

# A weak HOAS approach to the POPLmark Challenge

Alberto Ciaffaglione

Università di Udine, Italia  
Dipartimento di Matematica e Informatica  
via delle Scienze, 206 - 33100 Udine, Italia  
alberto.ciaffaglione@uniud.it

Ivan Scagnetto

Università di Udine, Italia  
Dipartimento di Matematica e Informatica  
via delle Scienze, 206 - 33100 Udine, Italia  
ivan.scagnetto@uniud.it

Capitalizing on previous encodings and formal developments about nominal calculi and type systems, we propose a weak Higher-Order Abstract Syntax formalization of the type language of pure System  $F_{<}$ , within Coq, a proof assistant based on the Calculus of Inductive Constructions.

Our encoding allows us to accomplish the proof of the transitivity property of algorithmic subtyping, which is in fact the first of the three tasks stated by the POPLmark Challenge, a set of problems that capture the most critical issues in formalizing programming language metatheory.

## 1 Introduction

It is well known that formal proofs about programming language metatheory and semantics are long and tedious, and that their complexity is essentially due to the management of the details; actually, it may happen that small mistakes or missed subtle cases cause to invalidate large amounts of work, with this effect that worsens as languages scale. Automated proof assistants can help to ease the problem, with several potential benefits: it may be simpler to reuse work, to keep definitions and proofs consistent, to ensure a firm relationship between theory and implementation. Nevertheless, it is apparent that computer-aided formal reasoning is not commonplace, even for programming language designers and researchers. Therefore, the POPLmark Challenge [3] has proposed a framework and a set of benchmarks for measuring the progress in the area, envisaging a future in which research papers on programming languages will be routinely accompanied by an electronic appendix with machine-checked proofs.

The Challenge concerns a set of problems about the metatheory of a variant of the System  $F_{<}$ : [33], *a.k.a.* polymorphic, or second-order, lambda calculus. This choice has the intent to pick out some features of programming languages that are known to be difficult to formalize; in such a way, the problematic aspects can be exploited to compare alternative technologies that have been successfully experimented on specific areas. In detail, the Challenge concentrates on variable binding, complex recursion and induction, definition and proof reuse, and experimentation of generated sample programs.

In this paper we focus on the *first task* among the three ones in the Challenge suite, by considering System  $F_{<}$ 's *type language*. Essentially, such an object system features variable binding and subtyping. In fact, we adopt a methodology for encoding and reasoning formally on System  $F_{<}$ : which takes most advantage of the features provided by logical frameworks based on *type theories*, and carry out our effort within the Coq implementation [38] of the *Calculus of Inductive Constructions* (CC<sup>Ind</sup>) [13, 31].

A common problem is that encoding and reasoning about a formal system adds further complexity to already cumbersome judgments and proofs. In order to be practically useful, therefore, it is important that the formalization is as clean and compact as possible: ideally, most (if not all) details implicitly taken for granted working with paper and pencil should be automatically provided by the formal development.

A central point pursued by the Challenge is an efficient management of inductively-defined structures with *binders*. To this end, we employ *Higher-Order Abstract Syntax* (HOAS) [19, 32], an approach that uses binders *in the metalanguage* to represent binders in the object language, thus providing an high level of abstraction. More precisely, since we work in a type theory with induction, we use *weak* HOAS [24]: binders are encoded as *second-order* term constructors that take as arguments functions over a parametric, open (*i.e.*, non-inductive) type of *variables*. In this way, while we keep benefiting from inductive definition and proof principles, we gain the advantage that  $\alpha$ -conversion of abstractions and capture-avoiding substitution of variables for variables are automatically ensured by the metalanguage.

The main drawback of (weak) HOAS in  $\text{CC}^{\text{Ind}}$  (and Coq) is that it is difficult to reason *about* the encodings, because there is a limited support for higher-order recursion and induction. To overcome this problem, we adopt the *Theory of Contexts* (ToC) [23], a small set of axioms which can be added to  $\text{CC}^{\text{Ind}}$  to represent some basic and natural properties of variable and term *contexts*. It is apparent that we lose full constructivity by using axioms; on the other hand, the ToC requires a very low mathematical and logical overhead for porting to the formal setting the arguments on paper.

In the end, by exploiting the above tools, we fulfill the first task of the Challenge: that is, we prove the *transitivity* and the *narrowing* properties of algorithmic subtyping for System  $F_{<}$ . We believe that our result is relevant because the present one is the *first* weak HOAS approach to the Challenge<sup>1</sup>, hence it provides extra feedback about the two issues of representing and reasoning about binders and carrying out formal proofs by mutual, nested structural induction on System  $F_{<}$ 's type language.

In the next two sections, we recap the first task of the Challenge and we rephrase it *on paper* as a preliminary step towards its formal treatment in  $\text{CC}^{\text{Ind}}$ . In the core Section 4 we present and discuss the formalization itself (the Coq code is available at the web appendix of this paper [12]), and in the final sections we connect it to the related literature and to the Challenge metrics of success.

## 2 Algorithmic subtyping in the System $F_{<}$ :

The POPLmark Challenge [3] addresses the metatheory of a call-by-value variant of System  $F_{<}$ , a calculus of moderate scale. The first part of the Challenge, which we deal with in the present paper, focuses just on the *type language*, that we consider in its *pure* version here, *i.e.*, without record types.

The syntax of *types* features variables (taken, as usual, from an infinite set of distinct symbols), the constant *Top* (the supertype of any type), functions, and bounded quantification (*i.e.*, universal types):

$$\begin{array}{llll} \text{Type} : & S, T ::= X & \text{type variable} & \text{Top} & \text{maximal type} \\ & S \rightarrow T & \text{function type} & \forall X <: S. T & \text{universal type} \end{array}$$

Universal types, which are the individual characteristic of  $F_{<}$ , arise by combining polymorphism and subtyping: on the one hand types such as  $\forall X. T$  are intended to specify the type of polymorphic functions; on the other hand bounded universal quantifiers such as  $\forall X <: S$  carry subtyping constraints. Actually, the universal type  $\forall X <: S. T$  has the effect of binding the occurrence of  $X$  in  $T$ , but not in  $S$ .

The *type environments* are formed by subtyping constraints too, involving type variables and types:

$$\begin{array}{ll} \text{Env} : & \Gamma ::= \emptyset & \text{empty type environment} \\ & \Gamma, X <: T & \text{type variable binding} \end{array}$$

Type variables within environments have to respect a *scoping* discipline: only fresh variables can be introduced, that is,  $X \notin \text{dom}(\Gamma)$ ; moreover, such variables cannot occur free in the type they are bound to,

<sup>1</sup>Among the proposed solutions collected by the Challenge web page [4], our encoding is also the first HOAS one *in Coq*.

*i.e.*,  $X \notin \text{fv}(T)$ ; finally, the variables that appear free in  $T$  have to be already collected in the environment  $\Gamma$ . Hence, a typical two-variable well-scoped environment is  $X <: \text{Top}$ ,  $Y <: X^2$ .

*Algorithmic* subtyping,  $\Gamma \vdash S <: T$ , captures the intuition that “ $S$  is a subtype of  $T$  under assumptions  $\Gamma$ ”, which means that “an instance of  $S$  may be safely used wherever an instance of  $T$  is expected”. It is defined by induction and it is intended to concern only *well-scoped* types (*i.e.*, when  $\Gamma \vdash S <: T$  is derived, all the type variables that occur free in  $S$  and  $T$  have to be in the domain of  $\Gamma$ ):

$$\begin{array}{c} \frac{}{\Gamma \vdash S <: \text{Top}} \text{(Top)} \quad \frac{}{\Gamma \vdash X <: X} \text{(Refl)} \quad \frac{X <: U \in \Gamma \quad \Gamma \vdash U <: T}{\Gamma \vdash X <: T} \text{(Trans)} \\ \\ \frac{\Gamma \vdash T_1 <: S_1 \quad \Gamma \vdash S_2 <: T_2}{\Gamma \vdash S_1 \rightarrow S_2 <: T_1 \rightarrow T_2} \text{(Arr)} \quad \frac{\Gamma \vdash T_1 <: S_1 \quad \Gamma, X <: T_1 \vdash S_2 <: T_2}{\Gamma \vdash \forall X <: S_1. S_2 <: \forall X <: T_1. T_2} \text{(All)} \end{array}$$

The Challenge focuses on the algorithmic version of subtyping because its ultimate goal is the *experimentation* of real implementations of the formalized definitions. On the other hand, being syntax-directed, algorithmic subtyping is easier *to reason with* than its equivalent, more familiar *declarative* presentation, where the rules (*Refl*) and (*Trans*) are replaced by the following ones:

$$\frac{X <: U \in \Gamma}{\Gamma \vdash X <: U} \text{(1)} \quad \frac{}{\Gamma \vdash S <: S} \text{(2)} \quad \frac{\Gamma \vdash S <: T \quad \Gamma \vdash T <: U}{\Gamma \vdash S <: U} \text{(3)}$$

In fact, the first task of the Challenge addresses the relationship between the two subtyping versions, as it consists to prove that the *transitivity* property (3) is a derivable property within the algorithmic system (the same holds for reflexivity (2), which is not problematic).

The proof of the transitivity is challenging essentially in two respects: it has to be proved *together* with the *narrowing* property, and such a proof requires a *mutual and nested induction* proof argument.

**Proposition 1** (Transitivity and Narrowing). *If  $\Gamma \vdash S <: Q$  and  $\Gamma \vdash Q <: T$ , then  $\Gamma \vdash S <: T$ .*

*If  $\Gamma, X <: Q, \Delta \vdash M <: N$  and  $\Gamma \vdash P <: Q$ , then  $\Gamma, X <: P, \Delta \vdash M <: N$ .*

*Proof.* By induction on the structure of the type  $Q$ .

The proof for transitivity proceeds by an inner induction on the structure of the derivation  $\Gamma \vdash S <: Q$ , with a case analysis on the final rule of such a derivation and on that of the second hypothesis  $\Gamma \vdash Q <: T$ . We illustrate the crucial case when both the derivations end with an application of the (*All*) rule:

$$\frac{\frac{\vdots}{\Gamma \vdash Q_1 <: S_1} \quad \frac{\vdots}{\Gamma, X <: Q_1 \vdash S_2 <: Q_2}}{\Gamma \vdash S \equiv \forall X <: S_1. S_2 <: \forall X <: Q_1. Q_2 \equiv Q} \text{(All)} \quad \frac{\frac{\vdots}{\Gamma \vdash T_1 <: Q_1} \quad \frac{\vdots}{\Gamma, X <: T_1 \vdash Q_2 <: T_2}}{\Gamma \vdash Q \equiv \forall X <: Q_1. Q_2 <: \forall X <: T_1. T_2 \equiv T} \text{(All)}$$

To conclude  $\Gamma \vdash \forall X <: S_1. S_2 <: \forall X <: T_1. T_2$  via the (*All*) rule, two premises are needed: first,  $\Gamma \vdash T_1 <: S_1$  may be derived by induction hypothesis from the third and the first subderivations; however, the induction hypothesis cannot be applied to the second and fourth subderivations (to deduce  $\Gamma, X <: T_1 \vdash S_2 <: Q_2$ ), because their environments are different. Hence, the narrowing property, *i.e.*, the *outer* induction hypothesis (being  $Q_1$  *structurally smaller* than  $Q$ ) has to be exploited, to derive  $\Gamma, X <: T_1 \vdash S_2 <: Q_2$  from the second and the third subderivations. Then, to construct the required derivation  $\Gamma, X <: T_1 \vdash S_2 <: Q_2$

<sup>2</sup>We will give formal definitions of the mentioned concepts (well-known, though) in Section 3.

from this last hypothesis and the fourth subderivation, it is necessary to apply again the *outer* induction hypothesis (the transitivity itself, with  $Q_2$  structurally smaller than  $Q$ ).

Similarly, the proof for narrowing proceeds by an inner induction on the structure of the derivation  $\Gamma, X <: Q, \Delta \vdash M <: N$ , again with a case analysis on the final rule applied. The treatment of this “twin” property is even subtler when the last rule applied is (*Trans*), and  $M$  is exactly  $X$ :

$$\frac{\begin{array}{c} \vdots \\ \hline \Gamma, X <: Q, \Delta \vdash Q <: N \end{array}}{\Gamma, X <: Q, \Delta \vdash M \equiv X <: N} \text{ (Trans)}$$

Now,  $\Gamma, X <: P, \Delta \vdash Q <: N$  may be derived by induction hypothesis, and  $\Gamma, X <: P, \Delta \vdash P <: Q$  via a straightforward *weakening* property. This time, the *outer* induction hypothesis has to be exploited *with the same*  $Q$ ; that is, the transitivity property is used to deduce  $\Gamma, X <: P, \Delta \vdash P <: N$  from the two inferred derivations. In the end, an application of the (*Trans*) rule allows to obtain  $\Gamma, X <: P, \Delta \vdash X <: N$ .

The present proof is reported in [3, 33], albeit not in a fully detailed fashion.  $\square$

We notice finally that the presentation of System  $F_{<}$ : [3], that we have displayed and commented on, leaves implicit those aspects that form the core of the Challenge:  $\alpha$ -conversion and capture-avoiding substitution (as in standard practice), and the well-scoping discipline (*on purpose*).

### 3 An alternative formulation of System $F_{<}$ :

We give now an alternative presentation of System  $F_{<}$ ’s subtyping, making explicit some concepts that have been left implicit in the original formulation reported in Section 2. While carrying out this step, we are mainly inspired by the features provided by logical frameworks based on type theory.

We use here the same syntax for *types* as in Section 2; on the other hand, we perform small changes on the *subtyping* system, and we prove that the new version is equivalent to the original one. The formalization in  $CC^{\text{Ind}}$  of the resulting system will be then discussed in the following section.

We manage the *type environment* as a concrete pair-component collection, thus pursuing a *sequent-style* encoding of subtyping; consequently, we state formally two concepts related to the environment itself. First, we define the *closure* of types  $T$  *w.r.t.* environments  $\Gamma$  (a sort of compatibility) via the relation  $\text{closed} \subseteq \text{Type} \times \text{Env}$ , to state that the free variables of  $T$  have to appear in the domain of  $\Gamma$ . Further, the *well-formedness* of environments  $\text{ok} \subseteq \text{Env}$  prescribes that, when a new pair  $\langle X, T \rangle$  makes an environment  $\Gamma$  grow,  $X$  must both be fresh *w.r.t.*  $\Gamma$  and not appear in  $T$ , and  $T$  has to be closed *w.r.t.*  $\Gamma$ .

In what follows, we write  $f_v(T)$  for the type variables occurring free in a type  $T$ , and overload the symbols “ $\in, \notin$ ” in a way which is clear from the context.

**Definition 1** (Closure, Well-formedness). *For  $\Gamma = \langle X_1, T_1 \rangle, \dots, \langle X_n, T_n \rangle$  an environment,  $T$  a type, we define the domain of  $\Gamma$  and the predicates *closed* and *ok* as follows:*

$$\begin{array}{l} \text{dom}(\Gamma) \triangleq \{X_1, \dots, X_n\} \quad \text{closed}(T, \Gamma) \triangleq \forall Y. Y \in f_v(T) \Rightarrow \exists U. \langle Y, U \rangle \in \Gamma \\ \frac{}{\text{ok}(\emptyset)} \text{ (ok-}\emptyset\text{)} \quad \frac{\text{ok}(\Gamma) \quad X \notin \text{dom}(\Gamma) \quad \text{closed}(T, \Gamma)}{\text{ok}(\Gamma, \langle X, T \rangle)} \text{ (ok-pair)} \end{array}$$

We notice that we do not need the condition  $X \notin \text{fv}(T)$  among the premises of the (*ok-pair*) rule, because it can be derived from the second and the third hypotheses. Finally, the main subtype judgment  $\Gamma \vdash S <: T$  is rendered as  $\text{sub}(\Gamma, S, T)$ , where  $\text{sub}$  is a predicate defined on 3-tuples,  $\text{sub} \subseteq \text{Env} \times \text{Type} \times \text{Type}$ .

**Definition 2** (Subtyping). *If  $\Gamma$  is a type environment,  $S, S_1, S_2, T, T_1, T_2, U$  types, then the predicate  $\text{sub}$  is defined by induction, as follows:*

$$\frac{\text{ok}(\Gamma) \quad \text{closed}(S, \Gamma)}{\text{sub}(\Gamma, S, \text{Top})} \text{(top)} \quad \frac{\text{ok}(\Gamma) \quad \langle X, U \rangle \in \Gamma}{\text{sub}(\Gamma, X, X)} \text{(var)}$$

$$\frac{\langle X, U \rangle \in \Gamma \quad \text{sub}(\Gamma, U, T)}{\text{sub}(\Gamma, X, T)} \text{(trs)} \quad \frac{\text{sub}(\Gamma, T_1, S_1) \quad \text{sub}(\Gamma, S_2, T_2)}{\text{sub}(\Gamma, S_1 \rightarrow S_2, T_1 \rightarrow T_2)} \text{(arr)}$$

$$\frac{\text{sub}(\Gamma, T_1, S_1) \quad \text{for all } X, \text{ok}(\Gamma, \langle X, T_1 \rangle) \Rightarrow \text{sub}(\Gamma, \langle X, T_1 \rangle, S_2, T_2)}{\text{sub}(\Gamma, \forall X <: S_1.S_2, \forall X <: T_1.T_2)} \text{(all)}$$

It is apparent that our presentation of subtyping is equivalent to the original one of Section 2: informally arguing for such an adequacy, we remark that we are using the same *type environments* and that we have formalized their *well-formedness* and a kind of *compatibility* between the types and the environments themselves, two concepts which are implicit in the POPLmark Challenge statement.

To prove *formally* such an adequacy, we have to relate the subtyping definitions in the two settings; this requires a preliminary lemma, to connect each other the three judgments defined in this section. In the following, given an environment  $\Gamma$ ,  $\text{perm}(\Gamma)$  stands for a permutation of its components.

**Lemma 1** (Auxiliary judgments). *For all  $\Gamma \in \text{Env}$ , and  $S, T \in \text{Type}$ :*

- 1)  $\text{sub}(\Gamma, S, T) \Rightarrow \text{ok}(\Gamma)$ ;
- 2)  $\text{sub}(\Gamma, S, T) \Rightarrow \text{closed}(S, \Gamma) \wedge \text{closed}(T, \Gamma)$ .

*Proof.* 1) By induction on the structure of the derivation of  $\text{sub}(\Gamma, S, T)$ . 2) By induction on the structure of the derivation of  $\text{sub}(\Gamma, S, T)$ , and point 1.  $\square$

**Theorem 1** (Adequacy). *For all  $\Gamma \in \text{Env}$ , and  $S, T \in \text{Type}$ :  $\text{sub}(\Gamma, S, T)$  if and only if  $\Gamma \vdash S <: T$ .*

*Proof.* By structural induction on the hypothetical derivations, and Lemma 1.  $\square$

**Lemma 2** (Environment). *For all  $\Gamma, \Delta \in \text{Env}$ , and  $X, P, Q, S, T \in \text{Type}$ :*

- 1) *Well-formedness:*  $\text{ok}(\Gamma, \langle X, Q \rangle, \Delta) \wedge \text{sub}(\Gamma, P, Q) \Rightarrow \text{ok}(\Gamma, \langle X, P \rangle, \Delta)$ ;
- 2) *Permutation:*  $\text{sub}(\Gamma, S, T) \wedge \text{ok}(\text{perm}(\Gamma)) \Rightarrow \text{sub}(\text{perm}(\Gamma), S, T)$ ;
- 3) *Weakening:*  $\text{sub}(\Gamma, S, T) \wedge \text{ok}(\Gamma, \Delta) \Rightarrow \text{sub}(\Gamma, \Delta, S, T)$ .

*Proof.* 1) By induction on the structure of  $\Delta$ , and Lemma 1.2. 2) By induction on the derivation of  $\text{sub}(\Gamma, S, T)$ , and Lemma 1.1. 3) By induction on the derivation of  $\text{sub}(\Gamma, S, T)$ , and point 2.  $\square$

We are ready now to address the first Challenge, by ensuring that our version of subtyping fulfills the reflexivity, transitivity and narrowing properties.

**Proposition 2** (POPLmark Challenge, 1A). *For all  $\Gamma, \Delta \in \text{Env}$ , and  $P, Q, M, N, S, T \in \text{Type}$ :*

**Reflexivity**  $\text{ok}(\Gamma) \wedge \text{closed}(S, \Gamma) \Rightarrow \text{sub}(\Gamma, S, S)$ ;

**Transitivity**  $sub(\Gamma, S, Q) \wedge sub(\Gamma, Q, T) \Rightarrow sub(\Gamma, S, T)$ ;

**Narrowing**  $sub((\Gamma, \langle X, Q \rangle, \Delta), M, N) \wedge sub(\Gamma, P, Q) \Rightarrow sub((\Gamma, \langle X, P \rangle, \Delta), M, N)$ .

*Proof.* **Reflexivity** By induction on the structure of  $S$ .

As shown in Proposition 1, Transitivity and Narrowing are proved simultaneously by induction on the structure of  $Q$ ; we point out here some extra details, which depend on the different cases of  $Q$ .

**Transitivity**  $Q=Top$ : via Lemma 1.2.  $Q=Y$ : by inner induction on the derivation of  $sub(\Gamma, S, Y)$ .  $Q=U \rightarrow V$ : by inner induction on the derivation of  $sub(\Gamma, S, U \rightarrow V)$ , Lemma 1.2, and the outer induction hypothesis, *i.e.*, the transitivity statement itself twice, with  $U$  and  $V$ , which are structurally smaller than  $Q$ .  $Q=\forall Y <: U.V$ : by inner induction on the derivation of  $sub(\Gamma, S, \forall Y <: U.V)$ , Lemma 1.2, and the outer induction hypothesis, this time both the narrowing statement with  $U$  and the transitivity with  $V$ , where, again, both  $U$  and  $V$  are structurally smaller than  $Q$  (see also Proposition 1).

**Narrowing** All the cases require an inner induction on the derivation of  $sub((\Gamma, \langle X, Q \rangle, \Delta), M, N)$ , and Lemmas 1.1, 2.1. When the  $(trs)$  rule is matched by such an inner induction, all the cases but the  $Q=Top$  one need the application of the outer induction hypothesis, *i.e.*, the transitivity statement with the starting  $Q$  (see also Proposition 1). Moreover, when  $(trs)$  is matched, the  $Q=Top$  case requires the Lemma 1.2, and the remaining cases the Weakening property (Lemma 2.3).  $\square$

## 4 Formalization of System $F_{<}$ in $CC^{Ind}$

When encoding a formal system in a type-theory based logical framework (LF), one of the most tedious and time-consuming tasks is that of representing variables and the related machinery of  $\alpha$ -conversion and capture-avoiding substitution. Traditional solutions like, *e.g.*, de Bruijn indices and first-order variables, force the user to spend a lot of time in formalizing and proving a huge number of properties about free and bound occurrences of variables, of  $\alpha$ -conversion, and involved concepts. Often, such development greatly outweighs over the core part of the metatheory’s formalization.

An alternative approach, known as Higher-Order Abstract Syntax (HOAS) [19, 32], has been introduced for overcoming such an overhead. Its gist amounts to use the metavariables of the LF to represent the variables of the object language; in such a way,  $\alpha$ -conversion and capture-avoiding substitution are completely delegated to the framework: in fact, binders are modeled by functional constructors, and substitution is modeled by functional application [2, 14]. Despite this apparent improvement, it is well known (see, *e.g.*, [14, 28]) that HOAS does not cope well with inductive types, yielding several problems:

- Impossibility to adopt “full” HOAS representation of binders: functional types like  $(T \rightarrow T) \rightarrow T$  violate the positivity constraints required by inductive constructors (thus, it is not possible to delegate the substitution of terms into terms to the metalevel).
- Lack of suitable higher-order induction/recursion principles, which would allow to program with and reason about functional terms.
- Impossibility to use inductive types, *e.g.*,  $Var$ , to represent variables: otherwise, higher-order constructors (like  $(Var \rightarrow T) \rightarrow T$ ) could generate “exotic” parasite terms, *i.e.*, terms not corresponding to any term of the object language.
- Difficulty or impossibility to reason at the object level about the concepts and mechanisms delegated to the metalanguage.

Several attempts have been made to reconcile binding constructs with induction principles, also via the design and implementation of new logics (*e.g.*, Nominal Logic [16, 34] and  $FO\lambda^{\Delta V}$  [30]). Although these solutions provide with advantages and support for a suitable representation of variables and binders, they require the user to switch to new and significantly different frameworks, to learn them from scratch, and reimplement/translate the preceding work.

In this paper, we resort to a more “conservative” approach instead, which has been already exploited in several case studies about the encoding of process algebras, and static and dynamic semantics [24, 25, 36, 10, 9, 11]. Actually, we introduce in the Coq implementation [38] of  $CC^{\text{Ind}}$  type theory [13, 31] a weak HOAS formalization of System  $F_{<}$ : (Sections 4.1, 4.2) together with a compact axiomatization of simple properties about variables, named the Theory of Contexts (Section 4.3).

#### 4.1 Encoding of syntax: types and type environments

In the following, `Var` is the *non-inductive* type representing System  $F_{<}$ ’s (*type*) *variables*; therefore we can represent in Coq variables like  $X, Y, \dots$  with metalanguage variables  $X, Y, \dots$  of type `Var`. Next, we define the *inductive* type `Tp` to represent System  $F_{<}$ ’s *types*, with four constructors for the maximal type, variables<sup>3</sup>, function and universal types (compare with Section 2):

```
Parameter Var: Set.
Inductive Tp: Set := var: Var -> Tp      | top: Tp
                    | arr: Tp -> Tp -> Tp | fa : Tp -> (Var -> Tp) -> Tp.
Coercion var: Var >-> Tp.
```

This encoding, via a parametric type `Var` for variables and an inductive type `Tp` for terms of the object system, is in fact a *weak* HOAS encoding. The constructor `fa`, which is higher-order (as it takes as second argument a function from `Var` to `Tp`), allows us to represent correctly System  $F_{<}$ ’s binder “ $\forall$ ”, by delegating to the Coq system the management of the bound variable  $X$  in the expression  $\forall X<:S.T$ . To be more precise, if we denote with  $S$  the encoding of  $S$  and with  $T[X]$  the encoding of  $T$  (where the occurrence of the encoded bound variable  $X$ , corresponding to  $X$ , is explicitly denoted by the square brackets), the representation of  $\forall X<:S.T$  is given by `(fa S (fun X:Var => T[X]))`. Hence, the variable  $X$  is bound by the metalanguage functional construct `fun`; it follows that  $\alpha$ -conversion and capture-avoiding substitution of variables for variables are automatically dealt with by the metalanguage of Coq.

As remarked in Section 3, in this paper we present an “explicit” encoding of *type environments*  $\Gamma$ ; these are encoded as *lists* of pairs, whose components belong to the types `Var` and `Tp`, respectively:

```
Definition envTp: Set := (list (Var * Tp)).
```

This choice is quite intuitive and natural, except for the fact that now, obviously, the environments grow “toward the left” (*i.e.*, the head of the list), while environments “on paper” grow toward the right.

In order to reason about variables, types and type environments, we need a set of auxiliary predicates that formalize the concepts defined in Section 3, *i.e.*, the (non)occurrence of variables into types, the freshness of variables/presence of pairs inside environments, and the well-scoping of types *w.r.t.* the environments themselves. First, we introduce the inductive predicates `isin` and `notin`:

```
Inductive isin (X:Var): Tp -> Prop := isin_var: isin X X
                    | isin_arr: forall S T:Tp, isin X S \ / isin X T -> isin X (arr S T)
```

<sup>3</sup>Notice that `var` is declared as a coercion operator, which avoids to type explicitly the constructor, where a variable should stand for a term of type `Tp`.

```

| isin_fa : forall S:Tp, forall U:Var->Tp,
  isin X S \ / (forall Y:Var, ~X=Y -> isin X (U Y)) -> isin X (fa S U).
Inductive notin (X:Var): Tp -> Prop := notin_top: notin X top
| notin_var: forall Y:Var, ~X=Y -> notin X Y
| notin_arr: forall S T:Tp, notin X S -> notin X T -> notin X (arr S T)
| notin_fa : forall S:Tp, forall U:Var->Tp,
  notin X S -> (forall Y:Var, ~X=Y -> notin X (U Y)) -> notin X (fa S U).

```

The intuitive meaning of  $(\text{isin } X \ T)$  is that the variable  $X$  occurs free in  $T$ ,  $X \in \text{fv}(T)$  in Section 3, while  $(\text{notin } X \ T)$  stands for the opposite concept,  $X \notin \text{fv}(T)$ . The two definitions are syntax-driven, with just one introduction rule for each constructor of type  $\text{Tp}$  (apart from the `top` case for `isin`).

Concerning the environments, we formalize the freshness of a variable  $X \notin \text{dom}(\Gamma)$  (`Gfresh`), the presence of a constraint  $\langle X, T \rangle \in \Gamma$  (`isinG`), and the closure of a type  $\text{closed}(T, \Gamma)$  (`Gclosed`) *w.r.t.* them:

```

Inductive Gfresh (X:Var): envTp -> Prop := GfVoid: Gfresh X nil
| GfGrow: forall G:envTp, forall Y:Var, forall T:Tp,
  Gfresh X G -> ~X=Y -> Gfresh X (cons (Y,T) G).
Inductive isinG (X:Var) (T:Tp): envTp -> Prop :=
  checkG: forall G:envTp, forall y:Var, forall U:Tp,
    (X=Y \ / T=U) \ / isinG X T G -> isinG X T (cons (Y,U) G).
Definition Gclosed (T:Tp) (G:envTp): Prop :=
  forall X:Var, (isin X T) -> exists U:Tp, isinG X U G.

```

We can then state the inductive formulation of the well-formedness of environments:

```

Inductive okEnv: envTp -> Prop := okVoid: okEnv nil
| okGrow: forall G:envTp, forall x:Var, forall T:Tp,
  okEnv G -> Gfresh X G -> Gclosed T G -> okEnv (cons (X,T) G).

```

## 4.2 Encoding of the subtyping relation

The representation of the subtyping relation, *sub* in Section 3, follows closely its counterpart on the paper, apart from the constructor for the universal type `sub_fa`, which is accommodated via an hypothetical premise about a fresh, locally quantified variable, which makes the encoding higher-order:

```

Inductive subTp: envTp -> Tp -> Tp -> Prop :=
  sub_top: forall G:envTp, forall S:Tp,
    okEnv G -> Gclosed S G -> subTp G S top
| sub_var: forall G:envTp, forall X:Var, forall U:Tp,
  okEnv G -> isinG X U G -> subTp G X X
| sub_trs: forall G:envTp, forall X:Var, forall U T:Tp,
  isinG X U G -> subTp G U T -> subTp G X T
| sub_arr: forall G:envTp, forall S1 S2 T1 T2:Tp,
  subTp G T1 S1 -> subTp G S2 T2 ->
  subTp G (arr S1 S2) (arr T1 T2)
| sub_fa : forall G:envTp, forall S1 T1:Tp, forall S2 T2:Var->Tp,
  subTp G T1 S1 ->
  (forall X:Var, okEnv (cons (X,T1) G) ->
    subTp (cons (X,T1) G) (S2 X) (T2 X)) ->
  subTp G (fa S1 S2) (fa T1 T2).

```



### 4.3 The Theory of Contexts

The *Theory of Contexts* (ToC, [23, 5]) is a type-theoretic axiomatization which has been proposed to give a metalogical account of the fundamental notions of *variable* and *context*<sup>4</sup> as they appear in HOAS. Moreover, when the ToC is instantiated in a weak HOAS setting, it is compatible with the recursive and inductive environments provided by type theory-based logical frameworks and their implementations.

In fact, the axioms of this theory aim to reflect in the logic some fundamental and natural properties of object-level “term contexts” and “variables” (or “names”, in some formal systems, like, *e.g.*, process algebras). The main advantages of this approach are that it requires a very low mathematical and logical overhead, and that it can be “plugged” in several existing proof environments without requiring any redesign of such systems. We present now the informal intended meaning of the ToC.

**Decidability of equality over variables** For any variables  $x$  and  $y$ , it is always possible to decide whether  $x = y$  or  $x \neq y$  (“=” is Leibniz’s equality).

**Freshness/Unsaturation** For any term  $M$ , there exists a variable  $x$  which does not occur free in it (another interpretation is that there is no term containing/saturating all the variables).

**Extensionality** Two term contexts are equal if they are equal on a fresh variable; that is, if  $M(x) = N(x)$  and  $x \notin M(\cdot), N(\cdot)$ , then  $M = N$ .

**$\beta$ -expansion** It is always possible to split a term into a context applied to a variable; that is, given a term  $M$  and a variable  $x$ , there exists a context  $N(\cdot)$  such that  $N(x) = M$  and  $x \notin N(\cdot)$ .

The instantiation process is very simple and syntax-driven. First, we state the following axiom (in fact the decidability is required for each type representing variables, the sole `Var` in our case):

Axiom `LEM_Var`: `forall X Y:Var, X=Y \ / \ ~X=Y.`

where the prefix `LEM` stands for *Law of Excluded Middle*; indeed, this is the minimum classical flavour that we require to reason about (free) occurrences of variables. Such assumption is very close to the common practice, when working on the paper with nominal systems.

The formalization of the Freshness/Unsaturation for terms of type `Tp` is straightforward too:

Axiom `unsat`: `forall T:Tp, exists X:Var, notin X T.`

Next we have the instantiations of extensionality (`tp_ext`) and  $\beta$ -expansion (`tp_exp`, `ho_tp_exp`). Notice that we need the  $\beta$ -expansion both at the level of first-order contexts (*i.e.*, terms with one hole, `tp_exp`) and at the level of second-order contexts (terms with two holes, `ho_tp_exp`):

Axiom `tp_ext`: `forall X:Var, forall S T:Var->Tp,`  
`(notin_ho X S) -> (notin_ho X T) -> (S X)=(T X) -> S=T.`

Axiom `tp_exp`: `forall S:Tp, forall X:Var,`  
`exists S': Var->Tp, (notin_ho X S') /\ S=(S' X).`

Axiom `ho_tp_exp`: `forall S:Var->Tp, forall X:Var,`  
`exists S': Var->Var->Tp,`  
`(notin_ho X (fun Y:Var => (fa top (S' Y)))) /\ S=(S' X).`

where `notin_ho` is a simple definition built on top of the predicate `notin`, stating that a variable does not occur in a context:

Definition `notin_ho`: `fun X: Var => fun S: Var->Tp =>`  
`forall Y: Var, ~X=Y -> (notin X (S Y)).`

<sup>4</sup>Contexts are “terms with holes”, where the holes can be filled in by variables.

The properties formalized by the ToC have emerged from practical reasoning about process algebras, and have been proved to be quite useful in a number of situations<sup>5</sup>. Ultimately, their combined effect is that of recovering the capability of reasoning by structural induction over contexts. We explain this fact by means of an individual example, about the *monotonicity* of the predicate `isin`, which is needed for deriving the reflexivity of the subtyping relation (see Section 4.4):

```
Lemma isin_mono: forall T:Var->Tp, forall X Y:Var, ~X=Y -> (isin X (T Y)) ->
  (forall Z: Var, ~X=Z -> (isin X (T Z))).
```

A direct way to prove the lemma would be by higher-order induction on the structure of `T:Var->Tp`; however, Coq does not provide such a principle. Moreover, a naïve (*i.e.*, first-order) induction on `(T Y)` does not work, since there is no way to infer something on the structure of the context `T` from the structure of `(T Y)` (notice that `Y` can occur free in `T`). Hence, we prove a preliminary lemma:

```
Lemma pre_isin_mono: forall n:nat, forall T:Tp, (lntp T n) ->
  forall Z:Var, forall U:Var->Tp, (notin_ho Z U) -> T=(U Z) ->
  forall X Y:Var, ~X=Y -> (isin X (U Y)) ->
  forall V:Var, ~X=V -> (isin X (U V)).
```

where `lntp` is the predicate which counts the number of constructors involved in a term of type `Tp`:

```
Inductive lntp: Tp -> nat -> Prop :=
  lntp_top : (lntp top (S 0))
| lntp_var : forall X:Var, (lntp X (S 0))
| lntp_arr : forall T T':Tp, forall n1 n2:nat,
  (lntp T n1) -> (lntp T' n2) ->
  (lntp (arr T T') (S (plus n1 n2)))
| lntp_fa : forall T:Tp, forall U:Var->Tp, forall n1 n2:nat,
  (lntp T n1) -> (forall X:Var, (lntp (U X) n2)) ->
  (lntp (fa T U) (S (plus n1 n2))).
```

Therefore, `(lntp T n)` states that the term `T` is “built” using `n` constructors of the inductive type `Tp`. This fact allows us to argue by *complete* induction on `n` in the proof of `pre_isin_mono`, thus recovering the structural information about `T` via inversion of the instance `(lntp T n)`. So far, we can apply  $\beta$ -expansion to infer the existence of a context `T':Var->Tp` such that `T=(T' z)`, where `z` does not occur free in `T'`. Then, by applying the extensionality property, we can deduce that `U=T'` and, since `T'` is not a variable but a concrete  $\lambda$ -abstraction, we “lift” structural information to the level of functional terms. Such an information can be finally used to solve the current goal, `isin_mono` in the case.

In order to be more concrete, let us consider the case where `(lntp (T z) 1)` holds. By inverting such an hypothesis, we get the case (among other ones) where the equality `(T z)=top` holds. Then, we apply  $\beta$ -expansion (`tp_exp`) to `top`, yielding a context `T'=(fun x:Tp => top)`; in particular, we can state that `(T z)=top=(T' z)`, whence we infer `(T z)=((fun x:Tp => top) z)`. Finally, by means of the extensionality axiom (`tp_ext`), we “lift” such structural information to higher-order terms: namely, we deduce `T=(fun x:Tp => top)`, *i.e.*, we get the structural information we need about `T`.

#### 4.4 Formal development of the POPLmark Challenge

In this section we illustrate the formal development carried out in the Coq system in order to solve the first task of the POPLmark Challenge, *i.e.* reflexivity, transitivity (and narrowing) of subtyping (Proposition 2). We start by introducing some auxiliary lemmas; the mostly used property is the following:

<sup>5</sup>Their consistency has been proved in [5], starting from an idea of M. Hofmann [22].

Lemma Gclosed\_lemma: forall G:envTp, forall S T:Tp,  
 subTp G S T -> Gclosed S G /\ Gclosed T G.

The informal meaning is that, if we derive (subTp G S T) (under such an hypothesis we are able to deduce that G is a well-formed environment, Lemma 1.1 of Section 3), then all the variables occurring free in S and T belong to the domain of G. The proof is carried out by induction on the derivation of (subTp G S T), using unsatG when we need a variable which is fresh *w.r.t.* the environment G:

Lemma unsatG: forall G:envTp, exists X:Var, Gfresh X G.

As the reader may guess, the proof of unsatG relies heavily upon the axiom unsat of the Theory of Contexts (see Section 4.3). Actually, given an environment G, the idea is just to scan the variable declaration list (X<sub>1</sub>,T<sub>1</sub>), ..., (X<sub>n</sub>,T<sub>n</sub>) in G, to build an arrow type (arr X<sub>1</sub> (arr ... (arr X<sub>n</sub> top) ...)). Then, by eliminating unsat on this type, we can get a fresh variable not occurring into such type and, consequently, not appearing in the domain of G:

Lemma domGtoT\_notin: forall G:envTp, forall X:Var,  
 notin X (domGtoT G) -> Gfresh X G.

where domGtoT is a function, defined by recursion on the environment G, which builds the mentioned arrow type from the variables belonging to its domain:

Fixpoint domGtoT (G:envTp):= match G with  
 | nil => top | (X,T)::G' => (arr X (domGtoT G')) end.

The proof of domGtoT\_notin is performed by induction on the structure of G, using the axiom LEM\_Var to discriminate between the occurrences of variables.

Coming in the end to the POPLmark Challenge properties, the *reflexivity* requires that the type environment is well-formed and the type under investigation is closed *w.r.t.* the environment itself:

Lemma reflexivity: forall T:Tp, forall G:envTp,  
 okEnv G -> Gclosed T G -> subTp G T T.

The proof is a straightforward induction on the structure of T, resorting to LEM\_Var when it is needed to discriminate between free variables, and using the monotonicity of the “occurrence” predicate isin.

*Transitivity* and *narrowing* are proved together (as on the paper), via an outer induction on the structure of the type Q, which is then isolated in front of the two properties:

Theorem trans\_narrow: forall Q:Tp,  
 (forall S:Tp, forall G:envTp,  
 (subTp G S Q) -> forall T:Tp, (subTp G Q T) -> (subTp G S T))  
 /\  
 (forall G':envTp, forall M N:Tp,  
 (subTp G' M N) -> forall D G:envTp, forall X:Var, forall P:Tp,  
 G'=(app D (cons (X,Q) G)) -> subTp G P Q ->  
 subTp (app D (cons (X,P) G)) M N).

The proof of transitivity is, apart from the use of the Theory of Contexts, similar to that on the paper, via an inner induction on the derivation of (subTp G S Q).

The same remark holds about the narrowing, whose management needs an inner induction on the derivation of (subTp G' M N), where the environment G' is Coq's list (app D (cons (X,Q) G)), which is built by means of the *append* function app. However, the narrowing requires two extra efforts.

First, as its formulation involves a structured environment, it has been necessary to prove a series of technical lemmas involving Coq's *lists* and their relationship with the predicates Gfresh, isinG,

Gclosed, okEnv. In carrying out such proofs, we have taken partial advantage of Coq’s built-in list library, especially about *permutations*, which are required by the Weakening property (Lemma 2.3).

To master the sophisticated interdependence between the outer and the inner structural inductions within the narrowing proof, we have exploited a slight elaboration of “modus ponens”:  $\forall A, B : Prop. A \wedge (A \Rightarrow B) \Rightarrow A \wedge B$  (where  $A$  and  $B$  are intended to play the role of transitivity and narrowing, respectively). In fact, when the inner induction hypothesis for narrowing matches the rule `sub_trs` (see the proof of Proposition 2), the outer induction hypothesis (*i.e.*, transitivity) has to be applied with the *starting*  $Q$ , not with a structurally smaller type. Therefore, to handle the involved cases within the outer induction (all but the  $Q=top$  one), we reduce to prove the transitivity alone and the narrowing with the proof context enriched by the transitivity additional hypothesis, instead of merely splitting the two main proofs.

## 5 Related work

At the time of writing, the POPLmark web page [4] collects fifteen contributions, included ours. In this section we give a brief account of the different approaches, filtering them through the perspective of the *first task* of the Challenge. Notice that we do not discuss here those works that employ the *pure* de Bruijn representation, because, according to the POPLmark document [3], it violates the “reasonable overhead” primary metric of success test. Nevertheless, de Bruijn’s technique can be taken into account to measure the progress of alternative representations, and its positive sides may be combined to novel ones.

An approach that keeps de Bruijn indices to represent bound variables, together with (first-order) names to manage free variables, is known as *locally nameless* representation. This was first experimented in Coq by Leroy [26, 27], then refined by Chlipala [8], Charguéraud [6, 7], and ported to the *Matita* proof assistant by Ricciotti [35]. As de Bruijn indices represent variables by positions relative to the enclosing binders, there is no need to introduce  $\alpha$ -equivalence for bound variables; on the other hand, two substitutions of types (for indices and names) have to be managed. Explicit environments are defined, and well-formedness of environments and types are introduced to describe the main subtyping concept.

The opposite encoding choice is made by Stump [37], who represents in Coq bound variables via names and free variables via de Bruijn indices, by taking advantage from the Barendregt variable convention, which assumes that bound and free variables come from *disjoint* sets.

*Higher-Order Abstract Syntax (HOAS)* encodings are closer to ours; we find an hybrid solution in ATS (commented on later in the section), and two full HOAS formalizations, in Abella and Twelf.

The work carried out by Gacek in Abella [17, 18] introduces a canonical HOAS representation of System  $F_{<}$ ’s types (notice, in particular, the signature of the universal constructor “ $\forall$ ”, named `all`):

```
ty    type.
top   ty.
arrow ty -> ty -> ty.
all   ty -> (ty -> ty) -> ty.
```

Since variables are represented by metavariables of type `ty`, the extra specification logic judgment `bound:ty->ty->o` has to be defined to cope with the environment assumptions, and a (simplified) environment well-formedness predicate `ctx:olist->prop` is introduced to reason about subtyping. Finally, to make structural induction on System  $F_{<}$ ’s types feasible, a predicate `wfty:ty->prop` is added.

The formalization carried out at Carnegie Mellon University within the Twelf system [1] uses the same signature for the syntax of System  $F_{<}$ ’s types (here, the universal constructor is named `forall`):

```
tp: type. ...
forall: tp -> (tp -> tp) -> tp.
```

Again, the environment assumptions require a distinguished judgment,  $\text{assm} : \text{tp} \rightarrow \text{tp} \rightarrow \text{type}$ , but, differently from the Abella approach, there is no explicit environment to reason on subtyping; instead, an extra judgment  $\text{var} : \text{tp} \rightarrow \text{type}$  is defined, to “mark” the types which play the role of variables.

Summing up, variables are represented by Abella’s and Twelf’s metavariables belonging to the types  $\text{ty}$  and  $\text{tp}$ , which are introduced to encode the syntax of System  $F_{<}$ ’s types. Differently, we adopt a weak HOAS approach, by choosing a separate, parametric type  $\text{Var}$  for representing variables:

```
Parameter Var: Set.
Inductive Tp: Set := ...
fa: Tp -> (Var -> Tp) -> Tp.
```

In this way, we keep the advantage of delegating  $\alpha$ -conversion and substitution of variables for variables to the metalanguage, while retaining Coq’s built-in induction principle for  $\text{Tp}$ . Of course, in Abella and Twelf one has the extra possibility of delegating the substitution of *types* for variables, while we should write an ad-hoc predicate. However, this kind of substitution is not required to deal with subtyping.

Also the solution proposed by Urban and coworkers in Isabelle [39], and based on the *Nominal (Logic)* datatype package, is quite related to our approach. The signature of types is the following:

```
atom – decl tyvrs
nominal – datatype ty =
  Tvar tyvrs
| Top
| Arrow ty ty    (– → – [100, 100] 100)
| Forall << tyvrs >> ty ty
```

In this formalization type variables are represented by atoms, therefore System  $F_{<}$ ’s “ $\forall$ ” binder is encoded via the abstraction operator  $\ll \dots \gg \dots$ ; this allows to prove that  $\alpha$ -equivalent types are equal. Then, a measure on the size of types and the notion of capture-avoiding substitution are defined.

We remark that the intrinsic concepts of *finite support* and *freshness* play in Nominal Logic a role which is similar to that of occurrence ( $\text{isin}$ ) and non-occurrence ( $\text{notin}$ ) predicates, which are bundled with our axioms of the Theory of Contexts (ToC). Actually, this is not fortuitous, since in [29] the relation between the intuitionistic Nominal Logic and the Theory of Contexts is clearly explained by means of a translation of terms, formulas and judgments of the former into terms and propositions of the  $\text{CC}^{\text{Ind}}$ , via a weak HOAS encoding. It turns out that the (translation of the) axioms and rules of the intuitionistic Nominal Logic are derivable in  $\text{CC}^{\text{Ind}}$  extended with the Theory of Contexts ( $\text{CC}^{\text{Ind}} + \text{ToC}$ ).

An alternative high-level encoding technique exploits nested datatypes for representing the variable binder in Coq [20, 21]. This approach, whose characteristic feature is the encoding of the “ $\forall$ ” operator ( $\text{Uni}$  in the following predicate), is named *nested abstract syntax* by its authors:

```
Inductive ftype (V:Type): Type := ...
| Uni: ftype V -> ftype ^V -> ftype V.
```

where the type  $\text{^V}$ , rendered by the option datatype, denotes  $V$  extended with a new “fresh” element:

```
Inductive option (V:Type): Type := Some: V -> option V
| None: option V.
```

The main advantages consist of retaining the induction and recursion principles provided by Coq and providing a categorical interpretation of the whole approach. On the other hand, as the heavy use of dependent typing is not always supported by Coq, ad-hoc techniques have to be picked out.

Xi’s *hybrid* solution in ATS [40] combines HOAS (for types) with de Bruijn indices (for environments). ATS is a powerful programming language, featuring dependent and linear types and supporting theorem proving. However, in this case it is not possible to state a meaningful comparison with our work, because Xi’s contribution does not address the first part of the Challenge.

Another approach which addresses a different part of the Challenge is due to Fairbairn and carried out in Alpha-Prolog [15], with a complementary parser and pretty printer written in OCaml. More precisely, this work provides a nominal-style formalization of System  $F_{<}$ : with records and patterns, allowing the user to “animate” the language, *i.e.*, to explore the language properties on specific examples.

## 6 Conclusion

Carrying out our weak HOAS formalization of System  $F_{<}$ :’s pure type language in Coq, we have tried to stick to the POPLmark primary metrics of success (see [3]).

- *Correctness.* In Section 3 we have given an alternative presentation of System  $F_{<}$ :’s subtyping concept, thus yielding a system which is equivalent to the original one (as stated by Theorem 1), but at the same time closer to the final formalization in  $CC^{\text{Ind}}$ . In other words, the translation from the system “on paper”, presented in Section 3, to its formal counterpart in Section 4 is, except for the use of weak HOAS, a matter of syntactic sugar.
- *Reasonable overhead.* The weak HOAS encoding approach, together with the (suitable instantiation of the) Theory of Contexts, provides a smooth treatment of the (type) variable binder, and frees the user from the burden of dealing with low-level mechanisms about variables<sup>6</sup>. In fact, bound variables are automatically dealt with by the metalanguage of Coq, which transparently renames them to avoid clashes with free ones. At the same time, our formalization allows the user to keep benefiting from the inductive features of  $CC^{\text{Ind}}$ , that is, recursion and induction principles. Remarkably, the Theory of Contexts grants the extra ability to handle and reason about contexts (*i.e.*, higher-order terms), lifting structural information to the level of functional terms.
- *Transparent technology.* In our opinion, both the formal representation of System  $F_{<}$ :’s type language and the encoding of fundamental theorems’ statements are easily readable and very close to their informal counterparts. Even the axioms of the Theory of Contexts are reminiscent of properties that are commonly taken for granted, working with “paper and pencil”.
- *Reasonable cost of entry.* The Coq system is one of the most used proof assistants based on type theory; it is well-documented, and the provided tutorial allows everyone who is knowledgeable about programming language theory to use fruitfully the proof assistant, after a reasonable training effort, for the goals within the Challenge. More specifically, the Theory of Contexts may be injected in Coq without the need of any redesign of the system; moreover, as we have already pointed out, such a theory is rather easy to add on top of a signature, since it is syntax-driven.

Concluding, we stress that, even we have not pursued neither optimization (of our encoding) nor competition (with the alternative ones)<sup>7</sup>, our formalization is still effective and very terse, in spite of lack of support for HOAS encodings in Coq. Actually, the source code of the development preliminary to the main goal is 33.4 KB long, including 12.7 KB required to manage the type environment; also the main

<sup>6</sup>Namely,  $\alpha$ -conversion and capture-avoiding substitution of variables for variables.

<sup>7</sup>In fact, our contribute is the *first* weak HOAS solution submitted to the POPLmark Challenge: as such, the spirit of our work is essentially to close a gap, and at the same time a first effort towards more ambitious goals (stated by the Challenge).

proof (Reflexivity, Transitivity and Narrowing) is rather compact (it is about 16 KB long), and it follows closely the trace of its “informal” counterpart, carried out “on paper”.

From a pragmatic point of view, we want just to add two remarks.

First, we have suffered a little from the lack of “smart” support for nested inductions, having to rearrange the goal statement and to enrich it with suitable equalities, to correctly “purge” the inconsistent cases automatically generated by the nested application of the `induction` tactic.

Second, we have spent almost the 40% of the preliminary script to handle the type environment, which could be seen as an overhead. In fact, we plan to investigate in future work the possibility to drop the list machinery used to represent the type environment, by adopting instead the *bookkeeping technique* [28, 10, 9, 11], with a “global” environment and local hypotheses modeled via hypothetical judgments.

## References

- [1] M. Ashley-Rollman, K. Crary & R. Harper: *A solution to the POPLmark Challenge*. Available at [4].
- [2] A. Avron, F. Honsell, I. A. Mason & R. Pollack (1992): *Using Typed Lambda Calculus to Implement Formal Systems on a Machine*. *J. Autom. Reasoning* 9(3), pp. 309–354. Available at <http://dx.doi.org/10.1007/BF00245294>.
- [3] B. E. Aydemir et al., (2005): *Mechanized Metatheory for the Masses: The PoplMark Challenge*. In Joe Hurd & Thomas F. Melham, editors: *TPHOLS, Lecture Notes in Computer Science* 3603, Springer, pp. 50–65. Available at [http://dx.doi.org/10.1007/11541868\\_4](http://dx.doi.org/10.1007/11541868_4).
- [4] B. E. Aydemir et al., *The POPLmark Challenge*. Available at <http://www.seas.upenn.edu/~plclub/poplmark/>.
- [5] A. Bucalo, F. Honsell, M. Miculan, I. Scagnetto & M. Hofmann (2006): *Consistency of the theory of contexts*. *J. Funct. Program.* 16(3), pp. 327–372. Available at <http://dx.doi.org/10.1017/S0956796806005892>.
- [6] A. Charguéraud: *A solution to the POPLmark Challenge*. Available at [4].
- [7] A. Charguéraud (2011): *The Locally Nameless Representation*. *Journal of Automated Reasoning*, pp. 1–46. Available at <http://dx.doi.org/10.1007/s10817-011-9225-2>.
- [8] A. Chlipala: *A solution to the POPLmark Challenge*. Available at [4].
- [9] A. Ciaffaglione, L. Liquori & M. Miculan (2003): *Imperative Object-Based Calculi in Co-inductive Type Theories*. In Moshe Y. Vardi & Andrei Voronkov, editors: *LPAR, Lecture Notes in Computer Science* 2850, Springer, pp. 59–77. Available at [http://dx.doi.org/10.1007/978-3-540-39813-4\\_4](http://dx.doi.org/10.1007/978-3-540-39813-4_4).
- [10] A. Ciaffaglione, L. Liquori & M. Miculan (2003): *Reasoning on an imperative object-based calculus in Higher Order Abstract Syntax*. In: *MERLIN*, ACM, pp. 1–10. Available at <http://doi.acm.org/10.1145/976571.976574>.
- [11] A. Ciaffaglione, L. Liquori & M. Miculan (2007): *Reasoning about Object-based Calculi in (Co)Inductive Type Theory and the Theory of Contexts*. *J. Autom. Reasoning* 39(1), pp. 1–47. Available at <http://dx.doi.org/10.1007/s10817-006-9061-y>.
- [12] A. Ciaffaglione & I. Scagnetto (2012): *A solution to the POPLmark Challenge*. Available at [4].
- [13] T. Coquand & G. P. Huet (1988): *The Calculus of Constructions*. *Inf. Comput.* 76(2/3), pp. 95–120. Available at [http://dx.doi.org/10.1016/0890-5401\(88\)90005-3](http://dx.doi.org/10.1016/0890-5401(88)90005-3).
- [14] J. Despeyroux, A. P. Felty & A. Hirschowitz (1995): *Higher-Order Abstract Syntax in Coq*. In Mariangiola Dezani-Ciancaglini & Gordon D. Plotkin, editors: *TLCA, Lecture Notes in Computer Science* 902, Springer, pp. 124–138. Available at <http://dx.doi.org/10.1007/BFb0014049>.
- [15] M. Fairbairn: *A solution to the POPLmark Challenge*. Available at [4].
- [16] M. Gabbay & A. M. Pitts (2002): *A New Approach to Abstract Syntax with Variable Binding*. *Formal Asp. Comput.* 13(3-5), pp. 341–363. Available at <http://dx.doi.org/10.1007/s001650200016>.

- [17] A. Gacek: *A solution to the POPLmark Challenge*. Available at [4].
- [18] A. Gacek (2009): *A Framework for Specifying, Prototyping, and Reasoning about Computational Systems*. Ph.D. thesis, University of Minnesota.
- [19] R. Harper, F. Honsell & G. D. Plotkin (1987): *A Framework for Defining Logics*. In: *LICS*, IEEE Computer Society, pp. 194–204.
- [20] A. Hirschowitz & M. Maggesi: *A solution to the POPLmark Challenge*. Available at [4].
- [21] A. Hirschowitz & M. Maggesi (2012): *Nested Abstract Syntax in Coq*. *J. Autom. Reasoning* 49(3), pp. 409–426. Available at <http://dx.doi.org/10.1007/s10817-010-9207-9>.
- [22] M. Hofmann (1999): *Semantical Analysis of Higher-Order Abstract Syntax*. In: *Proceedings of the 14th Annual IEEE Symposium on Logic in Computer Science, LICS '99*, IEEE Computer Society, Washington, DC, USA, pp. 204–. Available at <http://dl.acm.org/citation.cfm?id=788021.788940>.
- [23] F. Honsell, M. Miculan & I. Scagnetto (2001): *An Axiomatic Approach to Metareasoning on Nominal Algebras in HOAS*. In Fernando Orejas, Paul G. Spirakis & Jan van Leeuwen, editors: *ICALP, Lecture Notes in Computer Science 2076*, Springer, pp. 963–978. Available at [http://dx.doi.org/10.1007/3-540-48224-5\\_78](http://dx.doi.org/10.1007/3-540-48224-5_78).
- [24] F. Honsell, M. Miculan & I. Scagnetto (2001):  *$\pi$ -calculus in (Co)inductive-type theory*. *Theor. Comput. Sci.* 253(2), pp. 239–285. Available at [http://dx.doi.org/10.1016/S0304-3975\(00\)00095-5](http://dx.doi.org/10.1016/S0304-3975(00)00095-5).
- [25] F. Honsell, M. Miculan & I. Scagnetto (2001): *The Theory of Contexts for First Order and Higher Order Abstract Syntax*. *Electr. Notes Theor. Comput. Sci.* 62, pp. 116–135. Available at [http://dx.doi.org/10.1016/S1571-0661\(04\)00323-8](http://dx.doi.org/10.1016/S1571-0661(04)00323-8).
- [26] X. Leroy: *A solution to the POPLmark Challenge*. Available at [4].
- [27] X. Leroy (2007): *A locally nameless solution to the POPLmark challenge*. Research report 6098, INRIA.
- [28] M. Miculan (1997): *Encoding Logical Theories of Programs*. Ph.D. thesis, Dipartimento di Informatica, Università di Pisa, Italy.
- [29] M. Miculan, I. Scagnetto & F. Honsell (2005): *Translating specifications from nominal logic to CIC with the theory of contexts*. In Randy Pollack, editor: *MERLIN*, ACM, pp. 41–49. Available at <http://doi.acm.org/10.1145/1088454.1088460>.
- [30] D. Miller & A. Tiu (2005): *A proof theory for generic judgments*. *ACM Trans. Comput. Log.* 6(4), pp. 749–783. Available at <http://doi.acm.org/10.1145/1094622.1094628>.
- [31] C. Paulin-Mohring (1993): *Inductive Definitions in the system Coq - Rules and Properties*. In Marc Bezem & Jan Friso Groote, editors: *TLCA, Lecture Notes in Computer Science 664*, Springer, pp. 328–345. Available at <http://dx.doi.org/10.1007/BFb0037116>.
- [32] F. Pfenning & C. Elliott (1988): *Higher-Order Abstract Syntax*. In Richard L. Wexelblat, editor: *PLDI*, ACM, pp. 199–208. Available at <http://doi.acm.org/10.1145/53990.54010>.
- [33] B. C. Pierce (2002): *Types and programming languages*. MIT Press.
- [34] A. M. Pitts (2003): *Nominal logic, a first order theory of names and binding*. *Inf. Comput.* 186(2), pp. 165–193. Available at [http://dx.doi.org/10.1016/S0890-5401\(03\)00138-X](http://dx.doi.org/10.1016/S0890-5401(03)00138-X).
- [35] W. Ricciotti: *A solution to the POPLmark Challenge*. Available at [4].
- [36] I. Scagnetto & M. Miculan (2002): *Ambient Calculus and its Logic in the Calculus of Inductive Constructions*. *Electr. Notes Theor. Comput. Sci.* 70(2), pp. 76–95. Available at [http://dx.doi.org/10.1016/S1571-0661\(04\)80507-3](http://dx.doi.org/10.1016/S1571-0661(04)80507-3).
- [37] A. Stump: *A solution to the POPLmark Challenge*. Available at [4].
- [38] The Coq Development Team (2011): *The Coq Proof Assistant Reference Manual, version 8.3*. INRIA. Available at <http://coq.inria.fr/>.
- [39] C. Urban et al., *A solution to the POPLmark Challenge*. Available at [4].
- [40] H. Xi: *A solution to the POPLmark Challenge*. Available at [4].