"]`
$\lambda x.F_x\ x$	`lam x\ app [uva F [x], x]`

When it is clear from the context, we shall use the same syntax for $\mathcal{F}$ terms (although we never subscripts unification variables). We use $s, s_1, \ldots$ for terms in $\mathcal{F}$ and $t, t_1, \ldots$ for terms in $\mathcal{H}$.

2.2 Equational theories an unification

2.2.1 Term equality: $=_o$ and $=_\lambda$. For both languages, we extend the equational theory over ground terms to the full language by adding the reflexivity for unification variables (a variable is equal to itself).

The first four rules are common to both equalities and define the usual congruence over terms. Since we use an HOAS encoding, they also capture α-equivalence. In addition to that, $=_o$ has rules for η and β-equivalence.

```
type (=o) fm -> fm -> o.                                   (=o)
fcon X =o fcon X.
fapp A =o fapp B :- forall2 (=o) A B.
flam F =o flam G :- pi x\ x =o x => F x =o G x.            (λλ)
fuva N =o fuva N.
flam F =o T :-                                             (ηl)
  pi x\ beta T [x] (T' x), x =o x => F x =o T' x.
T =o flam F :-                                             (ηr)
  pi x\ beta T [x] (T' x), x =o x => T' x =o F x.
fapp [flam X | L] =o T :- beta (flam X) L R, R =o T.      (βl)
T =o fapp [flam X | L] :- beta (flam X) L R, T =o R.      (βr)

type (=λ) tm -> tm -> o.
con C =λ con C.
app A =λ app B :- forall2 (=λ) A B.
lam F =λ lam G :- pi x\ x =λ x => F x =λ G x.
uva N A =λ uva N B :- forall2 (=λ) A B.
```

Note that the symbol `|` separates the head of a list from the tail, that `forall2` applies a binary predicate to two lists (of the same length). Finally `=>` is λProlog syntax to augment the current program with an extra rule, and both procedures use it to assume that the fresh nominal constants introduces by `pi` are equal to themselves.

The main point in showing these equality tests is to remark how weaker $=_\lambda$ is, and to identify the four rules that need special treatment in the implementation of $\simeq_o$. For brevity, we omit the code of `beta`: it is sufficient to know that «`beta F L R`» computes in `R` the weak head normal form of «`app [F|L]`».

Substitution: ρs and σt. We write $\sigma = \{\ X \mapsto t\ \}$ for the substitution that assigns the term t to the variable X. We write σt for the application of the substitution to a term t, and $\sigma X = \{\ \sigma t \mid t \in X\ \}$ when X is a set of terms. We write $\sigma \subseteq \sigma'$ when σ is more general than σ'. We shall use ρ for $\mathcal{F}$ substitutions, and σ for the $\mathcal{H}$ ones. For brevity, in this section, we consider the substitution for $\mathcal{F}$ and $\mathcal{H}$ identical. We defer to section 3.1 a more precise description pointing out their differences.

Term unification: $\simeq_o$ vs. $\simeq_\lambda$. $\mathcal{H}$'s unification signature is:

```
type (≃λ) tm -> tm -> subst -> subst -> o.
```

We write $\sigma t_1 \simeq_\lambda \sigma t_2 \mapsto \sigma'$ when σt_1 and σt_2 unify with substitution σ'. Note that σ' is a refined (i.e. extended) version of σ; this is reflected by the signature above that relates two substitutions. We write $t_1 \simeq_\lambda t_2 \mapsto \sigma'$ when the initial substitution σ is empty. We write $\mathcal{L}$ as the set of terms that are in the pattern-fragment, i.e. every higher-order variable is applied to a list of distinct names.

The specification of a "good" unification procedure restricted to a domain $\mathcal{D}$ is the following:

Proposition 2.1 (Good unification). *A good unification $\simeq$ for equality $=$ in the domain $\mathcal{D}$ satisfies the following properties:*

$$\{\ t_1,\ t_2\ \} \subseteq \mathcal{D} \Rightarrow t_1 \simeq t_2 \mapsto \rho \Rightarrow \rho t_1 = \rho t_2 \quad (1)$$

$$\{\ t_1,\ t_2\ \} \subseteq \mathcal{D} \Rightarrow \rho t_1 = \rho t_2 \Rightarrow \exists \rho', t_1 \simeq t_2 \mapsto \rho' \wedge \rho' \subseteq \rho \quad (2)$$

The meta language of choice is expected to provide an implementation of $\simeq_\lambda$ that is a good unification for $=_\lambda$ in $\mathcal{L}$.

Even if we provide an implementation of the object-language unification $\simeq_o$ in section 3.6, our real goal is the simulation of an entire logic program.

2.3 The problem: logic-program simulation

We represent a logic program *run* in $\mathcal{F}$ as a sequence of *steps* of length $\mathcal{N}$. At each step p we unify two terms, $\mathbb{P}_{p_l}$ and $\mathbb{P}_{p_r}$, taken from the list of all unification problems $\mathbb{P}$. The composition of these steps starting from the empty substitution ρ_0 produces the final substitution $\rho_\mathcal{N}$, which is the result of the logic program execution.

$$\text{fstep}(\mathbb{P}, p, \rho) \mapsto \rho' \stackrel{def}{=\!=} \rho\mathbb{P}_{p_l} \simeq_o \rho\mathbb{P}_{p_r} \mapsto \rho'$$

$$\text{frun}(\mathbb{P}, \mathcal{N}) \mapsto \rho_\mathcal{N} \stackrel{def}{=\!=} \bigwedge_{p=1}^{\mathcal{N}} \text{fstep}(\mathbb{P}, p, \rho_{p-1}) \mapsto \rho_p$$

In order to simulate a $\mathcal{F}$ logic program in $\mathcal{H}$, we compile each $\mathcal{F}$ term s in $\mathbb{P}$ to a $\mathcal{H}$ term t. We write this translation as $\langle s \rangle \mapsto (t, m, l)$. The implementation of the compiler is detailed in sections 3, 5 and 7, here we just point out that it additionally produces a variable map m and a list of links l. The variable map connects unification variables in $\mathcal{H}$ to variables in $\mathcal{F}$ and is used to "decompile" the assignment, $\langle \sigma, m, l \rangle^{-1} \mapsto \rho$. Links are an accessory piece of information whose description is deferred to section 2.4. We write $\mathbb{P}_p = \{\ \mathbb{P}_{p_l}, \mathbb{P}_{p_r}\ \}$ and $s \in \mathbb{P} \Leftrightarrow \exists p, s \in \mathbb{P}_p$.

We simulate each run in $\mathcal{F}$ with a run in $\mathcal{H}$ as follows:

$$\text{hstep}(\mathbb{T}, p, \sigma, \mathbb{L}) \mapsto (\sigma'', \mathbb{L}') \stackrel{def}{=\!=}$$
$$\sigma\mathbb{T}_{p_l} \simeq_\lambda \sigma\mathbb{T}_{p_r} \mapsto \sigma' \wedge \text{progress}(\mathbb{L}, \sigma') \mapsto (\mathbb{L}', \sigma'')$$

$$\text{hrun}(\mathbb{P}, \mathcal{N}) \mapsto \rho_\mathcal{N} \stackrel{def}{=\!=}$$
$$\mathbb{T} \times \mathbb{M} \times \mathbb{L}_0 = \{(t, m, l) | s \in \mathbb{P}, \langle s \rangle \mapsto (t, m, l)\}$$
$$\bigwedge_{p=1}^{\mathcal{N}} \text{hstep}(\mathbb{T}, p, \sigma_{p-1}, \mathbb{L}_{p-1}) \mapsto (\sigma_p, \mathbb{L}_p)$$
$$\langle \sigma_\mathcal{N}, \mathbb{M}, \mathbb{L}_\mathcal{N} \rangle^{-1} \mapsto \rho_\mathcal{N}$$

By analogy with $\mathbb{P}$, we write $\mathbb{T}_{p_l}$ and $\mathbb{T}_{p_r}$ for the two $\mathcal{H}$ terms being unified at step p, and we write $\mathbb{T}_p$ for the set $\{ \mathbb{T}_{p_l}, \mathbb{T}_{p_r} \}$.
hstep is made of two sub-steps: a call to the meta language unification and a check for progress on the set of links, that intuitively will compensate for the weaker equational theory honored by $\simeq_\lambda$.
hrun compiles all terms in $\mathbb{P}$, then executes each step, and finally decompiles the solution. We claim:

Proposition 2.2 (Run equivalence). $\forall \mathbb{P}, \forall \mathcal{N}$, *if* $\mathbb{P} \subseteq \mathcal{L}$

$$\text{frun}(\mathbb{P}, \mathcal{N}) \mapsto \rho_{\mathcal{N}} \Leftrightarrow \text{hrun}(\mathbb{P}, \mathcal{N}) \mapsto \rho_{\mathcal{N}}$$

That is, the two executions give the same result if all terms in $\mathbb{P}$ are in the pattern fragment. Moreover:

Proposition 2.3 (Simulation fidelity). *In the context of* hrun, *if* $\mathbb{P} \subseteq \mathcal{L}$ *we have that* $\forall p \in 1 \ldots \mathcal{N}$,

$$\text{fstep}(\mathbb{P}, p, \rho_{p-1}) \mapsto \rho_p \Leftrightarrow \text{hstep}(\mathbb{T}, p, \sigma_{p-1}, \mathbb{L}_{p-1}) \mapsto (\sigma_p, \mathbb{L}_p)$$

In particular, this property guarantees that a *failure* in the $\mathcal{F}$ run is matched by a failure in $\mathcal{H}$ *at the same step*. We consider this property very important from a practical point of view since it guarantees that the execution traces are strongly related, and in turn, this enables a user to debug a logic program in $\mathcal{F}$ by looking at its execution trace in $\mathcal{H}$.

We also claim that hrun handles terms outside $\mathcal{L}$ in the following sense:

Proposition 2.4 (Fidelity recovery). *In the context of* hrun, *if* $\rho_{p-1}\mathbb{P}_p \in \mathcal{L}$ *(even if* $\mathbb{P}_p \notin \mathcal{L}$*) then*

$$\text{fstep}(\mathbb{P}, p, \rho_{p-1}) \mapsto \rho_p \Leftrightarrow \text{hstep}(\mathbb{T}, p, \sigma_{p-1}, \mathbb{L}_{p-1}) \mapsto (\sigma_p, \mathbb{L}_p)$$

In other words, if the two terms involved in a step re-enter $\mathcal{L}$, then hstep and fstep are again related, even if $\mathbb{P} \notin \mathcal{L}$ and hence proposition 2.3 does not apply. Indeed, the main difference between proposition 2.3 and proposition 2.4 is that the assumption of the former is purely static, it can be checked upfront. When this assumption is not satisfied, one can still simulate a logic program and have guarantees of fidelity if, at run time, decidability of higher-order unification is restored.

This property has practical relevance since in many logic programming implementations, including Elpi, the order in which unification problems are tackled does matter. The simplest example is the sequence $F \simeq \lambda x.a$ and $F\ a \simeq a$: the second problem is not in $\mathcal{L}$ and has two unifiers, namely $\sigma_1 = \{ F \mapsto \lambda x.x \}$ and $\sigma_2 = \{ F \mapsto \lambda x.a \}$. The first problem picks σ_2, making the second problem re-enter $\mathcal{L}$.

Backtracking. We omit it from our model of a logic-program execution since it plays a very minor role, orthogonal to higher-order unification. We point out that each *run* corresponds to a (proof search) branch in the logic program that either fails at some point, or succeeds. A computation that succeeds by backtracking, exploring multiple branches, could be modeled as a set of runs with (possibly non-empty) common prefixes.

2.4 The solution (in a nutshell)

A term s is compiled to a term t where every "problematic" sub term p is replaced by a fresh unification variable h with an accessory *link* that represents a suspended unification problem $h \simeq_\lambda p$. As a result $\simeq_\lambda$ is "well behaved" on t, in the sense that it does not contradict $=_o$ as it would otherwise do on the "problematic" sub-terms.
We now define "problematic" and "well behaved" more formally We use the $\diamond$ symbol since it stands for "possibly" in modal logic and all problematic terms are characterized by some "uncertainty".

Definition 2.5 ($\diamond\beta$). $\diamond\beta$ is the set of terms of the form $X\ x_1 \ldots x_n$ such that $x_1 \ldots x_n$ are distinct names (of bound variables).

An example of a $\diamond\beta$ term is the application $F\ x$. This term is problematic since the application node of its syntax tree cannot be used to justify a unification failure, i.e. by properly instantiating F the term head constructor may become a λ, or a constant, or remain an application.

Definition 2.6 ($\diamond\eta$). $\diamond\eta$ is the set of terms s such that $\exists \rho, \rho s$ is an eta expansion.

An example of a term s in $\diamond\eta$ is $\lambda x.\lambda y.F\ y\ x$ since the substitution $\rho = \{F \mapsto \lambda a.\lambda b.f\ b\ a\}$ makes $\rho s = \lambda x.\lambda y.f\ x\ y$, which is the eta long form of f. This term is problematic since its leading λ abstraction cannot justify a unification failure against a constant f.

Definition 2.7 ($\diamond\mathcal{L}$). $\diamond\mathcal{L}$ is the set of terms of the form $X\ t_1 \ldots t_n$ such that $t_1 \ldots t_n$ are not distinct names.

These terms are problematic for the very same reason terms in $\diamond\beta$ are, but they cannot be handled directly by the unification of the meta language, which is only required to handle terms in $\mathcal{L}$. Still, there exists a substitution ρ such that $\rho s \in \mathcal{L}$.

We write $\mathcal{P}(t)$ the set of sub-terms of t, and we write $\mathcal{P}(X) = \bigcup_{t \in X} \mathcal{P}(t)$ when X is a set of terms.

Definition 2.8 (Well behaved set). Given a set of terms $X \subseteq \mathcal{H}$,

$$\mathcal{W}(X) \Leftrightarrow \forall t \in \mathcal{P}(X), t \notin (\diamond\beta \cup \diamond\eta \cup \diamond\mathcal{L})$$

We write $\mathcal{W}(t)$ as a short for $\mathcal{W}(\{t\})$. We claim our compiler validates the following property:

Proposition 2.9 ($\mathcal{W}$-enforcing). *Given a term* s *in* $\mathcal{F}$,

$$\langle s \rangle \mapsto (t, m, l) \Rightarrow \mathcal{W}(t)$$

Proposition 2.10 (compiler-useful). *Given two terms* s_1 *and* s_2, *if* $\exists \rho, \rho s_1 =_o \rho s_2$, *then*

$$\langle s_i \rangle \mapsto (t_i, m_i, l_i) \text{ for } i \in \{1, 2\} \Rightarrow t_1 \simeq_\lambda t_2 \mapsto \sigma$$

In other words the compiler outputs terms in $\mathcal{W}$, even if its input is not. And if two terms can unify in the source language then these terms also unify in the target language. Note that the property holds for any substitution, ρ could be given by an oracle and/or not necessarily be a most general one: when applied to terms in $\mathcal{W}$, $\simeq_\lambda$ does not contradict $=_o$. Also note that a compiler that translate all terms to unification variables would satisfy this property, but wound fail to verify proposition 2.3.

Proposition 2.11 ($\mathcal{W}$-preservation). $\forall \mathbb{T}, \forall \mathbb{L}, \forall p, \forall \sigma, \forall \sigma'$

$$\mathcal{W}(\sigma\mathbb{T}) \wedge \sigma\mathbb{T}_{p_l} \simeq_\lambda \sigma\mathbb{T}_{p_r} \mapsto \sigma' \Rightarrow \mathcal{W}(\sigma'\mathbb{T})$$
$$\mathcal{W}(\sigma\mathbb{T}) \wedge \text{progress}(\mathbb{L}, \sigma) \mapsto (\_, \sigma') \Rightarrow \mathcal{W}(\sigma'\mathbb{T})$$

Proposition 2.11 is key to proving propositions 2.2 and 2.3. Informally, it says that the problematic terms moved on the side by the compiler are not reintroduced by hstep, hence $\simeq_\lambda$ can continue to

operate properly. In sections 3, 5 and 7 we describe how to recognize terms in $\diamond\beta$, $\diamond\eta$ and $\diamond\mathcal{L}$ and how progress takes care of them preserving $\mathcal{W}$ and ensuring propositions 2.2 to 2.4.

3 BASIC COMPILATION AND SIMULATION

3.1 Memory map ($\mathbb{M}$) and substitution (ρ and σ)

Unification variables are identified by a (unique) memory address. The memory and its associated operations are described below:

```
typeabbrev (mem A) (list (option A)).
type set? addr -> mem A -> A -> o.
type unset? addr -> mem A -> o.
type assign addr -> mem A -> A -> mem A -> o.
type new mem A -> addr -> mem A -> o.
```

If a memory cell is `none`, then the corresponding unification variable is not set. `assign` sets an unset cell to the given value, while `new` finds the first unused address and sets it to `none`.

Since each $\mathcal{H}$ unification variable occurs together with a scope, its assignment needs to be abstracted over it to enable the instantiation of the same assignment to different scopes. This is expressed by the `inctx` container, and in particular its `abs` binding constructor.

```
kind inctx type -> type.                                   (· ⊢ ·)
type abs (tm -> inctx A) -> inctx A.
type val A -> inctx A.
typeabbrev assignment (inctx tm).
typeabbrev subst (mem assignment).
```

A solution to a $\mathcal{F}$ variable is a plain term, that is `fsubst` is an abbreviation for `mem fm`.

The compiler establishes a mapping between variables of the two languages.

```
kind fvariable type.
type fv addr -> fvariable.
kind hvariable type.
type hv addr -> arity -> hvariable.
kind mapping type.
type (<->) fvariable -> hvariable -> mapping.
typeabbrev mmap (list mapping).
```

Each `hvariable` is stored in the mapping together with its arity (a number) so that the code of (*malloc*) below can preserve:

Invariant 1 (Unification-variable arity). *Each variable* `A` *in* $\mathcal{H}$ *has a (unique) arity* `N` *and each occurrence* `(uva A L)` *is such that* `L` *has length* `N`.

```
type m-alloc fvariable -> hvariable -> mmap -> mmap ->
  subst -> subst -> o.                                     (malloc)
m-alloc Fv Hv M M S S :- mem M (Fv <-> Hv), !.
m-alloc Fv Hv M [Fv <-> Hv|M] S S1 :- Hv = hv N _, new S N S1.
```

When a single `fvariable` occurs multiple times with different numbers of arguments, the compiler generates multiple mappings for it, on a first approximation, and then ensures the mapping are bijective by introducing η-`link`; this detail is discussed in section 6.

It is worth examining the code of `deref`, which applies the substitution to a $\mathcal{H}$ term. Notice how assignments are moved to the current scope, i.e. the `abs`-bound variables are renamed with the names in the scope of the unification variable occurrence.

```
type deref subst -> tm -> tm -> o.                         (σt)
deref _ (con C) (con C).
deref S (app A) (app B) :- map (deref S) A B.
deref S (lam F) (lam G) :-
  pi x\ deref S x x => deref S (F x) (G x).
deref S (uva N L) R :- set? N S A,
  move A L T, deref S T R.
deref S (uva N A) (uva N B) :- unset? N S,
  map (deref S) A B.
```

Note that `move` strongly relies on invariant 1: the length of the arguments of all occurrences of a unification variable is the same. Hence, they have the same simple type for the meta-level, and therefore the number of `abs` nodes in the assignment matches that length. This guarantees that `move` never fails.

```
type move assignment -> list tm -> tm -> o.
move (abs Bo) [H|L] R :- move (Bo H) L R.
move (val A)  []  A :- !.
```

We write $\sigma = \{\, A_{xy} \mapsto y \,\}$ for the assignment «`abs x\abs y\y `» and $\sigma = \{\, A \mapsto \lambda x.\lambda y.y \,\}$ for «`lam x\lam y\y `».

3.2 Links ($\mathbb{L}$)

As mentioned in section 2.4, the compiler replaces terms in $\diamond\eta$, $\diamond\beta$, and $\diamond\mathcal{L}$ with fresh variables linked to the problematic terms. Terms in $\diamond\beta$ do not need a link since $\mathcal{H}$ variables faithfully represent the problematic term thanks to their scope.

```
kind baselink type.
type link-eta  tm -> tm -> baselink.
type link-llam tm -> tm -> baselink.
typeabbrev link (inctx baselink).
typeabbrev links (list link).
```

The right-hand side of a link, the problematic term, can occur under binders. To accommodate this situation, the compiler wraps `baselink` using the `inctx` container (see $\cdot \vdash \cdot$ also used for `subst`).

Invariant 2 (Link left hand side). *The left-hand side of a suspended link is a variable.*

New links are suspended by construction. If the left-hand side is assigned during a step, then the link is considered for progress and possibly eliminated. This is discussed in section 5 and section 7.

When detailing examples, we represent links as equations between two terms under a context. The equality sign is subscripted with the kind of `baselink`. For example $x \vdash A_x =_{\mathcal{L}} F_x\ a$ corresponds to:

```
abs x\ val (link-llam (uva A [x]) (app[uva F [x],con "a"]))
```

3.3 Compilation

The simple compiler described in this section serves as a basis for the extensions in sections 4, 5 and 7. Its main task is to beta normalize the term and map one syntax tree to the other. In order to bring back the substitution from $\mathcal{H}$ to $\mathcal{F}$ the compiler builds a "memory map" connecting the $\mathcal{F}$ variables to the $\mathcal{H}$ ones using (*malloc*).

The signature of the `comp` predicate below allows for the generation of links (suspended unification problems), which play no role

in this section but play a major role in sections 4, 5 and 7. With respect to section 2, the signature also allows for updates to the substitution.

```
type comp fm -> tm -> mmap -> mmap -> links -> links ->
  subst -> subst -> o.
comp (fcon C) (con C) M M L L S S.
comp (flam F) (lam F1) M1 M2 L1 L2 S1 S2 :-                (c_λ)
  comp-lam F F1 M1 M2 L1 L2 S1 S2.
comp (fuva A) (uva B []) M1 M2 L L S1 S2 :-
  m-alloc (fv A) (hv B (arity z)) M1 M2 S1 S2.
comp (fapp A) (app A1) M1 M2 L1 L2 S1 S2 :-                (c_@)
  fold6 comp A A1 M1 M2 L1 L2 S1 S2.

type compile fm -> tm -> mmap -> mmap ->  links -> links ->
  subst -> subst -> o.
compile F G M1 M2 L1 L2 S1 S2 :-
  beta-normal F F', comp F' G M1 M2 L1 L2 S1 S2.
```

The code above uses that possibility in order to allocate space for the variables, i.e. it sets their memory address to `none` (a detail not worth mentioning in the previous sections).

```
type comp-lam (fm -> fm) -> (tm -> tm) ->
  mmap -> mmap -> links -> links -> subst -> subst -> o.
comp-lam F G M1 M2 L1 L3 S1 S2 :-
  pi x y\ (pi M L S\ comp x y M M L L S S) =>              (H_λ)
    comp (F x) (G y) M1 M2 L1 (L2 y) S1 S2,
  close-links L2 L3.
```

In the code above, the syntax `pi x y\..` is syntactic sugar for iterated `pi` abstraction, as in `pi x\ pi y\...`. The auxiliary predicate `fold6` folds a predicate with three accumulators (the memory map, the links and the substitution) over a lists to obtain a new list and the final values of the accumulators.

The auxiliary function `close-links` tests if the bound variable `v` really occurs in the link. If it does, the link is wrapped into an additional `abs` node binding `v`. In this way links generated deep inside the compiled terms can be moved outside their original context of binders.

```
type close-links (tm -> links) -> links -> o.
close-links (v\[X v|L v]) [abs X|R] :- close-links L R.
close-links (_\[]) [].
```

3.4 Execution

A step in $\mathcal{H}$ consists of unifying two terms and reconsidering all links for progress. If either of these tasks fails, we consider the entire step to fail. It is at this granularity that we can relate steps in the two languages.

```
type hstep tm -> tm -> links -> links -> subst -> subst -> o.
hstep T1 T2 L1 L2 S1 S3 :-
  (T1 ≃λ T2) S1 S2,
  progress L1 L2 S2 S3.
```

Note that the infix notation `((A ≃λ B) C D)` is syntactic sugar for `((≃λ) A B C D)`.

Reconsidering links is a fixpoint process because the progress of a link can update the substitution, which may then enable another link to progress.

```
type progress links -> links -> subst -> subst -> o.
progress L L3 S S3 :-
  progress1 L L1 S S1,
  occur-check-links L1,
  scope-check L1 L2 S1 S2
  if (L = L2, S = S2)
     (L3 = L2, S3 = S2)
     (progress L2 L3 S2 S3).
```

3.4.1 Progress. In the base compilation scheme, `progress1` is the identity function on both the links and the substitution, so the fixpoint trivially terminates. Sections 5 and 7 add rules to `progress1` and explain why the don't hinder termination.

3.4.2 Scope check. The predicate `scope-check` walks through all links. Each link of the form $\Gamma \vdash X_{x_1 \dots x_n} =_\eta t$ is replaced by $x_1 \dots x_n \vdash X_{x_1 \dots x_n} =_\eta t'$ whenever $\{x_1 \dots x_n\} \subset \Gamma$. The term $t' = \lambda x.Y_{x_1 \dots x_n, x}$ is obtained after executing $\lambda x.Y_{x_1 \dots x_n}\ x \simeq_\lambda t$. This unification ensures that t' cannot contain variables in $\Gamma / \{x_1 \dots x_n\}$, and therefore grants fidelity. In fact, a link represents a suspended unification problem between a unification variable X and a "problematic" term t. This unification is possible iff the free variables in t are also in the scope of X.

3.4.3 Occur check. Since compilation moves problematic terms out of the sight of $\simeq_\lambda$, that procedure can only perform a partial occur check. For example, the unification problem $X \simeq_\lambda f\ Y$ cannot generate a cyclic substitution alone, but should be disallowed if a $\mathbb{L}$ contains a link like $\vdash Y =_\eta \lambda z.X_z$: we don't know yet if Y will feature a lambda in head position, but we surely know it contains X, hence $f\ Y$ and that fails the occur check. The procedure `occur-check-links` is in charge of performing this check that is needed in order to guarantee proposition 2.3 (Simulation fidelity).

3.5 Substitution decompilation

Decompiling the substitution involves three steps.

First and foremost, problematic terms stored in $\mathbb{L}$ have to be moved back into the game: a suspended link must be turned into a valid assignment. This operation is possible thanks to invariant 2 (Link left hand side), which ensures that no link causes an occur-check (3.4.3) and the fact that $\mathbb{L}$ is duplicate-free (see section 6).

The second step involves allocating new variables in the memory of $\mathcal{F}$. This technicality is required because some higher-order unifications may require pruning a variable. For example, $F \cdot x \cdot y = F \cdot x \cdot z$ requires allocating a variable G in order to express the assignment $F_{ab} \mapsto G_a$.

The final step is to decompile each assignment. Decompiling a term is straightforward since $\mathbb{M}$ is a bijection. The only complex part concerns the `abs` node. In our simple setting, the `flam` node carries no additional information (other than the function body), so each `abs` node can be trivially converted to a `flam` one. However, in the case of Coq, where lambdas carry the type of the bound variable, one must store this information somewhere. Note that this information is similar to the arity of variables; that in Coq, unification variables have a (function) type, and this type can be used to annotate the lambdas needed to express their assignment.

Proposition 3.1 (Compilation round trip). *If* $\langle s \rangle \mapsto (t, m, l)$ *and* $l \in \mathbb{L}$ *and* $m \in \mathbb{M}$ *and* $\sigma = \{A \mapsto t\}$ *and* $X \mapsto A^n \in \mathbb{M}$ *then* $\langle \sigma, \mathbb{M}, \mathbb{L} \rangle^{-1} \mapsto \rho$ *and* $\rho X =_o \rho s$.

The statement above roughly states that the translation from $\mathcal{F}$ to $\mathcal{H}$ is not lossy, it can be reversed. The statement is made convoluted by the fact that we hid the procedure to decompile a term in favor of the one to decompile substitutions. We omit to sketch the proof of this property for brevity.

3.6 Definition of $\simeq_o$ and its properties

We already have all the pieces to show the code of $\simeq_\lambda$.

```
type (≃o) fm -> fm -> fsubst -> o.
(A ≃o B) F :-
  compile A A' [] M1 [] L1 [] S1,
  compile B B' M1 M2 L1 L2 S1 S2,
  hstep A' B' L2 L3 S2 S3,
  decompile M2 L3 S3 [] F.
```

So far the compiler is very basic. It does not really enforce that the terms passed to hstep are in $\mathcal{W}$, and indeed makes no use of the higher-order capabilities of the meta language (all generated variables have an empty scope). Still, we can prove that $\simeq_o$ is a good "first-order" unification algorithm if the input already happens to be in $\mathcal{W}$. Later, when the compiler will enforce proposition 2.9 the proof will be adjusted to cover for the new cases.

Lemma 3.2 (Properties of $\simeq_o$ in $\mathcal{W}$). *The implementation of* $\simeq_o$ *above is a good unification (as per proposition 2.1) for* $=_o$ *in the domain* $\mathcal{W}$.

Proof sketch. In this setting, $=_\lambda$ is as strong as $=_o$ on ground terms. What we have to show is that whenever two different $\mathcal{F}$ terms can be made equal by a substitution ρ (plus the β_l and β_r if needed), we can produce this ρ by finding a σ via $\simeq_\lambda$ on the corresponding $\mathcal{H}$ terms and by decompiling it. If we look at the syntax of $\mathcal{F}$, terms the only interesting case is `fuva X` $\simeq_o$ s. In this case, after compilation, we have $Y \simeq_\lambda t$ that succeeds with $\sigma = \{Y \mapsto t\}$ and σ is decompiled to $\rho = \{X \mapsto s\}$ by proposition 3.1. □

Theorem 3.3 (Fidelity in $\mathcal{W}$). *Proposition 2.2 (Run equivalence) and proposition 2.3 (Simulation fidelity) hold if* $\mathcal{W}(\mathbb{P})$.

Proof sketch. Trivial since `progress1` is a no-op and fstep and hstep are the same, and by lemma 3.2 $\simeq_\lambda$ is equivalent to $\simeq_o$. □

3.7 Notational conventions

In the following sections, we adopt this notation discuss the compiler's output: $\mathbb{P}$ represents the input set of problems that compiled to $\mathbb{T}$ with memory mapping $\mathbb{M}$ and links $\mathbb{L}$. For example:

$$\begin{array}{rl} \mathbb{P} = \{ & p_1 \simeq_o p_2 \quad p_3 \simeq_o p_4 \ \} \\ \mathbb{T} = \{ & t_1 \simeq_\lambda t_2 \quad t_3 \simeq_\lambda t_4 \ \} \\ \mathbb{M} = \{ & X_1 \mapsto A_1^x \quad X_2 \mapsto A_2^y \ \} \\ \mathbb{L} = \{ & \Gamma \vdash a =_\eta b \ \} \end{array}$$

We index each sub-problem, sub-mapping, and sub-link with its position starting from 1 and counting from left to right, top to bottom. For example, $\mathbb{T}_2$ corresponds to the $\mathcal{H}$ problem $t_3 \simeq_\lambda t_4$.

4 HANDLING OF $\diamond\beta$

In order to make $\simeq_o$ higher-order, we need to take care of terms in $\diamond\beta$. In the example below, we can see that the basic compilation given in the previous section is not able to make the $\mathcal{H}$ unification problem succeeds.

$$\begin{array}{rl} \mathbb{P} = \{ & \lambda x.(f\ (X\ x)\ a) \simeq_o \lambda x.(f\ x\ a) \ \} \\ \mathbb{T} = \{ & \lambda x.(f\ (A\ x)\ a) \simeq_\lambda \lambda x.(f\ x\ a) \ \} \\ \mathbb{M} = \{ & X \mapsto A^0 \ \} \end{array}$$

The unification problem $\mathbb{T}_1$ fails while trying to unify $A\ x$ and x, which is equivalent to «`app [uva A [], x]`» versus `x`. In order to exploit the higher-order unification algorithm of the meta language, we compile the $\mathcal{F}$ term $X\ x$ into the $\mathcal{H}$ term A_x.

4.1 Compilation and decompilation

We add the following rule before rule $(c_@)$, where `pattern-fragment` is a predicate checking if a list of terms is a list of distinct names.

```
comp (fapp [fuva A|Ag]) (uva B Ag1) M1 M2 L L S1 S2 :-
  pattern-fragment Ag, !,
    fold6 comp Ag Ag1 M1 M1 L L S1 S1,
    len Ag Arity,
    m-alloc (fv A) (hv B (arity Arity)) M1 M2 S1 S2.
```

Note that compiling `Ag` cannot create new mappings nor links, since `Ag` is made of bound variables, and the hypothetical rule (H_λ) loaded by `comp-lam` grants this property.

Decompilation. Since no link is created by the compilation of $\diamond\beta$ terms, no modification to the `commit-link` is needed.

Progress. Similarly to decompilation, since no link is produced, no modification to the `progress` predicate is needed.

Definition 4.1 ($\mathcal{W}_\beta$). $\mathcal{W}_\beta(X) \Leftrightarrow \forall t \in \mathcal{P}(X), t \notin (\diamond\eta \cup \diamond\mathcal{L})$

Lemma 4.2 (Properties of $\simeq_o$ in $\mathcal{W}_\beta$). *Given the updated compilation scheme, the* $\simeq_o$ *of section 3.6 is a good unification (as per proposition 2.1) for* $=_o$ *in the domain* $\mathcal{W}_\beta$.

Proof sketch. If we look at the $\mathcal{F}$ terms, there is one more interesting case, namely `fapp[fuva X|W]` $\simeq_o$ s when `W` are distinct names compiled to $\vec{w}$. In this case the $\mathcal{H}$ problem is $Y_{\vec{w}} \simeq_\lambda t$ that succeeds with $\sigma = \{Y_{\vec{y}} \mapsto t[\vec{w}/\vec{y}]\}$, which in turn is decompiled to $\rho = \{Y \mapsto \lambda\vec{y}.s[\vec{w}/\vec{y}]\}$. Thanks to β_l $(\lambda\vec{y}.s[\vec{w}/\vec{y}])\ \vec{w} =_o s$. □

Lemma 4.3 ($\mathcal{W}$-partial-enforcement). $\forall s, \langle s \rangle \mapsto (t, m, l)$, *if* $\mathcal{W}_\beta(s)$ *then* $\mathcal{W}(t)$.

In other word the compiler eliminates all subterms that are in $\diamond\beta$.

Theorem 4.4 (Fidelity in $\mathcal{W}_\beta$). *Proposition 2.2 (Run equivalence) and proposition 2.3 (Simulation fidelity) hold if* $\mathcal{W}_\beta(\mathbb{P})$.

Proof sketch. thanks to lemma 4.3 $\simeq_\lambda$ is as powerful as $\simeq_o$ in $\diamond\beta$, as well as in $\mathcal{W}$ by lemma 4.2. □

5 HANDLING OF $\diamond\eta$

A term $\lambda x.t\ x$ is said to be the η-expansion of t if x does not occur free in t, and conversely, t is the η-contraction of $\lambda x.t\ x$. The equational theory of $\mathcal{F}$ identifies these terms, but the current compilation scheme does not, as shown by the following example:

$$\begin{aligned}\mathbb{P} &= \{\ \lambda x.X\ x \simeq_o f\ \}\\ \mathbb{T} &= \{\ \lambda x.A_x \simeq_\lambda f\ \}\\ \mathbb{M} &= \{\ X \mapsto A^1\ \}\end{aligned}$$

While $\lambda x.X\ x \simeq_o f$ does admit the solution $\rho = \{\ X \mapsto f\ \}$, the corresponding problem in $\mathbb{T}$ does not: `lam x\ uva A [x]` and `con"f"` start with different, rigid, term constructors hence $\simeq_\lambda$ fails.

In order to guarantee proposition 2.2, we detect lambda abstractions that can disappear by η-contraction (section 5.1), and we modify the compiler so that it generates fresh unification variables in their place and moves the problematic term from $\mathbb{T}$ to $\mathbb{L}$ (section 5.2). The compilation of the problem $\mathbb{P}$ above is refined to:

$$\begin{aligned}\mathbb{P} &= \{\ \lambda x.X\ x \simeq_o f\ \}\\ \mathbb{T} &= \{\ A \simeq_\lambda f\ \}\\ \mathbb{M} &= \{\ X \mapsto B^1\ \}\\ \mathbb{L} &= \{\ \vdash A =_\eta \lambda x.B_x\ \}\end{aligned}$$

As per invariant 2 the η-`link` left-hand side is a variable while the right-hand side is a term in $\diamond\eta$ that has the following property:

Invariant 3 (η-`link` rhs). *The rhs of any η-`link` has the shape $\lambda x.t$ and t is $\mathcal{W}$.*

Each η-`link` is kept in the link store $\mathbb{L}$ during execution and is activated under some conditions. Activation is implemented by extending the `progress1` predicate defined in section 3.4.

5.1 Detection of $\diamond\eta$

When compiling a term t, we need to determine if any subterm $s \in \mathcal{P}(t)$ that is of the form $\lambda x.r$, where x occurs in r, can be a η-expansion, i.e. if there exists a substitution ρ such that $\rho(\lambda x.r) =_o s$. The detection of lambda abstractions that can "disappear" is not as trivial as it may seems. Here a few examples:

$\lambda x.f\ (A\ x)$	$\in \diamond\eta$	$\rho = \{\ A \mapsto \lambda x.x\ \}$
$\lambda x.f\ (A\ x)\ x$	$\in \diamond\eta$	$\rho = \{\ A \mapsto \lambda x.a\ \}$
$\lambda x.f\ x\ (A\ x)$	$\notin \diamond\eta$	
$\lambda x.\lambda y.f\ (A\ x)\ (B\ y\ x)$	$\in \diamond\eta$	$\rho = \{\ A \mapsto \lambda x.x,\ B \mapsto \lambda y.\lambda x.y\ \}$

The first two examples are easy, and show how a unification variable can expose or erase a variable in its scope, turning the resulting term into an η-expansion or not.

The third example shows that when a variable occurs outside the scope of a unification variable, it cannot be erased and can hence prevent a term from being an η-expansion.

The last example shows the recursive nature of the check we need to implement. The term starts with a spine of two lambdas, hence the whole term is in $\diamond\eta$ iff the inner term $\lambda y.f\ (A\ x)\ (B\ y\ x)$ is in $\diamond\eta$ itself. If it is, it could η-contract to $f\ (A\ x)$ making $\lambda x.f\ (A\ x)$ a potential η-expansion.

We can now define more formally how $\diamond\eta$ terms are detected together with its auxiliary functions:

Definition 5.1 (may-contract-to). A β-normal term s *may-contract-to* a name x if there exists a substitution ρ such that $\rho s =_o x$.

Lemma 5.2. *A β-normal term $s = \lambda x_1 \dots x_n.t$* may-contract-to *$x$ only if one of the following three conditions holds:*

1. *$n = 0$ and $t = x$;*
2. *t is the application of x to a list of terms l and each l_i* may-contract-to *x_i (e.g. $\lambda x_1 \dots x_n.x\ x_1 \dots x_n =_o x$);*
3. *t is a unification variable with scope W, and for any $v \in \{x, x_1 \dots x_n\}$, there exists a $w_i \in W$, such that w_i* may-contract-to *v (if $n = 0$ this is equivalent to $x \in W$).*

Proof sketch. Since our terms are in β-normal form there is only one rule that can play a role (namely η_l), hence if the term s is not exactly x (case 1) it can only be an η-expansion of x, or a unification variable that can be assigned to x, or a combination of both. If s begins with a lambda, then the lambda can only disappear by η contraction. In that case, the term t is under the spine of binders $x_1 \dots x_n$, t can either be x applied to terms that can *may-contract-to* these variables (case 2), or a unification variable that can be assigned to that application (case 3). □

Definition 5.3 (occurs-rigidly). A name x *occurs-rigidly* in a β-normal term t, if $\forall \rho, x \in \mathcal{P}(\rho t)$

In other words, x *occurs-rigidly* in t if it occurs in t outside of the scope of a unification variable X; otherwise, an instantiation of X can make x disappears from t. Moreover, note that η-contracting t cannot make x disappear, since x is not a locally bound variable inside t.

We can now describe the implementation of $\diamond\eta$ detection:

Definition 5.4 (maybe-eta). Given a β-normal term $s = \lambda x_1 \dots x_n.t$, *maybe-eta s* holds if any of the following holds:

1. t is a constant or a name applied to the arguments $l_1 \dots l_m$ such that $m \geq n$ and for every i such that $m - n < i \leq m$ the term l_i *may-contract-to* x_i, and no x_i *occurs-rigidly* in $l_1 \dots l_{m-n}$;
2. t is a unification variable with scope W and for each x_i there exists a $w_j \in W$ such that w_j *may-contract-to* x_i.

Lemma 5.5 ($\diamond\eta$ detection). *If t is a β-normal term and $t \in \diamond\eta$ then* maybe-eta *t holds.*

Proof sketch. Follows from definition 5.3 and lemma 5.2 □

Remark that the converse of lemma 5.5 does not hold: there exists a term t satisfying the criteria (1) of definition 5.4 that is not in $\diamond\eta$, i.e. there exists no substitution ρ such that ρt is an η-expansion. A simple counter example is $\lambda x.f\ (A\ x)\ (A\ x)$ since x does not *occur-rigidly* in the first argument of f, and the second argument of f *may-contract-to* x. In other words $A\ x$ may either use or discard x, but our analysis does not take into account that *the same term* cannot have two contrasting behaviors.

As we will see in the rest of this section, this is not a problem since it does not break proposition 2.2 nor proposition 2.3.

5.2 Compilation and decompilation

Compilation. The following rule is inserted just before rule (c_λ) from the code in section 3.3.

```
comp (flam F) (uva A Scope) M1 M2 L1 L3 S1 S3 :-
  maybe-eta (flam F) [], !,
    alloc S1 A S2,
    comp-lam F F1 M1 M2 L1 L2 S2 S3,
    get-scope (lam F1) Scope,
    L3 = [val (link-eta (uva A Scope) (lam F1)) | L2].
```

Whenever `flam F` is detected to be in $\Diamond\eta$ it is compiled to `lam F1` and replaced by the fresh variable `A`. This variable sees all the names free in `lam F1`. The variable is connected to `lam F1` via a η-`link`. Invariant invariant 2 (Link left hand side) holds for this link. Moreover:

Corollary 5.6. *The rhs of any η-`link` has exactly one lambda abstraction, hence the rule above respects invariant 3 (η-`link` rhs).*

Proof sketch. By contradiction, suppose that the rule above is applied and that the rhs of the link is $\lambda x.\lambda y.t$, where x and y occur in t. If *maybe-eta* $\lambda y.t$ holds then the recursive call to `comp` (made by `comp-lam`) must have put a fresh variable in its place, so this case is impossible. Otherwise, if *maybe-eta* $\lambda y.t$ does not hold, then also *maybe-eta* $\lambda x.\lambda y.t$ does not hold either, contradicting the assumption that the rule was applied. □

Definition 5.7 ($\mathcal{W}_{\beta\eta}$). $\mathcal{W}_{\beta\eta}(X) \Leftrightarrow \forall t \in \mathcal{P}(X), t \notin \Diamond\mathcal{L}$

Lemma 5.8 ($\mathcal{W}$-partial-enforcement). *$\forall s, \langle s\rangle \mapsto (t, m, l)$, if $\mathcal{W}_{\beta\eta}(s)$ then $\mathcal{W}(t)$.*

Proof sketch. By lemma 5.5 □

Decompilation. The decompilation of a η-`link` is performed by unifying the lhs with the rhs. Note that this unification never fails, since lhs is a flexible term not appearing in any other η-`link` (by definition 5.10).

5.3 Progress

η-`link`s are meant to delay the unification of "problematic" terms until we know for sure if the term has to be η-contracted or not.

Definition 5.9 (η-progress-lhs). A link $\Gamma \vdash X =_\eta t$ is removed from $\mathbb{L}$ when X becomes rigid. Let $y \in \Gamma$, there are two cases:

(1) if $X = a$ or $X = y$ or $X = f\ a_1 \dots a_n$ we unify the η-expansion of X with t, that is we run $\lambda x.X\ x \simeq_\lambda t$
(2) if $X = \lambda x.t$ we run $X \simeq_\lambda t$.

Definition 5.10 (η-progress-deduplicate). A link $\Gamma \vdash X_{\vec{s}} =_\eta T$ is removed from $\mathbb{L}$ when another link $\Delta \vdash X_{\vec{r}} =_\eta T'$ is in $\mathbb{L}$. By invariant 1 the length of $\vec{s}$ and $\vec{r}$ is the same; hence we can move the term T' from Δ to Γ by renaming its bound variables, i.e. $T'' = T'[\vec{r}/\vec{s}]$. We then run $T \simeq_\lambda T''$ (under the context Γ).

Lemma 5.11. *Let $\lambda x.t$ the rhs of a η-`link`, then $\mathcal{W}(t)$, enforcing invariant 3.*

Proof sketch. By construction, every "problematic" term in $\mathcal{F}$ is replaced with a variable in the corresponding $\mathcal{H}$ term. Therefore, $\mathcal{W}(t)$. □

Lemma 5.12. *Given a η-`link` $\Gamma \vdash X =_\eta \lambda x.t$, the unification done by η-progress-lhs is between terms in $\mathcal{W}$*

Proof sketch. Let σ be the substitution, such that $\mathcal{W}(\sigma X)$ (since $\simeq_\lambda$ preserves $\mathcal{W}$). By invariant 3, we have $\mathcal{W}(t)$. If $\sigma X = \lambda x.r$, then r is unified with t: both terms are $\mathcal{W}$. Otherwise, $\lambda x.Xx$ is unified with $\lambda x.t$, and Xx and t are both $\mathcal{W}$. □

Lemma 5.13. *The unification done by η-progress-deduplicate is between terms in $\mathcal{W}$.*

Proof. Given two η-`links` $\Gamma_1 \vdash X =_\eta \lambda x.t$ and $\Gamma_2 \vdash Y =_\eta \lambda x.t'$ the unification is performed between t and t'. Both terms are $\mathcal{W}$ and therefore, unification is done between $\mathcal{W}$ terms. □

Lemma 5.14. *The progress of η-`link` guarantees proposition 2.11 ($\mathcal{W}$-preservation)*

Proof sketch. By lemmas 5.12 and 5.13, every unification performed by the activation of a η-`link` is done between terms in $\mathcal{W}$, therefore, the substitution remains $\mathcal{W}$. □

Lemma 5.15. `progress` *terminates.*

Proof sketch. Rules definition 5.9 and definition 5.10 remove one link from $\mathbb{L}$, hence they cannot be applied indefinitely. Moreover each rule only relies on terminating operations such as $\simeq_\lambda$, η-contraction, η-expansion, relocation (a recursive copy of a finite term). □

Theorem 5.16 (Fidelity in $\mathcal{W}_{\beta\eta}$). *Given a list of unification problems $\mathbb{P}$, such that $\mathcal{W}_{\beta\eta}(\mathbb{P})$, if the memory map is bijective, then the introduction of η-`link` guarantees proposition 2.3 (Simulation fidelity).* [1]

Proof sketch. For any step i, we want to prove that fstep_i succeeds iff hstep_i succeeds. A hstep_i is made by a unification u and a link progression p. Without loss of generality, we consider a $\mathcal{F}$unification problem of the form $s_1 \simeq_o s_2$ where $s_1 \in \Diamond\eta$. s_1 is compiled to X with the accessory link $\Gamma \vdash X =_\eta \lambda x.t_1$. The unification u always succeeds, since X is a fresh variable, we only have to consider the link progression p. Two cases should be analyzed:

- $s_2 \notin \Diamond\eta$, in this case s_2 is compiler to t_2 and u assigns t_2 to X and triggers *η-progress-lhs* if t_2 is rigid. If s_1 and s_2 unify thanks to η_l then progression p unifies $\lambda x.t_1$ with the η-expansion of t_2 namly $\lambda x.t_2\ x$, otherwise they unify thanks to **??** and p unifies $\lambda x.t_1$ with t_2. Alternatively, if s_1 and s_2 fails to unify, it cannot be because of the head λ constructors, since wither lam-lam or η_l move under it and find different sub terms s_1' and s_2'. By theorem 4.4, $\simeq_\lambda$ fails on terms t_1' and t_2' even if *η-progress-lhs* η-expands t_2.
- $s_2 \in \Diamond\eta$, in this case, the unification problem becomes $X \simeq_\lambda Y$ with the extra link $\vdash Y =_\eta \lambda x.t_2$. After the unification of X and Y, *η-progress-deduplicate* is fired and, once the λ are crossed, t_1 and t_2 are unified. This unification succeeds iff $s_1 \simeq_o s_2$ succeeds by theorem 4.4.

□

to re-formulate

explain why

[1] This premise is fulfilled in section 6

Corollary 5.17 (Properties of $\simeq_o$ in $\mathcal{W}_{\beta\eta}$). *Given the updated compilation scheme, the $\simeq_o$ of section 3.6 is a good unification (as per proposition 2.1) for $=_o$ in the domain $\mathcal{W}_{\beta\eta}$.*

Example of η-progress-lhs. The example at the beginning of section 5, once $\sigma = \{ A \mapsto f \}$, triggers *$\eta$-progress-lhs* since the link becomes $\vdash f =_\eta \lambda x.B_x$ and the lhs is a constant. This rule runs $\lambda x.f\ x \simeq_\lambda \lambda x.B_x$, resulting in $\sigma = \{ A \mapsto f\ ;\ B_x \mapsto f \}$. By the definition of `η-link` decompilation, decompilation generates $\rho = \{ X \mapsto \lambda x.f\ x \}$, since: X is mapped to B_x and B_x is decompiled into $\lambda x.f\ x$.

6 MAKING $\mathbb{M}$ A BIJECTION

In section 3.1, we introduced the definition of memory map $\mathbb{M}$. This map allows to decompile the $\mathcal{H}$ substitution to the object language. Given the higher-order nature of Coq the same unification variable X can be used multiple times with different arities.

$$\begin{array}{rl} \mathbb{P} = \{ & \lambda x.(X\ x) \simeq_o a \quad X \simeq_o \lambda x.a \ \} \\ \mathbb{T} = \{ & A \simeq_\lambda a \quad C \simeq_\lambda \lambda x.a \ \} \\ \mathbb{M} = \{ & X \mapsto C^0 \quad X \mapsto B^1 \ \} \\ \mathbb{L} = \{ & \vdash A =_\eta \lambda x.B_x \ \} \end{array}$$

In the unification problems $\mathbb{P}$ above, we see that X is used with arity 1 in $\mathbb{P}_1$ and with arity 0 in $\mathbb{P}_2$. In order to preserve invariant 1 (Unification-variable arity) the compiler did generate two entries in $\mathbb{M}$ for X, namely B and C. However, there is no connection between these two variables and any incompatible assignements to them would not be detected, breaking, in turn proposition 2.3. This incompatibility will only be detected during the decompilation phase. To address this issue, we post-processing the compiler's output we want to ensure the follwoing property:

Proposition 6.1 ($\mathbb{M}$ is a bijection). *After compilation, for each $\mathcal{F}$ variable X in $\mathbb{P}$ and for each $\mathcal{H}$ variable A in $\mathbb{T}$ there is exactly one entry $X \mapsto A^n$ (for any arity n).*

Note that the execution in $\mathcal{H}$ may require allocating new variables as explained in section 3.5. The property above does not concern these.

The core procedure of this post-processing step is *align-arity* that is iterated by `map-deduplication`:

*Definition 6.2 (*align-arity*).* Given two mappings $m_1 : X \mapsto A^m$ and $m_2 : X \mapsto C^n$ where $m < n$ and $d = n - m$, *align-arity* $m_1\ m_2$ generates the following d links, one for each i such that $0 \le i < d$,

$$x_0 \dots x_{m+i} \vdash B^i_{x_0 \dots x_{m+i}} =_\eta \lambda x_{m+i+1}.B^{i+1}_{x_0 \dots x_{m+i+1}}$$

where B^i is a fresh variable of arity $m + i$, and $B^0 = A$ as well as $B^d = C$.

The intuition is that we η-expand the occurrence of the variable with higher arity to match the lower arity. Since each `η-link` can add exactly one lambda, we need as many links as the difference between the two arities.

*Definition 6.3 (*map-deduplication*).* Forall mappings $m_1, m_2 \in \mathbb{M}$ such that $m_1 : X \mapsto A^m$ and $m_2 : X \mapsto C^n$ and $m < n$ we remove m_1 from $\mathbb{M}$ and add to $\mathbb{L}$ the result of *align-arity* $m_1\ m_2$.

Theorem 6.4 (Fidelity with *map-deduplication*). *Given a list of unification problems $\mathbb{P}$, such that $\mathcal{W}_{\beta\eta}(\mathbb{P})$, if $\mathbb{P}$ contains the same $\mathcal{F}$ variable used at different arities, then* map-deduplication *guarantees proposition 2.3 (Simulation fidelity)*

Proof sketch. By the definition of *map-deduplication*, any two occurrencies of the same $\mathcal{F}$ variable used at different arities are compiled to two variables A^m and C^n related by a chain of `η-link`. Without loss of generality, we pose $m < n$. If A^m is assigned to a term $\lambda\vec{x}.t$ with q being the length of $\vec{x}$. If t is a rigid term, then the chain of links between A^m and C^n is completely triggered so that C^n is assigned to $\lambda\vec{x}.t$ η-expanded $n-m$ times. Note that in this case fidelity is guaranteed, since term unified to C^n sohuld also unify with A^m. Otherwise, if t is a variable, the chain of links is shrinked by q. Note that if this length is bigger then $n - m$ again the full chain collapse and A^m and C^n are agian tiny coupled. Otherwise, if $q < n - m$, it means that C^n can always be assigned to any term starting with at least q lambdas. In this second case fidelity is also guaranteed, due to the constraint of the number of lambda by which C^n should start. □

Note that shortening the chain of links allows unification to fail if X_1 and X_2 are unified with different terms.

Example of map-deduplication. If we take back the example give at the beginning of this section, *map-deduplication* produces the following result:

$$\begin{array}{rl} \mathbb{P} = \{ & \lambda x.(X\ x) \simeq_o a \quad X \simeq_o \lambda x.a \ \} \\ \mathbb{T} = \{ & A \simeq_\lambda a \quad C \simeq_\lambda \lambda x.a \ \} \\ \mathbb{M} = \{ & X \mapsto B^1 \ \} \\ \mathbb{L} = \{ & \vdash C =_\eta \lambda x.B_x \quad \vdash A =_\eta \lambda x.B_x \ \} \end{array}$$

Note that $X \mapsto B^1$ desappears from $\mathbb{M}$ in favour of the auxiliary `η-link` $x \vdash E_x =_\eta \lambda y.C_{xy}$. The resolution of $\mathbb{T}_1$ assignes a to A. This wakes up $\mathbb{L}_2$ by *η-progress-lhs*, assigning «$a\ x$» to B_x. The resolution of $\mathbb{T}_2$ instantiates C to $\lambda x.a$, which, in turn triggers $\mathbb{L}_1$ by *η-progress-lhs*. This link perfroms $\lambda x.a \simeq_\lambda \lambda x.(a\ x)$, which, as expected, fails.

7 HANDLING OF $\diamond\mathcal{L}$

Even if we do not requrie $\simeq_\lambda$ to handle problems outside of $\mathcal{L}$ it is worth handling terms in $\diamond\mathcal{L}$ since, in practice, these terms often re-enter $\mathcal{L}$ at runtime, as observed in [15] for example, or to accommodate for the introduction of heuristics.

In the following example problem $\mathbb{P}_2$ is $X\ a \simeq_o a$ that admits two different substitutions: $\rho_1 = \{X \mapsto \lambda x.x\}$ and $\rho_2 = \{X \mapsto \lambda x.a\}$. The unification algorithm alone cannot chose, since no solution is more general than the other, although the first problem solve this dilemma at run-time making the second problem well behaved:

$$\begin{array}{rl} \mathbb{P} = \{ & X \simeq_o \lambda x.a \quad (X\ a) \simeq_o a \ \} \\ \mathbb{T} = \{ & A \simeq_\lambda \lambda x.a \quad (A\ a) \simeq_\lambda a \ \} \\ \mathbb{M} = \{ & X \mapsto A^0 \ \} \end{array}$$

We want to support this scenario but we have to improve a little our compiler and progress routines. In particular $\mathbb{T}_1$ generates $\sigma = \{A \mapsto \lambda x.a\}$ making $\sigma\mathbb{T}_2$ equal to $(\lambda x.a)\ a \simeq_\lambda a$ that $\simeq_\lambda$ cannot solve since it lacks rules β_l and β_r.

To address this problem the compiler must recognize and replace $\diamond\mathcal{L}$ terms with fresh variables and generate a new kind of links that we call $\mathcal{L}$`-link`.

In addition to invariant 2 (Link left hand side), the term on the rhs of a $\mathcal{L}$-link has the following property:

Invariant 4 ($\mathcal{L}$-link rhs). *The rhs of any $\mathcal{L}$-link has the shape $X\ t_1 \dots t_m$ where X is a unification variable in $\mathcal{L}$ (with scope $s_1 \dots s_n$) and $t_1 \dots t_m$ is a list of terms such that $m > 0$ and t_1 is either a variable occurring in $s_1 \dots s_n$ or a term other than a variable.*

Note that the shape of such as rhs is «app [uva X S | L]», where S = $s_1 \dots s_n$ and L = $t_1 \dots t_m$.

7.1 Compilation and decompilation

For the detection of $\diamond\mathcal{L}$ it is sufficient to identify applications with a flexible head and arguments that are not in distinct names. The following rule for $\diamond\mathcal{L}$ compilation is inserted just before rule ($c_@$).

```
comp (fapp [fuva A|Ag]) (uva B Scope) M1 M3 L1 L3 S1 S4 :- !,
  pattern-fragment-prefix Ag Pf Extra, alloc S1 B S2,
  len Pf Ar, m-alloc (fv A) (hv C (arity Ar)) M1 M2 S2 S3,
  fold6 comp Pf    Pf1    M2 M2 L1 L1 S3 S3,
  fold6 comp Extra Extra1 M2 M3 L1 L2 S3 S4,
  Beta = app [uva C Pf1 | Extra1],
  get-scope Beta Scope,
  L3 = [val (link-llam (uva B Scope) Beta) | L2].
```

The list Ag is split into the two parts: Pf is in $\mathcal{L}$, and can be empty; Extra cannot be empty and is such that append Pf Extra Ag. The rhs of the $\mathcal{L}$-link is the application of a fresh variable C having in scope all names in Pf1 (the compilation of Pf). The variable B, returned has the compiled term, is a fresh variable having in scope all the free variables occurring in Pf1 and Extra1 (the compilation of Extra). This construction enforces invariant 4.

Lemma 7.1 ($\mathcal{W}$-enforcement). *$\forall s, \langle s \rangle \mapsto (t, m, l)$, then $\mathcal{W}(t)$.*

Proof sketch. By lemmas 4.3 and 5.8 and the rule above. □

Decompilation. All $\mathcal{L}$-link should be solved before decompilation. If any $\mathcal{L}$-link remains in $\mathbb{L}$, decompilation fails.

7.2 Progress

Given a $\mathcal{L}$-link l of the form $\Gamma \vdash T =_{\mathcal{L}} X_{s_1 \dots s_n}\ t_1 \dots t_m$, we provide the following activation rules:

Definition 7.2 ($\mathcal{L}$-progress-refine). Let σ be a substitution such that σt_1 is a name s not occurring $s_1 \dots s_n$. If $m = 1$, then l is removed and lhs is unified with $X_{s_1 \dots s_n}\ s$. If $m > 1$, then l is replaced by the link $\Gamma \vdash T =_{\mathcal{L}} Y_{s_1 \dots s_n}\ s\ t_2 \dots t_m$ (where Y is a fresh variable of arity $n+1$) and link $\Gamma \vdash X_{s_1 \dots s_n} =_\eta \lambda x. Y_{s_1 \dots s_n}\ x$ is added to $\mathbb{L}$.

Definition 7.3 ($\mathcal{L}$-progress-rhs). Link l is removed from $\mathbb{L}$ if $X_{s_1 \dots s_n}$ is instantiated to a term t and $t\ t_1 \dots t_m$ β-reduces to a $t' \in \mathcal{L}$.

Definition 7.4 ($\mathcal{L}$-progress-fail). progress fails whenever there exists another link $l' \in \mathbb{L}$ with the same lhs or the lhs become rigid.

We will relax this last failure condition to accommodate for the implementation of heuristics in section 7.3.

Finally, in order to correctly correlate a variable appearing in the lhs of a η-link and in the rhs of a $\mathcal{L}$-link, we should introduce the following η-link progression rule.

Definition 7.5 (η-progress-rhs). A link $\Gamma \vdash X =_\eta T$ is removed from $\mathbb{L}$ when either 1) *maybe-eta* T does not hold (anymore) or 2) by η-contracting T to T' where T' does not start with the lam constructor. In the first case, X is unified with T, and in the second one, X is unified with T' (under the context Γ).

The idea behind this is to instantiate the variable of a η-link whenever its rhs is for sure a $\mathcal{W}$ term.

Lemma 7.6. progress *terminates*

Proof sketch. Let l a $\mathcal{L}$-link in the store $\mathbb{L}$. If l is activated by $\mathcal{L}$-*progress-rhs*, then it disappears from $\mathbb{L}$ and progress terminates. Otherwise, the rhs of l is made by a variable applied to m arguments. At each activation of $\mathcal{L}$-*progress-refine*, l is replaced by a new $\mathcal{L}$-link l^1 having $m-1$ arguments. At the m^{th} iteration, the $\mathcal{L}$-link l^m has no more arguments and is removed from $\mathbb{L}$. Note that at the m^{th} iteration, m new η-link have been added to $\mathbb{L}$, however, by lemma 5.15, the algorithm terminates. $\mathcal{L}$-*progress-fail* guarantees termination since it immediately fails and η-*progress-rhs* terminates since it executes terminating instructions and if its permises succeed, ther considered η-link is removed from $\mathbb{L}$. □

Theorem 7.7 (Fidelity in $\mathcal{F}$). *The introduction of $\mathcal{L}$-link guarantees proposition 2.4 (Fidelity recovery) if $\simeq_o$ falls outside $\mathcal{L}$.*

Proof sketch. Let $\mathbb{P}_i$ be the first problem in $\mathbb{P}$, such that it is not in $\mathcal{L}$ and le σ be the substitution obtained solving $\mathbb{T}_1 \dots \mathbb{T}_{i-1}$. After the execution of hstep_{i-1}, each variable X corresponding to a $\diamond\eta$ subterm in the original $\mathcal{F}$unification problem, is instantiated if it is known for sure that X is no more a $\diamond\eta$. If $\sigma\mathbb{T}_i$ is in $\mathcal{L}$, then by definitions 7.2 and 7.3 the associated $\mathcal{L}$-link is solved and removed. Note that, in this case, all calls to $\simeq_\lambda$ are between terms in $\mathcal{L}$ and by theorem 4.4 fidelity is guaranteed. If $\sigma\mathbb{T}$ is still in $\diamond\mathcal{L}$, then by definition 7.4 unification fails as the corresponding unification in $\mathcal{F}$ would. □

7.3 Relaxing definition 7.4 ($\mathcal{L}$-*progress-fail*)

Working with terms in $\mathcal{L}$ is sometime too restrictive [1] and we could find in literature a few strategies to go beyond $\mathcal{L}$ without implementing Huet's algorithm [11]. Some implementations of λProlog [16] such as Teyjus [15] delay the resolution of $\diamond\mathcal{L}$ unification problems until the substitution makes them reenter $\mathcal{L}$. Other systems, for example of the unification algorithm of Coq used in its type-class solver [23], apply heuristics like preferring projection over mimic, and commit to that solution.

In this section we show how we can implement these strategies by simply adding (or removing) rules to the progress predicate. In the example below $\mathbb{P}_1$ is in $\diamond\mathcal{L}$.

$$\begin{aligned}
\mathbb{P} &= \{\ (X\ a) \simeq_o a \quad X \simeq_o \lambda x.Y\ \} \\
\mathbb{T} &= \{\ \quad A \simeq_\lambda a \quad B \simeq_\lambda \lambda x.C\ \} \\
\mathbb{M} &= \{\ Y \mapsto C^0 \quad X \mapsto B^0\ \} \\
\mathbb{L} &= \{\ \vdash A =_{\mathcal{L}} (B\ a)\ \}
\end{aligned}$$

If we want the object language unification to delay the first unification problem (waiting for X to be be instantiated), we can relax definition 7.4. Instead of failing when the lhs of $\mathbb{L}_1$ becomes rigid (equal to a), we keep it in $\mathbb{L}$ until the head of its rhs also become rigid. In this case, since both the lhs and rhs have rigid heads, they can

be unified. While this relaxed rule does not break proposition 2.3 (Simulation fidelity) per se, the `occur-check-links` procedure becomes incomplete since invariant 2 (Link left hand side) is broken. Also note that delaying unification outside $\mathcal{L}$ can leave $\mathcal{L}$`-link` for the decompilation phase. Therefore `commit-links` should be modified accordingly.

If instead we want $\simeq_o$ to follow the second strategy and pick an arbitrary solution we can modify progress by applying the desired heuristic instead of failing. For instance, in $X\,a\,b = Y\,b$, the last argument of the two terms is the same and unification can succeed by assigning Xa to Y. This heuristic is used by [23].

8 ACTUAL IMPLEMENTATION IN ELPI

In this paper we did study a compiler and simulation loop on a minimal language. The actual implementation uses the Coq-Elpi meta language to both compile the sequence of problems (the rules) and execute them, that is Elpi plays the role of $\mathcal{H}$ as well.

The main difference is that we cannot implement hrun since it comes as part of the runtime of the programming language. In particular the runtime iterates $\simeq_\lambda$, but hstep also needs to check for progress. Luckily Elpi extends [10] λProlog with syntactic constraints (suspended goals) and Constraint Handling Rules (CHR) [7] to operate on them. An important design choice is that constraints are suspended on a user computed list of unification variables, and are resumed as soon as one of them is assigned, before any other existing goal is considered. In turn this property enables a timely activation of links that grants proposition 2.3 (Simulation fidelity). For brevity we only provide two pseaudo-code snippets. The first one depicts how η`-link` are suspended or make progress.

```
link-eta L R :- var L, maybe-eta R HolesInR, !,
  declare_constraint (link-eta L R) [L|HolesInR].
link-eta L R :- not (var L), !, eta-progress-lhs L R.
```

The second snippet illustrates the deduplication of η`-link`. The syntax «`N ▹ G ?- P`» denotes a λProlog sequent, that is a goal `P` under a set `G` of hypothetical rules (introduced by `=>`) and where the program context binds (via the `pi` operator) `N` heigenvariables. Sequents are presented to CHR with their higher order unification variables replaced by "frozen constants", that is A_{xyz} becomes «`uvar` f_A `[x,y,z]`» for a fresh constant f_A. Frozen constants are "defrost" when they are part of a new goal (see [10, section 4.3]).

```
rule (N1 ▹ G1 ?- link-eta (uvar X LX1) T1)   % match
  /  (N2 ▹ G2 ?- link-eta (uvar X LX2) T2)   % remove
  |  (relocate LX1 LX2 T2 T2')               % condition
 <=> (N1 ▹ G1 ?- T1 = T2').                  % new goal
```

The first directive matches a constraint whose lhs is a variable `X`; the second mathes and removes a constraint on the same variable; the third relocates `T2` and the latter crafs the new goal that unifies `T1` with `T2'` under `G1` and the set of heigenvariables `N1`.

9 RELATED WORK AND CONCLUSION

Different strategies can be used to unify terms of the object language. The first approach that comes to mind consist in implementing $\simeq_o$ as a regular routine in the ML, i.e. write rules as follows:

```
decision X :- X ≃o (all A x\ app [P, x]), finite A,
  pi x\ decision (app [P, x]).
```

Opting for this method would result in a suboptimal utilization of the logic programming engine provided by the ML, as it degrades indexing by eliminating all data from rule heads. Additionally, implementing a unification procedure in the ML is likely to be significantly slower compared to the built-in one.

Another possibility is to avoid having application and abstraction nodes in the syntax tree, and use the ones of the ML, as in:

```
decision (all A x\ P x) :- finite A, pi x\ decision (P x).
```

However, this encoding has two big limitations. First it is not always feasible to adopt it for Coq due to the fact that the type system of the ML is too limited to accommodate for that one the object language, e.g. Coq can typecheck variadic functions [2].
Second, the encoding of Coq terms provided by Elpi is primarily utilized for meta programming, in order to extend the Coq system. Consequently, it must be able to manipulate terms that are not known in advance without relying on introspection primitives such as Prolog's `functor` and `arg`. In this context, constants need to live in an open world, akin to the `string` data type used in the preceding examples, they cannot be symbols of the ML.

In the literature we could find a related encoding of the Calculus of Constructions (CC) [4]. The goal of that work is to exhibit a logic program performing proof checking for CC and hence relate the proof system of intuitionistic higher-order logic (that animates λProlog programs) with the one of CC. The encoding is hence tailored toward a different goal, for example it utilizes three relations to represent the equational theory of CC, and that choice alone makes things harder for us. Section 6 contains a discussion about the use of the unification procedure of the ML in presence of non ground goals, but the authors do not aim at exploiting it to the degree we want.

sucks

Another work that is, somewhat surprisingly, only superficially related to ours is the type-class engine built in Isabelle's meta language. In [29] classes identify (simple) types, they are not higher order predicates as in Coq, hence the solver does not require a higher-order unification procedure.

The approach presented in this paper provides a third option that addresses all the concerns mentioned earlier. It capitalizes on the benefit of not requiring to fully implement the unification algorithm of the object language. Instead, it employs the unification capabilities of the meta language, facilitated by the various links to manage "problematic" subterms. As a result of this choice our encoding takes advantage of indexing data structures and mode analysis for clause filtering. It it worth mentioning that we only replace terms with variables only when it is strictly needed, leaving the rest of the term structure intact and hence indexable by the meta language logic programming engine. Moreover, the unification process we obtain is ready to take advantage of potential improvements to the programming engine, such as tabled search, and apply forms of static analysis for the meta language, such as determinacy, to the object language. Finally, our approach is flexible enough to accommodate different strategies and heuristics to handle terms outside the pattern fragment, and it is not tightly coupled with Coq.

mention preliminar experiment show that our prolog is 2x

We considered mechanizing our results with Abella [8], especially in the early phases. Unfortunately we could not. One reason is that eliminating the cut operator, although possible, has a high cost in verbosity. Another problem is that the logic of Abella does

not let one quantify over predicates and combinators like `forall` are used pervasively in our code.

finish

REFERENCES

[1] Andreas Abel and Brigitte Pientka. "Extensions to Miller's Pattern Unification for Dependent Types and Records". In: 2018. URL: https://api.semanticscholar.org/CorpusID:51885863.

[2] Adam Chlipala. *Certified Programming with Dependent Types: A Pragmatic Introduction to the Coq Proof Assistant*. The MIT Press, 2013. ISBN: 0262026651.

[3] Cvetan Dunchev et al. "ELPI: Fast, Embeddable, λProlog Interpreter". In: *Logic for Programming, Artificial Intelligence, and Reasoning - 20th International Conference, LPAR-20 2015, Suva, Fiji, November 24-28, 2015, Proceedings*. Ed. by Martin Davis et al. Vol. 9450. 2015, pp. 460–468. DOI: 10.1007/978-3-662-48899-7_32. URL: http://dx.doi.org/10.1007/978-3-662-48899-7%5C_32.

[4] Amy Felty. "Encoding the Calculus of Constructions in a Higher-Order Logic". In: ed. by M. Vardi. IEEE, June 1993, pp. 233–244. DOI: 10.1109/LICS.1993.287584.

[5] Amy Felty and Dale Miller. "Specifying theorem provers in a higher-order logic programming language". In: *Ninth International Conference on Automated Deduction*. Ed. by Ewing Lusk and Ross Overbeck. 310. Argonne, IL: Springer, May 1988, pp. 61–80. DOI: 10.1007/BFb0012823.

[6] Davide Fissore and Enrico Tassi. "A new Type-Class solver for Coq in Elpi". In: *The Coq Workshop 2023*. Bialystok, Poland, July 2023. URL: https://inria.hal.science/hal-04467855.

[7] Thom Fruehwirth. *Constraint Handling Rules - What Else?* 2017. arXiv: 1701.02668 [cs.PL].

[8] Andrew Gacek. *The Abella Interactive Theorem Prover (System Description)*. 2008. arXiv: 0803.2305 [cs.LO].

[9] Benjamin Grégoire, Jean-Christophe Léchenet, and Enrico Tassi. "Practical and sound equality tests, automatically – Deriving eqType instances for Jasmin's data types with Coq-Elpi". In: *CPP '23: 12th ACM SIGPLAN International Conference on Certified Programs and Proofs*. CPP 2023: Proceedings of the 12th ACM SIGPLAN International Conference on Certified Programs and Proofs. Boston MA USA, France: ACM, Jan. 2023, pp. 167–181. DOI: 10.1145/3573105.3575683. URL: https://inria.hal.science/hal-03800154.

[10] FERRUCCIO GUIDI, CLAUDIO SACERDOTI COEN, and ENRICO TASSI. "Implementing type theory in higher order constraint logic programming". In: *Mathematical Structures in Computer Science* 29.8 (2019), pp. 1125–1150. DOI: 10.1017/S0960129518000427.

[11] Gérard P. Huet. "A Unification Algorithm for Typed lambda-Calculus". In: *Theor. Comput. Sci.* 1.1 (1975), pp. 27–57. DOI: 10.1016/0304-3975(75)90011-0. URL: https://doi.org/10.1016/0304-3975(75)90011-0.

[12] RALF JUNG et al. "Iris from the ground up: A modular foundation for higher-order concurrent separation logic". In: *Journal of Functional Programming* 28 (2018), e20. DOI: 10.1017/S0956796818000151.

[13] Dale Miller. "Unification under a mixed prefix". In: *Journal of Symbolic Computation* 14.4 (1992), pp. 321–358. DOI: 10.1016/0747-7171(92)90011-R.

[14] Dale Miller and Gopalan Nadathur. *Programming with Higher-Order Logic*. Cambridge University Press, 2012. DOI: 10.1017/CBO9781139021326.

[15] Gopalan Nadathur. "The Metalanguage λprolog and Its Implementation". In: *Functional and Logic Programming*. Ed. by Herbert Kuchen and Kazunori Ueda. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 1–20. ISBN: 978-3-540-44716-0.

[16] Gopalan Nadathur and Dale Miller. "An Overview of Lambda-Prolog". In: June 1988, pp. 810–827.

[17] Tobias Nipkow, Lawrence C. Paulson, and Markus Wenzel. *Isabelle/HOL - A Proof Assistant for Higher-Order Logic*. Vol. 2283. Lecture Notes in Computer Science. Springer, 2002. ISBN: 3-540-43376-7.

[18] Lawrence C. Paulson. "Set theory for verification. I: from foundations to functions". In: *J. Autom. Reason.* 11.3 (Dec. 1993), pp. 353–389. ISSN: 0168-7433. DOI: 10.1007/BF00881873. URL: https://doi.org/10.1007/BF00881873.

[19] F. Pfenning. "Elf: a language for logic definition and verified metaprogramming". In: *Proceedings of the Fourth Annual Symposium on Logic in Computer Science*. Pacific Grove, California, USA: IEEE Press, 1989, pp. 313–322. ISBN: 0818619546.

[20] F. Pfenning and C. Elliott. "Higher-order abstract syntax". In: *Proceedings of the ACM SIGPLAN 1988 Conference on Programming Language Design and Implementation*. PLDI '88. Atlanta, Georgia, USA: Association for Computing Machinery, 1988, pp. 199–208. ISBN: 0897912691. DOI: 10.1145/53990.54010. URL: https://doi.org/10.1145/53990.54010.

[21] Frank Pfenning and Carsten Schürmann. "System Description: Twelf — A Meta-Logical Framework for Deductive Systems". In: *Automated Deduction — CADE-16*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 202–206. ISBN: 978-3-540-48660-2.

[22] Brigitte Pientka and Jana Dunfield. "Beluga: A Framework for Programming and Reasoning with Deductive Systems (System Description)". In: *Automated Reasoning, 5th International Joint Conference, IJCAR 2010, Edinburgh, UK, July 16-19, 2010. Proceedings*. Ed. by Jürgen Giesl and Reiner Hähnle. Vol. 6173. Lecture Notes in Computer Science. Springer, 2010, pp. 15–21. DOI: 10.1007/978-3-642-14203-1_2. URL: https://doi.org/10.1007/978-3-642-14203-1%5C_2.

[23] Matthieu Sozeau and Nicolas Oury. "First-Class Type Classes". In: *Theorem Proving in Higher Order Logics*. Ed. by Otmane Ait Mohamed, César Muñoz, and Sofiène Tahar. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 278–293. ISBN: 978-3-540-71067-7.

[24] Enrico Tassi. "Deriving proved equality tests in Coq-elpi: Stronger induction principles for containers in Coq". In: *ITP 2019 - 10th International Conference on Interactive Theorem Proving*. Portland, United States, Sept. 2019. DOI: 10.4230/LIPIcs.CVIT.2016.23. URL: https://inria.hal.science/hal-01897468.

[25] Enrico Tassi. "Elpi: an extension language for Coq (Metaprogramming Coq in the Elpi λProlog dialect)". In: *The Fourth*

International Workshop on Coq for Programming Languages. Los Angeles (CA), United States, Jan. 2018. URL: https://inria.hal.science/hal-01637063.

[26] The Coq Development Team. *The Coq Reference Manual – Release 8.18.0*. https://coq.inria.fr/doc/V8.18.0/refman. 2023.

[27] P. Wadler and S. Blott. "How to Make Ad-Hoc Polymorphism Less Ad Hoc". In: *Proceedings of the 16th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*. POPL '89. Austin, Texas, USA: Association for Computing Machinery, 1989, pp. 60–76. ISBN: 0897912942. DOI: 10.1145/75277.75283. URL: https://doi.org/10.1145/75277.75283.

[28] Makarius Wenzel, Lawrence C. Paulson, and Tobias Nipkow. "The Isabelle Framework". In: *Theorem Proving in Higher Order Logics*. Ed. by Otmane Ait Mohamed, César Muñoz, and Sofiène Tahar. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 33–38. ISBN: 978-3-540-71067-7.

[29] Markus Wenzel. "Type classes and overloading in higher-order logic". In: *Theorem Proving in Higher Order Logics*. Ed. by Elsa L. Gunter and Amy Felty. Berlin, Heidelberg: Springer Berlin Heidelberg, 1997, pp. 307–322. ISBN: 978-3-540-69526-4.