HO unification from object language to meta language

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

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

ABSTRACT

Specifying and implementing a logic from scratch requires significant effort. Logical Frameworks and Higher Order Logic Programming Languages provide dedicated, high-level Meta Languages (ML) to facilitate this task in two key ways: 1) variable binding and substitution are simplified when ML binders represent object logic ones; 2) proof construction, and even proof search, is greatly simplified by leveraging the unification procedure provided by the ML. Notable examples of ML are Elf [13], Twelf [14], λProlog [10] and Isabelle [20] which have been utilized to implement various formal systems such as First Order Logic [5], Set Theory [12], Higher Order Logic [11], and even the Calculus of Constuctions [4].

The object logic we are interested in is Coq's [18] Dependent Type Theory (DTT), for which we aim to implement a unification procedure $\simeq_o$ using the ML Elpi [3], a dialect of λProlog. Elpi's equational theory comprises $\eta\beta$ equivalence and comes equipped with a higher order unification procedure $\simeq_\lambda$ restricted to the pattern fragment [9]. We want $\simeq_o$ to be as powerful as $\simeq_\lambda$ but on the object logic DTT. Elpi also comes with an encoding for DTT that works well for meta-programming [17, 16, 7, 6]. Unfortunately this encoding, which we refer to as $\mathcal{F}_o$, "underuses" $\simeq_\lambda$ by restricting it to first-order unification problems only. To address this issue, we propose a better-behaved encoding, $\mathcal{H}_o$, demonstrate how to map unification problems in $\mathcal{F}_o$ to related problems in $\mathcal{H}_o$, and illustrate how to map back the unifiers found by $\simeq_\lambda$, effectively implementing $\simeq_o$ on top of $\simeq_\lambda$ for the encoding $\mathcal{F}_o$.

We apply this technique to the implementation of a type-class [19] solver for Coq [18]. Type-class solvers are proof search procedures based on unification that back-chain designated lemmas, providing essential automation to widely used Coq libraries such as Stdpp/Iris [8] and TLC [1]. These two libraries constitute our test bed.

KEYWORDS

Logic Programming, Meta-Programming, Higher-Order Unification, Proof Automation

ACM Reference Format:
Enrico Tassi and Davide Fissore. XXXX 2024. HO unification from object language to meta language. In *YYY*. ACM, New York, NY, USA, 9 pages. https://doi.org/ZZZZZZZZZZZZ

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

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

1 INTRODUCTION

Specifying and implementing a logic from scratch requires significant effort. Logical Frameworks and Higher Order Logic Programming Languages provide dedicated, high-level Meta Languages (ML) to facilitate this task in two key ways: 1) variable binding and substitution are simplified when ML binders represent object logic ones; 2) proof construction, and even proof search, is greatly simplified by leveraging the unification procedure provided by the ML. Notable examples of ML are Elf [13], Twelf [14], λProlog [10] and Isabelle [20] which have been utilized to implement various formal systems such as First Order Logic [5], Set Theory [12], Higher Order Logic [11], and even the Calculus of Constuctions [4].

The object logic we are interested in is Coq's [18] Dependent Type Theory (DTT), and we want to code a type-class [19] solver for Coq [18] using the Coq-Elpi [17] meta programming framework. Type-class solvers are unification based proof search procedures that combine a set of designated lemmas in order to providing essential automation to widely used Coq libraries.

As the running example we take the `Decide` type class, from the Stdpp [8] library. The class identifies predicates equipped with a decision procedure. The following three designated lemmas (called `Instances` in the type-class jargon) state that: 1) the type `fin n`, of natural numbers smaller than `n` is finite; 2) the predicate `nfact n nf`, linking a natural number `n` to its prime factors `nf`, is decidable; 3) the universal closure of a predicate has a decision procedure if the predicate has and if its domain is finite.

```
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).
```

Under this context of instances a type-class solver is able to prove the following statement automatically by back-chaining.

```
Check _ : Decision (forall y: fin 7, nfact y 3).        (g)
```

The encoding of DTT provided by Elpi, that we will discuss at length later in section **??** and **??**, is an Higher Order Abstract Syntax (HOAS) datatype `tm` featuring (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 standard λProlog [10] the concrete syntax to abstract, at the meta level, an expression `e` over a variable `x` is «`x\ e`», and square brackets denote a list of terms separated by comma. As an example we show the encoding of the Coq term «`∀y:t, nfact y 3`»:

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

We now illustrate the 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; `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 translation of rule $(r3)$ uses the predicate `P` as a first order term for the meta language (its type is `tm`). If we try to backchain the rule $(r3)$ on the encoding of the goal (g):

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

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

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

In this paper we study a more sophisticated encoding of Coq terms allowing us to rephrase the problematic rule $(r3)$ as follows:

```
decision (all A x\ Pm x) :- link Pm P A, finite A,          (r3a)
  pi x\ decision (app[P, x]).
```

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

```
app[con"nfact", y, con"3"] = Pm y                           (p')
Pm = x\ app[con"nfact", x, con"3"]      % assignment for Pm
A = app[con"fin", con"7"]               % assignment for A
```

After unifying the head of rule $(r3a)$ with the goal, Elpi runs the premise «`link Pm A P`» that is in charge of bringing the assignment for `Pm` (that has type `tm -> tm`) back to the domain of Coq terms:

```
P = lam A a\ app[con"nfact", a, 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\`):

```
decision (app[lam A (a\ app[con"nfact", a, con"3"]), w])
```

In turn this redex prevents the rule $(r2)$ to backchain 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 sketched in the running example is that the unification procedure $\simeq_\lambda$ of the meta language is not aware of the equational theory of the object logic, even if both theories include $\eta\beta$-conversion and admit most general unifiers for unification problems in the pattern fragment $\mathcal{L}_\lambda$ [9].

Contributions. In this paper we discuss alternative encodings of Coq in Elpi 2, then we identify a minimal language $\mathcal{F}_o$in which the problems sketched here can be fully described. We then detail an encoding `comp` from $\mathcal{F}_o$ to $\mathcal{H}_o$ (the language of the meta language) and a decoding `decomp` to relate the unifiers bla bla.. TODO citare Teyjus.

2 PROBLEM STATEMENT

The equational theory of Coq's Dependent Type Theory is very rich. In addition to the usual $\eta\beta$-equivalence for functions, terms (hence types) are compared up to definition unfolding and fixpoint unrolling. Still, for efficiency and predictability reasons, most form of automatic proof search employ a unification procedure that captures a simpler one, just $\eta\beta$, and that solves higher-order problems restricted to the pattern fragment $\mathcal{L}_\lambda$ [9]. We call this unification procedure $\simeq_o$.

The equational theory of the meta language Elpi that we want to use to implement a form of proof automation is strikingly similar, since it it comprises $\eta\beta$ (for the meta language functions), and the unification procedure $\simeq_\lambda$ solves higher-order problems in $\mathcal{L}_\lambda$.

In spite of the similarity the link between $\simeq_\lambda$ and $\simeq_o$ is not trivial, since the abstraction and application term constructors the two unification procedures deal with are different. For example

`x\ f x`	$\simeq_\lambda$	`f`
`lam A x\ app[con"f", x]`	$\simeq_o$	`con"f"`
`lam A x\ app[con"f", x]`	$\not\simeq_\lambda$	`con"f"`
`P x`	$\simeq_\lambda$	`x`
`app[P, x]`	$\simeq_o$	`x`
`app[P, x]`	$\not\simeq_\lambda$	`x`

One could ignore this similarity, and "just" describe the object language unification procedure in the meta language, that is crafting a `unif` predicate to be used as follows in rule $(r3)$:

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

This choice would underuse the logic programming engine provided by the metalanguage since by removing any datum from the head of rules indexing degenerates. Moreover the unification procedure built in the meta language is likely to be faster than one implemented in it, especially if the meta language is interpreted as Elpi is.

To state precisely the problem we solve we need a $\mathcal{F}_o$ representation of DTT terms and a $\mathcal{H}_o$ one. We call $=_o$ the equality over ground terms in $\mathcal{F}_o$, $=_\lambda$ the equality over ground terms in $\mathcal{H}_o$, $\simeq_o$ the unification procedure we want to implement and $\simeq_\lambda$ the one provided by the meta language. TODO extend $=_o$ and $=_\lambda$ with reflexivity on uvars.

We write $t_1 \simeq_\lambda t_2 \mapsto \sigma$ when t_1 and t_2 unify with substitution σ, we write σt for the application of the substitution to t, $\sigma \subseteq \sigma'$ when σ is more general than σ', and we assume that the unification of our meta language is correct:

$$t_i \in \mathcal{L}_\lambda \Rightarrow t_1 \simeq_\lambda t_2 \mapsto \rho \Rightarrow \rho t_1 =_\lambda \rho t_2 \tag{1}$$

$$t_i \in \mathcal{L}_\lambda \Rightarrow \rho t_1 =_\lambda \rho t_2 \Rightarrow \exists \rho', t_1 \simeq_\lambda t_2 \mapsto \rho' \wedge \rho' \subseteq \rho \tag{2}$$

We illustrate a compilation $\langle s \rangle \mapsto (t, l)$ that maps a term s in $\mathcal{F}_o$ to a term t in $\mathcal{H}_o$ and a list of links l. The links connect unification variables in $\mathcal{H}_o$ with variables in $\mathcal{F}_o$ and are used to decompile the assignment, $\langle \sigma, l \rangle^{-1} \mapsto \rho$.

Given

$$\langle s_1 \rangle \mapsto (t_1, l_1) \wedge \langle s_2 \rangle \mapsto (t_2, l_2)$$

we define

$$s_1 \simeq_o s_2 \mapsto \rho \stackrel{def}{=} t_1 \simeq_\lambda t_2 \mapsto \sigma \wedge \langle \sigma, l_1 + l_2 \rangle^{-1} \mapsto \rho$$

Where $l_1 + l_2$ is the list concatenation of links.

We write $s \in \mathcal{L}_\lambda$ if all unif variables in s are applied to distinct bound variables.

$$s_i \in \mathcal{L}_\lambda \Rightarrow s_1 \simeq_o s_2 \mapsto \rho \Rightarrow \rho s_1 =_o \rho s_2 \quad (3)$$

$$s_i \in \mathcal{L}_\lambda \Rightarrow \rho s_1 =_o \rho s_2 \Rightarrow \exists \rho', s_1 \simeq_o s_2 \mapsto \rho' \wedge \rho' \subseteq \rho \quad (4)$$

$$\rho s_1 =_o \rho s_2 \Rightarrow \rho' \subseteq \rho \Rightarrow \rho' s_i \in \mathcal{L}_\lambda \Rightarrow \rho' s_1 \simeq_o \rho' s_2 \quad (5)$$

Properties 3 and 4 state, respectively, that in $\mathcal{L}_\lambda$ the implementation of $\simeq_o$ is correct, complete and returns the most general unifier.

Property 5 states that $\simeq_o$ is resilient to problems outside $\mathcal{L}_\lambda$ if a third party provides a (partial) solution for its problem. Since we are interested in using $\simeq_o$ in a proof search procedure, made of a sequence of unification problems, not necessarily in $\mathcal{L}_\lambda$. In practice it is often the case the order in which these problems are stated matters. A Typical example is the following problem

```
app [F, con"a"] = app[F, con"a", con"a"]
```

preceded by

```
F = lam x\app[const f,x,x]
```

becomes solvable in DTT trivially, since the term is ground (hence in $\mathcal{L}_\lambda$), but is one substitutes F in the LHS does not find, structurally, the RHS hence $\simeq_\lambda$ would fail (since $\simeq_\lambda$ does not know about the β rule of DTT). Our compiler takes care of making property 5 hold, see section XXX.

Property 4 is also relevant to use $\simeq_o$ for logic programming. In particular we want failures to occur as early as possible, so want the decomp phase to take place immediately after $\simeq_\lambda$, and fail if need be. This becomes particularly important since compile may introduce two ho variables for the same fo one, leaving the task of unifying the solutions to decomp.

3 ALTERNATIVE ENCODINGS AND RELATED WORK

Paper [2] introduces semi-shallow.

Our encoding of DTT may look "semi shallow" since we use the meta-language lambda abstraction but not its application (for the terms of type `tm`). A fully shallow encoding unfortunately does not fit our use case, although it would make the running example work:

```
finite (fin N).
decision (nfact N NF).
decision (all A x\ P x) :- finite A, pi x\ decision (P x).
```

There are two reasons for dismissing this encoding. The first one is that in DTT it is not always possible to adopt it since the type system of the meta language is too weak to accommodate terms with a variable arity, like the following example:

```
Fixpoint arr T n := if n is S m then T -> arr T m else T.
Definition sum n : arr nat n := ...
Check sum 2   7 8   : nat.
Check sum 3   7 8 9 : nat.
```

The second reason is the encoding for Coq is used for meta programming the system, hence it must accommodate the manipulation of terms that are now know in advance (not even defined in Coq) without using introspection primitives such as Prologs's `functor` and `arg`.

In the literature we could find a few related encoding of DTT. TODO In [4] is related and make the discrepancy between the types of ML and DTT visible. In this case one needs 4 application nodes. Moreover the objective is an encoding of terms, proofs, not proof search. Also note the conv predicate, akin to the unif we rule out.

TODO This other paper [15] should also be cited.

None of the encodings above provide a solution to our problem.

4 PRELIMINARIES: $\mathcal{F}_o$ AND $\mathcal{H}_o$

In order to reason about unification we provide a description of the $\mathcal{F}_o$ and $\mathcal{H}_o$ languages where unification variables are first class terms, i.e. they have a concrete syntax. We keep these languages minimal, for example we omit the `all` quantifier of DTT we used in the example in Section 1.

```
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 nat -> fm.               type uva nat -> list tm -> tm.
```

Figure 1: $\mathcal{F}_o$ and $\mathcal{H}_o$ language

In the case of $\mathcal{F}_o$ unification variables `fuva` have no explicit scope: Unification variables standing for functions are applied their arguments via the `fapp` constructor. For example in the statement of the instance `forall_dec` the term `P x` is represented as `fapp[fuva N, x]`, where `N` is of type `nat` and `x` is a bound variable.

In $\mathcal{H}_o$ the representation of `P x` is instead `uva N [x]`. We say that the unification variable `uva N L` is in $\mathcal{L}_\lambda$ iff `distinct-names L` holds.

```
type distinct-names list tm -> o.
distinct-names [].
distinct-names [X|XS] :- name X, not(mem X XS),
  distinct-names XS.
```

The `name` builtin predicate tests if a term is a bound variable. The compiler **??** needs to support terms outside $\mathcal{L}_\lambda$ for practical reasons, so we don't assume all out terms are in $\mathcal{L}_\lambda$ but rather test.

In both languages unification variables are identified by a natural number, which can be seen as a memory address. The memory and its associated operations are described below:

```
typeabbrev memory A (list (option A)).
type set?   nat -> memory A -> A -> o.
type unset  nat -> memory A -> o.
type assign nat -> memory A -> A -> memory 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.

Since in $\mathcal{H}_o$ unification variables have a scope, their solution needs to be abstracted over it in order to enable the instantiation of a single solution to different scopes. On the contrary solutions to $\mathcal{F}_o$variables are plain terms.

```
typeabbrev fsubst (memory ftm).
kind assmt type.
type abs (tm -> assmt) -> assmt.
```

```
type val tm -> assmt.
typeabbrev subst (memory assmt).
```

We call `fsubst` the memory of $\mathcal{F}_o$, while we call `subst` the one of $\mathcal{H}_o$. Both have the invariant that they are not cyclic, TODO explain.

4.1 Equational theory and Unification

here we give the functions/signatures to express the properties 3-5 in the problem statement

Together with the description of the terms of the language, we need some auxiliary functions to perform operations like term equality, unification, dereferencing. There predicates are supposed to be implemented in the OL and the ML following respectively their specification. In the following few paragraphs we give a brief definition of them.

Term dereferencing: ρs and σt. Since in our encoding we explicitly carry a substitution we need to define the operation that applies it to a term. Its definition takes care to normalize (flatten) applications, for example it turns `(app [app [con"f",con"a"],con"b"])` into `(app [con"f",con"a",con"b"])`.

dereference variables of the two languages. This is particularly useful to check if two terms in the OL (resp. in the ML) are equal. The constructors representing rigid terms, namely `app`, `lam` and `con`, make the dereferencing procedure to recurse over the their subterms. The code below display this behavior for the dereferencing performed by the OL:

```
type fderef fsubst -> fm -> fm -> o.
% flattening
fderef S (fapp [fuva N|A]) R :- set? N S (fapp B), !,
  append A B C, fderef S (fapp C) R.
% traversal
fderef S (fapp A) (fapp B) :- map (fderef S) A B.
fderef S (flam F) (flam G) :-
  pi x\ fderef S x x => fderef S (F x) (G x).
fderef _ (fcon C) (fcon C).
% dereferencing
fderef S (fuva N) R :- set? N S T, fderef S T R.
fderef _ (fuva N) (fuva N) :- unset N S.
```

We use the cut operator to keep the code compact. It is possible to rewrite the rule for application traversal so that it is mutually exclusive with the first one, but that requires a rather verbose analysis of the head of `A`.

The corresponding code for $\mathcal{H}_o$ is similar, we only show the last two rules that differ in a substantial way:

```
type deref subst -> tm -> tm -> o.
% ... similar to above ...
deref S (uva N A) R :- set? N S F, move F A T, deref S T R.
deref S (uva N A) (uva N B) :- unset N S, map (deref S) A B.
type move assignment -> list tm -> tm -> o.
move (abs F) [X | L] R :- move (F X) L R.
move (val A)         [] A :- !.
move (val (app A))    L (app X) :- append A L X.
move (val (uva N A)) L (uva N X) :- append A L X.
move (val (con H))    L (app [con H | L]).
```

```
type (=o) ftm -> ftm -> o.
% congruence
fapp A =o fapp B :- map (=o) A B.
flam F =o flam G :- pi x\ x =o x => F x =o G x.
fcon C =o fcon C.
fuva N =o fuva N.
% eta
flam F =o T :- pi x\ beta T [x] (T' x),                    (η1)
  x =o x => F x =o T' x.
T =o flam F :- pi x\ beta T [x] (T' x),                    (η2)
  x =o x => T' x =o F x.
% beta
fapp [flam X | TL] =o T :- beta (flam X) TL T', T' =o T.  (β1)
T =o fapp [flam X | TL] :- beta (flam X) TL T', T =o T'.  (β2)
```

Figure 2: Equal predicate OL

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

Figure 3: Equal predicate ML

Note that when the substitution `S` maps a unification variable `N` to an assignment `F` we ....

Important!!! A different reasoning is to be addressed to the variables of the ML. Firstly, a meta variable cannot appear in the `app` node as the first element of the list, we will explain why in section 5

Term equality: $=_o$ vs. $=_\lambda$. We can test if two terms are equal following the equational theory of the language being considered. In fig. 2 we provide an implementation of the $=_o$ predicate. The first four rules check if the two terms are equal regarding the structure of the current node, that is, two terms are equal if they have same head and if recursively each subterm is two by two equal. Moreover, since the theory of the OL accepts η- and β-equivalence, then we implement the corresponding rules.
The equality relation for the ML, accepts $\eta\beta$-equivalence between terms of the ML. Recall that `abs x\ f x`, is a valid η expansion of the function `f` and that `lam x\ app[f, x]` is not that equivalent to `f` at meta level. However, since we are interested in using the unification procure of the ML, by eq. (1), we can use the $\simeq_\lambda$ relation to test, when needed if two terms are equal in the ML.

Term unification: $\simeq_o$ vs. $\simeq_\lambda$. The last but not least important relation we should take care of before presenting our full algorithm aiming to unify terms of the OL in the ML and provide the substitution produced in the ML to the OL, is term unification. This procedure is a more powerful version of the equal predicate, since unification checks if two terms can be equal be assigning unification variables. In our representation, variable assignment (or refinement) is performed by modifying the corresponding substitution mapping. We will not give an implementation of $\simeq_o$, since we are giving an implementation of it using our algorithm, see **??**.

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

On the other hand, unification in the ML needs to be defined. In fig. 4, we give an implementation of $\simeq_\lambda$ but that is actually what our meta language provides as a builtin.

This predicate has four arguments, the two terms t_1 and t_2 to unify, the old substitution map ρ_1, and the new substitution map ρ_2, with the invariant $\rho_1 \subseteq \rho_2$. The first three rules unify terms with same rigid heads, and call the unification relation on the sub-terms. If t_1 (resp. t_2) is an assigned variables, t_1 is dereferenced to t_1' (resp. t_2') and the unification is called between t_1' and t_2 (resp. t_1 and t_2'). If both terms are unification variables, we test that their arguments are in the pattern fragment, we allocate a new variable w in ρ_1 such that w is the pruning of the arguments of t_1 and t_2, we assign both t_1 and t_2 to w and return the new mapping ρ_2 containing all the new variable assignment. Finally, if only one of the two terms is an unification variable v, after having verified that v does not occur in the other term t, we bind v to t and return the new substitution mapping.

OLD

A key property needed in unification is being able to verify if two terms are equal wrt a given equational theory. This relation allow to compare terms under a certain substitution mapping, so that any time a variable v is assigned in a subterm, a dereferencing of v is performed. After variable dereferencing, the test for equality is continued on the new-created subterm.

The base equality function over terms can be defined as follows:

The solution we are proposing aim to overcome these unification issues by 1) compiling the terms t and u of the OL into an internal version t' and u' in the ML; 2) unifying t' and u' at the meta level instantiating meta variables; 3) decompiling the meta variable into terms of the OL; 4) assigning the variables of the OL with the decompiled version of their corresponding meta variables. We claim that t and u unify if and only if t' and u' unify and that the substitution in the object language is the same as the one returned by the ML.

same or $\supseteq$ or $\subseteq$

In the following section we explain how we deal with term (de)compilation and links between unification variables.

5 COMPILATION

TODO: Goal: $s_1 \simeq_o s_2$ is compiled into $t_1 \simeq_\lambda t_2$

TODO: What is done: uvars `fo_uv` of OL are replaced into uvars `ho_uv` of the ML

TODO: Each `fo_uv` is linked to an `ho_uv` of the OL

TODO: Example: `lam x\ app[uv 0, x]` $\simeq_\lambda$ `lam x\ c"f"`

TODO: Links used to instantiate vars of elpi

TODO: After all links, the solution in links are compacted and given to coq

TODO: It is not so simple, see next sections (multi-vars, eta, beta)

The compilation step is meant to recover the higher-order variables of the OL, expressed in a first order way, by replacing them with higher-order variables in the ML. In particular, every time a variable of the OL is encountered in the original term, it is replaced with a meta variable, and if the OL variable is applied to a list of distinct names L, then this list becomes the scope of the variable. For all the other constructors of `tm`, the same term constructor is returned and its arguments are recursively compiled. The predicate in charge for term compilation is:

```
type comp tm -> tm -> links -> links -> subst -> subst -> o.
```

where, we take the term of the OL, produce the term of the ML, take a list of link and produce a list of new links, take a substitution and return a new substitution.

In particular, due to programming constraints, we need to drag the old subst and return a new one extended, if needed, with the new declared meta-variables.

The following code

```
kind link type.
type link nat -> nat -> nat -> subst.
```

defines a link, which is a relation between to variables indexes, the first being the index of a OL variable and the second being the index of a ML variable. The third integer is the number of term in the scope of the two variables, or equivalently, in a typed language, their arity.

integer or nat?

As an example, let's study the following unification problem (a slightly modified version from section 1):

```
lam x\ app[c"decision", app[c"nfact", x, c"3"]] ≃o
  lam x\ app [c"decision", app[uv 0, x]]
```

we have the main unification problem where the nested `app` nodes have lists of different lengths making the unification to fail. The compilation of these terms produces a new unification problem with the following shape:

```
lam x\ app[c"decision", app[c"nfact", x, c"3"]] ≃λ
  lam x\ app [c"decision", uv 1 [x]]
```

The main difference is the replacement of the subterm `app[uv 0, x]` of the OL with the subterm `uv 0 [x]`. Variable indexes are chosen by the ML, that is, the index `0` for that unification variable of the OL term has not the sam meaning of the index `0` in the ML. There exists two different substitution mapping, one for the OL and one for the ML and the indexes of variable point to the respective substitution.

6 USE OF MULTIVARS

6.1 Problems with η

TODO: The following goal: `X = lam x\ lam y\ Y x y, X = lam x\ f`

TODO: The snd unif pb, we have to unif `lam x\ lam y\ Y x y` with `lam x\ f`

TODO: It is not doable, with the same elpi var

TODO: An other example:

```
@lam x\ @app[@f, @app[@X, x]] = @Y, (@lam x\ x) = @X.
```

6.2 Problems with β

TODO: The following goal: `X = lam x\ x, app[X, 3] = 3`

TODO: We use links-beta

6.3 Tricky examples

```
triple ok (@lam x\ @app[@f, @app[@X, x]]) @Y,
triple ok @X (@lam x\ x),
triple ok @Y @f
```

7 FIRST ORDER APPROXIMATION

TODO: Coq can solve this: `f 1 2 = X 2`, by setting X to f 1
TODO: We can re-use part of the algo for β given before

8 UNIF ENCODING IN REAL LIFE

TODO: Il ML presentato qui è esattamente elpi
TODO: Il OL presentato qui è esattamente coq
TODO: Come implementatiamo tutto ciò nel solver

9 RESULTS: STDPP AND TLC

TODO: How may rule are we solving?
TODO: Can we do some perf test

10 CONCLUSION

REFERENCES

[1] Arthur Charguéraud. "The Optimal Fixed Point Combinator". In: *Interactive Theorem Proving*. Ed. by Matt Kaufmann and Lawrence C. Paulson. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 195–210. ISBN: 978-3-642-14052-5.

[2] Cvetan Dunchev, Claudio Sacerdoti Coen, and Enrico Tassi. "Implementing HOL in an Higher Order Logic Programming Language". In: *Proceedings of the Eleventh Workshop on Logical Frameworks and Meta-Languages: Theory and Practice*. LFMTP '16. Porto, Portugal: Association for Computing Machinery, 2016. ISBN: 9781450347778. DOI: 10.1145/2966268.2966272. URL: https://doi.org/10.1145/2966268.2966272.

[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] 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.

[8] 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.

[9] 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.

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

[11] 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.

[12] 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.

[13] F. Pfening. "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.

[14] 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.

[15] Colin Rothgang, Florian Rabe, and Christoph Benzmüller. "Theorem Proving in Dependently-Typed Higher-Order Logic". In: *Automated Deduction – CADE 29*. Ed. by Brigitte Pientka and Cesare Tinelli. Cham: Springer Nature Switzerland, 2023, pp. 438–455. ISBN: 978-3-031-38499-8.

[16] 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.

[17] 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.

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

[19] 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.

[20] 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.

APPENDIX

Note that `(a infix b) c d` de-sugars to `(infix) a b c d`.

```
type (≃λ) tm -> tm -> subst -> subst -> o.
% Congruence
(app A ≃λ app B) S S1 :- fold2 (≃λ)A B S S1.
(lam F ≃λ lam G) S S1 :- pi x\ (pi S\ (x ≃λ x) S S) => (F x ≃λ G x) S S1.
≃λ (con C) (con C) S S.
% deref
(uva N A ≃λ T) S S1 :- set? N S F, move F A T1, (T1 ≃λ T) S S1.
(T ≃λ uva N A) S S1 :- set? N S F, move F A T1, (T ≃λ T1) S S1.
% flex-flex
(uva N A ≃λ uva M B) S S3 :-  unset M, unset N,
  distinct-names A, distinct-names B,
  new S W S1, prune W Args1 B Ass,
  assign N S1 Ass S2, assign M S2 Ass S3.
% assignment
(uva N A ≃λ T) S S1 :- distinct-names A, not (T = uva _ _), not_occ N S T,
  bind A T T1, assign N S T1 S1.
(T ≃λ uva N A) S S1 :- distinct-names A, not (T = uva _ _), not_occ N S T,
  bind A T T1, assign N S T1 S1.

type distinct-names list tm -> o.
distinct-names [].
distinct-names [X|XS] :- name X, not(mem X XS),
distinct-names XS.

typeabbrev memory A (list (option A)).
type set? nat -> memory A -> A -> o.
set? N S T :- nth N S (some T).
type unset nat -> memory A -> o.
unset N S :- nth N S none.
type assign nat -> memory A -> A -> memory A -> o.
assign z [none|M] T [some T|M].
assign (s N) [X|M] T [X|M1] :- assign N M T M1.
kind nat type.
type z nat.
type s nat -> nat.
type nth nat -> list A -> A -> o.
nth z [X|_] X.
nth (s N) [_|L] X :- nth N L X.

type new memory A -> nat -> memory A -> o.
type prune .
type move .
type beta.
TODO
```

Figure 4: Implementation of the $\simeq_\lambda$ predicate for $\mathcal{H}_o$