



**HAL**  
open science

## Formalizing Implicative Algebras in Coq

Étienne Miquey

► **To cite this version:**

Étienne Miquey. Formalizing Implicative Algebras in Coq. ITP 2018 - 9th International Conference on Interactive Theorem Proving, Jul 2018, Oxford, United Kingdom. pp.459-476, 10.1007/978-3-319-94821-8\_27 . hal-01703524

**HAL Id: hal-01703524**

**<https://inria.hal.science/hal-01703524>**

Submitted on 7 Feb 2018

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Formalizing Implicative Algebras in Coq

Étienne Miquey

Équipe Gallinette  
Inria, LS2N (CNRS)  
etienne.miquey@inria.fr

**Abstract.** We present a Coq formalization of Alexandre Miquel’s *implicative algebras* [18], which aim at providing a general algebraic framework for the study of classical realizability models. We first give a self-contained presentation of the underlying *implicative structures*, which roughly consists of a complete lattice equipped with a binary law representing the implication. We then explain how these structures can be turned into models by adding separators, giving rise to the so-called implicative algebras. Additionally, we show how they generalize Boolean and Heyting algebras as well as the usual algebraic structures used in the analysis of classical realizability.

## 1 Introduction

***Krivine classical realizability*** It is well-known since Griffin seminal work [10] that a classical Curry-Howard correspondence can be obtained by adding control operators to the  $\lambda$ -calculus. Several calculi were born from this idea, amongst which Krivine  $\lambda_c$ -calculus [13], defined as the  $\lambda$ -calculus extended with Scheme’s `call/cc` operator (for *call-with-current-continuation*). Elaborating on this calculus, Krivine developed in the late 90s the theory of *classical realizability* [13], which is a complete reformulation of its intuitionistic twin. Originally introduced to analyze the computational content of classical programs, it turned out that classical realizability also provides interesting semantics for classical theories. While it was first tailored to Peano second-order arithmetic (*i.e.* second-order type systems), classical realizability actually scales to more complex classical theories, *e.g.* ZF [14], and gives rise to surprisingly new models. In particular, it generalizes Cohen’s forcing [14,17] and allows for the direct definition of a model in which neither the continuum hypothesis nor the axiom of choice hold [16].

***Algebraization of classical realizability*** During the last decade, the study of the algebraic structure of the models that classical realizability induces have been an active research topic. This line of work was first initiated by Streicher, who proposed the concept of *abstract Krivine structure* [24], followed by Ferrer, Frey, Guillermo, Malherbe and Miquel who introduced other structures peculiar to classical realizability [6,7,5,8,9]. Aside from the algebraic study of classical realizability models, these works had the interest of building the bridge with the algebraic structures arising from intuitionistic realizability. In particular,

Streicher showed in [24] how classical realizability could be analyzed in terms of *tripos* [21], the categorical framework arising from intuitionistic realizability models, while the later work of Ferrer *et al.* [6,7] connected it to Hofstra and Van Oosten’s notion of *ordered combinatory algebras* [12]. More recently, Alexandre Miquel came up with the elegant concept of *implicative structure* and *implicative algebra* [18]<sup>1</sup>, which appears to encompass the previous approaches and which we present in this paper.

**Implicative structures** In addition to providing an algebraic framework conducive to the analysis of classical realizability, an important feature of implicative structures is that they allow us to identify *realizers* (*i.e.*  $\lambda$ -terms) and *truth values* (*i.e.* formulas). Concretely, implicative structures are complete lattices equipped with a binary operation  $a \rightarrow b$  verifying properties coming from the logical implication. As we will see, they indeed allow us to interpret both the formulas and the terms in the same structure. For instance, the ordering relation  $a \leq b$  will encompass different intuitions depending on whether we regard  $a$  and  $b$  as formulas or as terms. Namely,  $a \leq b$  will be given the following meanings:

- the formula  $a$  is a *subtype* of the formula  $b$ ;
- the term  $a$  is a *realizer* of the formula  $b$ ;
- the realizer  $a$  is *more defined* than the realizer  $b$ .

The last item corresponds to the intuition that if  $a$  is a realizer of all the formulas of which  $b$  is a realizer,  $a$  is more precise than  $b$ , or more powerful as a realizer. Therefore,  $a$  and  $b$  should be ordered.

In terms of the Curry-Howard correspondence, this means that not only do we identify types with formulas and proofs with programs, but *we also identify types and programs*.

**Implicative Algebras** Because we consider formulas as realizers, any formula will be at least realized by itself. In particular, the lowest formula  $\perp$  is realized. While this can be dazzling at first sight, it merely reflects that implicative structures do not come with an intrinsic criterion of consistency. To this purpose, we will introduce the notion of *separator*, which is similar to the usual notion of filter for Boolean algebras. *Implicative algebras* will be defined as implicative structures equipped with a separator. As we shall see, they capture the algebraic essence of classical realizability models. In particular, we will embed both the  $\lambda_c$ -calculus and its second-order type system in such a way that the adequacy is preserved. Implicative algebras therefore appear to be the adequate algebraic structure to study classical realizability and the models it induces.

**Coq formalization** The formalization of implicative algebras that we present in this paper has been written using the Coq proof assistant. It was written during the author PhD, as a way of (1) checking the correctness of implicative

---

<sup>1</sup> Independently, very similar structures can be found in Frédéric Ruyer’s Ph.D. thesis [22] under the name of *applicative lattices*.

algebras properties (which, at the time, were neither published nor formally written with their proofs) (2) easing the further study of similar structures<sup>2</sup>

Technically, it relies on Charguéraud’s *locally nameless representation* of  $\lambda$ -terms [2], and the corresponding LN library<sup>3</sup>, which was developed at the occasion of the POPLmark challenge [1]. As for the different algebraic structures evoked in the paper, we systematically represent them as classes using Sozeau-Oury’s `Class` mechanism [23].

**Outline of the paper** We begin by briefly recalling the structures of classical realizability models in Section 2. We then present in Section 3 the concept of implicative structures and explain how it generalizes well-known algebraic structures<sup>4</sup>. We then show in Section 4 how  $\lambda_c$ -terms and second-order types can be adequately embedded within implicative structures. Finally, we introduce implicative algebras in Section 5. We study their internal logic and finally explain how they give rise to models. *It should be clear to the reader that the notion of implicative algebra and its properties are due to Alexandre Miquel [18].*

*The theorems in the paper are hyperlinked with their formalizations in the Coq development<sup>5</sup>. Detailed proofs can be found in [19, Chapter 10] from which this paper is partially taken.*

## 2 Krivine classical realizability

Due to the lack of space, it is not possible to fully introduce here Krivine classical realizability and its models defined using the machinery of the  $\lambda_c$ -calculus<sup>6</sup>. Rather than that, we choose to present it through the lenses of Streicher’s *abstract Krivine structures* (AKS), which are merely an axiomatization of the Krivine abstract machine for the  $\lambda_c$ -calculus viewed as an algebraic structure:

**Definition 1. (AKS)** *An abstract Krivine structure is given by a septuple  $(\mathbf{A}, \mathbf{\Pi}, \mathit{app}, \mathit{push}, \mathit{k}_-, \mathit{k}, \mathit{s}, \mathit{cc}, \mathbf{PL}, \perp\!\!\!\perp)$  where:*

1.  $\mathbf{A}$  and  $\mathbf{\Pi}$  are non-empty sets, respectively called the terms and the stacks;
2.  $\mathit{app} : t, u \mapsto tu$  if a function (called application) from  $\mathbf{A} \times \mathbf{A}$  to  $\mathbf{A}$ ;
3.  $\mathit{push} : t, \pi \mapsto t \cdot \pi$  if a function (called push) from  $\mathbf{A} \times \mathbf{\Pi}$  to  $\mathbf{\Pi}$ ;
4.  $\mathit{k}_- : \pi \mapsto \mathit{k}_\pi$  if a function from  $\mathbf{\Pi}$  to  $\mathbf{A}$  ( $\mathit{k}_\pi$  is called a continuation);
5.  $\mathit{k}, \mathit{s}$  and  $\mathit{cc}$  are three distinguished terms of  $\mathbf{A}$ ;

<sup>2</sup> Namely, one of the goal of the author’s PhD work was to define disjunctive and conjunctive algebras, based on the decomposition of the implication  $A \rightarrow B$  as  $\neg A \vee B$  and  $\neg(A \wedge \neg B)$ . See [19] for further details.

<sup>3</sup> In doing so, our development implicitly relies on assumptions of functional

<sup>4</sup> We will not recall the definition of lattices, Heyting algebras and so on, for a more detailed introduction we refer the reader to [19, Chapter 9]

<sup>5</sup> <http://www.irif.fr/~emiquey/ITP/>

<sup>6</sup> For a detailed introduction on this topic, we refer the reader to [13] or the author’s PhD thesis [19, Chapter 3].

6.  $\perp\!\!\!\perp \subseteq \mathbf{A} \times \mathbf{II}$  (called the pole) is a relation between terms and stacks, also written  $t \star \pi \in \perp\!\!\!\perp$ . This relation fulfills the following axioms for all terms  $t, u, v \in \mathbf{A}$  and all stacks  $\pi, \pi' \in \mathbf{A}$ :

$$\left. \begin{array}{l} t \star u \cdot \pi \in \perp\!\!\!\perp \Rightarrow tu \star \pi \in \perp\!\!\!\perp \\ t \star \pi \in \perp\!\!\!\perp \Rightarrow \mathbf{k} \star t \cdot u \cdot \pi \in \perp\!\!\!\perp \\ tv(uv) \star \pi \in \perp\!\!\!\perp \Rightarrow \mathbf{s} \star t \cdot u \cdot v \cdot \pi \in \perp\!\!\!\perp \end{array} \right| \begin{array}{l} t \star \mathbf{k}_\pi \cdot \pi \in \perp\!\!\!\perp \Rightarrow \mathbf{cc} \star t \cdot \pi \in \perp\!\!\!\perp \\ t \star \pi \in \perp\!\!\!\perp \Rightarrow \mathbf{k}_\pi \star t \cdot \pi' \in \perp\!\!\!\perp \end{array}$$

7.  $\mathbf{PL} \subseteq \mathbf{A}$  is a subset of  $\mathbf{A}$  (whose elements are called the proof-like terms), which contains  $\mathbf{k}, \mathbf{s}, \mathbf{cc}$  and is closed under application.

Given any subset of stacks  $X \subseteq \mathbf{II}$  (which we call a falsity value), we write  $X^\perp$  for its orthogonal set with respect to the pole:

$$X^\perp \triangleq \{t \in \mathbf{A} : \forall \pi \in X, t \star \pi \in \perp\!\!\!\perp\}$$

Orthogonality for subsets  $X \subseteq \mathbf{A}$  (i.e. a truth value) is defined identically. Intuitively, classical realizability models are mainly given by the choice of the sets  $\perp\!\!\!\perp$  and  $\mathbf{PL}$  together with the interpretation of formulas as falsity values. A term  $t \in \mathbf{A}$  is called a *realizer* of a formula  $A$  if  $t \in \|A\|^\perp$  where  $\|A\| \in \mathcal{P}(\mathbf{II})$  is the falsity value of  $A$ .

### 3 Implicative structures

#### 3.1 Definition

Intuitively, *implicative structures* are tailored to represent both the formulas of second-order logic and realizers arising from Krivine's  $\lambda_c$ -calculus. We shall see in the sequel how they indeed allow us to define  $\lambda$ -terms, but let us introduce them by focusing on their logical facet. We are interested in formulas of second-order logic, that is to say of system  $F$ , which are defined by a simple grammar:

$$A, B ::= X \mid A \Rightarrow B \mid \forall X.A$$

Implicative structures are therefore defined as meet-complete lattices (for the universal quantification) with an internal binary operation satisfying the properties of the implication:

**Definition 2.** An implicative structure is a complete meet-semilattice  $(\mathcal{A}, \preceq)$  equipped with a binary operation  $(a, b) \mapsto (a \rightarrow b)$ , called the implication of  $\mathcal{A}$ , that fulfills the following axioms:

1. Implication is anti-monotonic with respect to its first operand and monotonic with respect to its second operand, in the sense that for all  $a, a_0, b, b_0 \in \mathcal{A}$ :

$$\text{(Variance)} \quad \text{if } a_0 \preceq a \text{ and } b \preceq b_0 \text{ then } (a \rightarrow b) \preceq (a_0 \rightarrow b_0)$$

2. Arbitrary meets distribute over the second operand of implication, in the sense that for all  $a \in \mathcal{A}$  and for all subsets  $B \subseteq \mathcal{A}$ :

$$\text{(Distributivity)} \quad \bigwedge_{b \in B} (a \rightarrow b) = a \rightarrow \bigwedge_{b \in B} b$$

**Remark 3.** In the particular case where  $B = \emptyset$ , the axiom of distributivity states that  $a \rightarrow \top = \top$  for all  $a \in \mathcal{A}$ .

### 3.2 Examples of implicative structures

**Complete Heyting algebras** The first example of implicative structures is given by complete Heyting algebras. Indeed, the axioms of implicative structures are intuitionistic tautologies verified by any complete Heyting algebra. Therefore, every complete Heyting algebra induces an implicative structure with the same arrow:

**Proposition 4.** *Every complete Heyting algebra is an implicative structure.*

*Proof.* Since  $\mathcal{H}$  is complete, by definition we have  $a \rightarrow b = \bigvee \{x \in \mathcal{H} : a' \wedge x \preceq b\}$ , from which we deduce that  $a \wedge c \preceq b \Leftrightarrow a \preceq c \rightarrow b$ . The axioms defining implicative structures are straightforward to prove using these observations.

The converse is obviously false, since the implication of an implicative structure  $\mathcal{A}$  is in general not determined by the lattice structure of  $\mathcal{A}$ . Besides, since any (complete) Boolean algebra is in particular a (complete) Heyting algebra, *a fortiori* any complete Boolean algebra induces an implicative structure:

**Proposition 5.** *If  $\mathcal{B}$  is a complete Boolean algebra, then  $\mathcal{B}$  induces an implicative structure where the implication is defined for all  $a, b \in \mathcal{B}$  by  $a \rightarrow b \triangleq \neg a \vee b$ .*

**Dummy structures** Given a complete lattice  $\mathcal{L}$ , it is easy to check that the following definitions induce dummy implicative structures:

**Proposition 6.** *If  $\mathcal{L}$  is a complete lattice, the following definitions give rise to implicative structures: 1.  $a \rightarrow b \triangleq \top$  2.  $a \rightarrow b \triangleq b$  (for all  $a, b \in \mathcal{L}$ )*

Both definitions lead to implicative structures which are meaningless from the point of view of logic. Nonetheless, they will provide us with useful counter-examples.

**Ordered combinatory algebras** We recall the notion of *ordered combinatory algebra*, abbreviated in OCA, which is a variant<sup>7</sup> of Hofstra and Van Oosten's notion of ordered partial combinatory algebras [12]. Ferrer *et al.* structures to represent Krivine realizability, called  $\mathcal{I}OCA$  or  $\mathcal{K}OCA$ , are particular cases of OCA [6,7,5].

**Definition 7. (OCA)** *An ordered combinatory algebra is given by a quintuple  $(\mathcal{A}, \leq, \mathbf{app}, \mathbf{k}, \mathbf{s})$ , where:*

- $\leq$  is a partial order over  $\mathcal{A}$ ,
- $\mathbf{app} : (a, b) \mapsto ab$  is a monotonic function<sup>8</sup> from  $\mathcal{A} \times \mathcal{A}$  to  $\mathcal{A}$ ,
- $\mathbf{k} \in \mathcal{A}$  is such that  $\mathbf{k}ab \leq a$  for all  $a, b \in \mathcal{A}$ ,
- $\mathbf{s} \in \mathcal{A}$  is such that  $\mathbf{s}abc \leq ac(bc)$  for all  $a, b, c \in \mathcal{A}$ .

<sup>7</sup> In partial combinatory algebras, the application is defined as a partial function.

<sup>8</sup> Observe that the application, which is written as a product, is neither commutative nor associative in general.

Any ordered combinatory algebra also induces an implicative structure: Similarly, we can define an implication on the complete lattice  $\mathcal{P}(\mathcal{A})$  which give rise to an implicative structure:

**Proposition 8.** *If  $\mathcal{A}$  is an ordered combinatory algebra, then the complete lattice  $\mathcal{P}(\mathcal{A})$  equipped with the implication<sup>9</sup> :*

$$A \rightarrow B \triangleq \{r \in \mathcal{A} : \forall a \in A. ra \in B\} \quad (\forall A, B \subseteq \mathcal{A})$$

*is an implicative structure*

*Proof.* Both conditions (variance/distributivity) are trivial from the definition.

**Implicative structure of classical realizability** Our final example of implicative structure—which is the main motivation of this work—is given by classical realizability. As we saw in Section 2, the construction of classical realizability models, whether it be from Krivine’s realizability algebras [14,15,16] in a set-theoretic like fashion or in Streicher’s AKS [24], takes place in a structure of the form  $(\mathbf{A}, \mathbf{II}, \cdot, \perp\!\!\!\perp)$  where  $\mathbf{A}$  is the set of realizers;  $\mathbf{II}$  is the set of stacks;  $(\cdot) : \mathbf{A} \times \mathbf{II} \rightarrow \mathbf{II}$  is a binary operation for pushing a realizer onto a stack and  $\perp\!\!\!\perp \subseteq \mathbf{A} \times \mathbf{II}$  is the pole. Given such a quadruple, we can define for all  $a, b \in \mathcal{A}$ :

$$\mathcal{A} \triangleq \mathcal{P}(\mathbf{II}) \quad a \preceq b \triangleq a \supseteq b \quad a \rightarrow b \triangleq a^{\perp\!\!\!\perp} \cdot b = \{t \cdot \pi : t \in a^{\perp\!\!\!\perp}, \pi \in b\}$$

where as usual  $a^{\perp\!\!\!\perp}$  is  $\{t \in \mathbf{A} : \forall \pi \in a, (t, \pi) \in \perp\!\!\!\perp\} \in \mathcal{P}(\mathbf{A})$ , the orthogonal set of  $a \in \mathcal{P}(\mathbf{II})$  with respect to the pole  $\perp\!\!\!\perp$ . Here again, it is easy to verify that this defines an implicative structure.

**Proposition 9.** *The triple  $(\mathcal{A}, \preceq, \rightarrow)$  is an implicative structure.*

*Proof.* The proof is again trivial. Variance conditions correspond to the usual monotonicity of truth and falsity values in Krivine realizability [13], while the distributivity follows directly by unfolding the definitions.

## 4 Interpreting the $\lambda$ -calculus

### 4.1 Interpretation of $\lambda$ -terms

We motivated the definition of implicative structures with the aim of obtaining a common framework for the interpretation both of types and programs. We shall now see how  $\lambda$ -terms can indeed be defined in implicative structures.

From now on, let  $\mathcal{A} = (\mathcal{A}, \preceq, \rightarrow)$  denotes an arbitrary implicative structure.

<sup>9</sup> This definition is related with the construction of a realizability tripos from an OCA  $\mathcal{A}$ . Indeed, given a set  $X$ , the ordering on predicates of  $\mathcal{P}(\mathcal{A})^X$  is defined by:

$$\varphi \vdash_X \psi \triangleq \exists r \in \mathcal{A}. \forall x \in X. \forall a \in \mathcal{A}. (a \in \varphi(x) \Rightarrow ra \in \psi(x))$$

where  $r$  is broadly a *realizer* of  $\forall x \in X. \varphi(x) \Rightarrow \psi(x)$ . See [12] for further details.

**Definition 10. (Application)** Given two elements  $a, b \in \mathcal{A}$ , we call the application of  $a$  to  $b$  and write  $ab$  the element of  $\mathcal{A}$  that is defined by

$$ab \triangleq \bigwedge \{c \in \mathcal{A} : a \preceq (b \rightarrow c)\}.$$

If we think of the order relation  $a \preceq b$  as “ $a$  is more precise than  $b$ ”, the above definition actually defines the application  $ab$  as the meet of all the elements  $c$  such that  $b \rightarrow c$  is an approximation of  $a$ . This definition fulfills the usual properties of the  $\lambda$ -calculus:

**Proposition 11. (Properties of application)** For all  $a, a', b, b', c \in \mathcal{A}$  :

1. If  $a \preceq a'$  and  $b \preceq b'$ , then  $ab \preceq a'b'$  (Monotonicity)
2.  $(a \rightarrow b)a \preceq b$  ( $\beta$ -reduction)
3.  $a \preceq (b \rightarrow ab)$  ( $\eta$ -expansion)
4.  $ab = \min\{c \in \mathcal{A} : a \preceq (b \rightarrow c)\}$  (Minimum)
5.  $ab \preceq c \Leftrightarrow a \preceq (b \rightarrow c)$  (Adjunction)

*Proof.* Simple lattice manipulations using the properties of the arrow.

**Remark 12. (Galois connection)** The adjunction  $ab \preceq c \Leftrightarrow a \preceq (b \rightarrow c)$  expresses the existence of a family of Galois connections  $f_b \dashv g_b$  indexed by all  $b \in \mathcal{A}$ , where the left and right adjoints  $f_b, g_b : \mathcal{A} \rightarrow \mathcal{A}$  are defined by:

$$f_b : a \mapsto ab \quad \text{and} \quad g_b : c \mapsto (b \rightarrow c) \quad (\text{for all } a, b, c \in \mathcal{A})$$

Recall that in a Galois connection, the left adjoint is fully determined by the right one (and vice-versa). In the particular case of a complete Heyting algebra  $(\mathcal{H}, \preceq, \rightarrow)$ , this implies that the application is characterized by  $ab = a \wedge b$  for all  $a, b \in \mathcal{H}$ . Indeed, in any Heyting algebra, the adjunction  $a \wedge b \preceq c \Leftrightarrow a \preceq (b \rightarrow c)$  holds for all  $a, b, c \in \mathcal{H}$ , by uniqueness of the left adjoint,  $ab$  and  $a \wedge b$  are thus equal.

**Definition 13. (Abstraction)** Given a function  $f : \mathcal{A} \rightarrow \mathcal{A}$ , we call abstraction of  $f$  and write  $\lambda f$  the element of  $\mathcal{A}$  defined by:

$$\lambda f \triangleq \bigwedge_{a \in \mathcal{A}} (a \rightarrow f(a))$$

Once again, if we think of the order relation  $a \preceq b$  as “ $a$  is more precise than  $b$ ”, the meet of the elements of a set  $S$  is an element containing the union of all the informations given by the elements of  $S$ . With this in mind, the above definition sets  $\lambda f$  as the union of all the step functions  $a \rightarrow f(a)$ . This definition, together with the definition of the application, fulfills again properties expected from the  $\lambda$ -calculus:

**Proposition 14. (Properties of the abstraction)** The following holds for any  $f, g : \mathcal{A} \rightarrow \mathcal{A}$ :

1. If for all  $a \in \mathcal{A}$ ,  $f(a) \preceq g(a)$ , then  $\lambda f \preceq \lambda g$ . (Monotonicity)

2. For all  $a \in \mathcal{A}$ ,  $(\lambda f)a \preceq f(a)$ . ( $\beta$ -reduction)  
3. For all  $a \in \mathcal{A}$ ,  $a \preceq \lambda(x \mapsto ax)$ . ( $\eta$ -expansion)

*Proof.* Again, the proof consists in easy lattices manipulations.

We call a  $\lambda$ -term with parameters (in  $\mathcal{A}$ ) any term defined from the following grammar<sup>11</sup>:

$$t, u ::= x \mid a \mid \lambda x.t \mid tu$$

where  $x$  is a variable and  $a$  is an element of  $\mathcal{A}$ . We can thus associate to each closed  $\lambda$ -term with parameters  $t$  an element  $t^{\mathcal{A}}$  of  $\mathcal{A}$ , defined by induction on the size of  $t$  as follows (where  $a \in \mathcal{A}$ ):

$$a^{\mathcal{A}} \triangleq a \quad (tu)^{\mathcal{A}} \triangleq (t^{\mathcal{A}})u^{\mathcal{A}} \quad (\lambda x.t)^{\mathcal{A}} \triangleq \lambda(a \mapsto (t[a/x])^{\mathcal{A}})$$

Thanks to the properties of the application and of the abstraction in implicative structures that we proved, we can check that the embedding of  $\lambda$ -term is sound with respect to the  $\beta$ -reduction:

**Proposition 15.** *For all closed  $\lambda$ -terms  $t$  and  $u$  with parameters in  $\mathcal{A}$ , if  $t \rightarrow_{\beta} u$ , then  $t^{\mathcal{A}} \preceq u^{\mathcal{A}}$ .*

*Proof.* By induction on the reduction  $t \rightarrow_{\beta} u$  using Propositions 11 and 14.

Again, if we think of the order relation  $a \preceq b$  as “ $a$  is more precise than  $b$ ”, it makes sense that the  $\beta$ -reduction  $t \rightarrow_{\beta} u$  is reflected in the ordering  $t^{\mathcal{A}} \preceq u^{\mathcal{A}}$ : the result of a computation contains indeed less information than the computation itself<sup>10</sup>.

## 4.2 Adequacy

We now dispose of a structure in which we can interpret types and  $\lambda$ -terms. We saw that the interpretation of terms was intuitively sound with respect to the  $\beta$ -reduction. We shall now prove that the typing rules of System F are adequate with respect to the interpretation of terms, that is to say that if  $t$  is a closed  $\lambda$ -term of type  $T$ , then  $t^{\mathcal{A}} \preceq T^{\mathcal{A}}$ . The last statement can again be understood as the fact that a term (*i.e.* a computation) carries more information than its type, just like a realizer of a formula is more informative about the formula than the formula itself.

**Adequacy of the interpretation** For the formalization of the former result, we chose a slightly different approach that we shall now sketch. First, we extend the usual formulas of System F by defining second-order formulas with parameters as:

$$A, B ::= a \mid X \mid A \Rightarrow B \mid \forall X.A \quad (a \in \mathcal{A})$$

<sup>10</sup> For instance, 0 contains less information than  $15 - (3 \times 5)$  or than  $\mathbf{1}_{\mathbb{Q}}(\sqrt{(2)})$ .

We can then embed closed formulas with parameters into the implicative structure  $\mathcal{A}$ . The embedding is trivially defined (where  $a \in \mathcal{A}$ ):

$$a^{\mathcal{A}} \triangleq a \quad (A \Rightarrow B)^{\mathcal{A}} \triangleq A^{\mathcal{A}} \rightarrow B^{\mathcal{A}} \quad (\forall X.A)^{\mathcal{A}} \triangleq \bigwedge_{a \in \mathcal{A}} (A\{X := a\})^{\mathcal{A}}$$

We define a type system for the  $\lambda_c$ -calculus with parameters<sup>11</sup> (that is  $\lambda$ -terms with parameter plus an instruction  $\mathbf{cc}$ ). Typing contexts are defined as usual by finite lists of hypotheses of the shape  $(x : A)$  where  $x$  is a variable and  $A$  a formula with parameters. The inference rules, given in Figure 1, are the same as in System F (with the extended syntaxes of terms and formulas with parameters), plus the additional rules for  $\mathbf{cc}$ .

In order to prove the adequacy of the type system with respect to the embedding, we define substitutions, which we write  $\sigma$ , as functions mapping variables (of terms and types) to element of  $\mathcal{A}$ :

$$\sigma ::= \varepsilon \mid \sigma[x \mapsto a] \mid \sigma[X \mapsto a] \quad (a \in \mathcal{A}, x, X \text{ variables})$$

In the spirit of the proof of adequacy in classical realizability, we say that a substitution  $\sigma$  realizes a typing context  $\Gamma$ , which we write  $\sigma \Vdash \Gamma$ , if for all bindings  $(x : A) \in \Gamma$  we have  $\sigma(x) \preceq (A[\sigma])^{\mathcal{A}}$ .

**Theorem 16. (Adequacy)** *The typing rules of Figure 1 are adequate with respect to the interpretation of terms and formulas: if  $t$  is a  $\lambda_c$ -term with parameters,  $A$  a formula with parameters and  $\Gamma$  a typing context such that  $\Gamma \vdash t : A$  then for all substitutions  $\sigma \Vdash \Gamma$ , we have  $(t[\sigma])^{\mathcal{A}} \preceq (A[\sigma])^{\mathcal{A}}$ .*

*Proof.* The proof resembles the usual proof of adequacy in classical realizability (see [13,19]), namely by induction on typing derivations.

In the particular case where  $t$  is a closed term typed by  $A$  in the empty context, we obtain that  $t^{\mathcal{A}} \preceq A^{\mathcal{A}}$ . This result will be fundamental in the next section.

**Corollary 17.** *For all  $\lambda$ -terms  $t$ , if  $\vdash t : A$ , then  $t^{\mathcal{A}} \preceq A^{\mathcal{A}}$ .*

### 4.3 Combinators

The previous results indicate that any closed  $\lambda$ -term is, through the interpretation, lower than the interpretation of its principal type. We give here some examples of closed  $\lambda$ -terms which are in fact equal to their principal types through the interpretation in  $\mathcal{A}$ . Let us now consider the following combinators:

$$\mathbf{i} \triangleq \lambda x.x \quad \mathbf{k} \triangleq \lambda xy.x \quad \mathbf{s} \triangleq \lambda xyz.xz(yz) \quad \mathbf{w} \triangleq \lambda xy.xyy$$

<sup>11</sup> In practice, we use Charguéraud's locally nameless representation [2] for terms and formulas. Without giving too much details, we actually define pre-terms and pre-types which allow both for names (for free variables) and De Bruijn indices (for bounded variables). Terms and types are then defined as pre-terms and pre-types without free De Bruijn indices. Such a representation is particularly convenient to prevent from name clashes to arise.

$\frac{(x : A) \in \Gamma}{\Gamma \vdash x : A}$	$\frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x. t : A \rightarrow B}$	$\frac{\Gamma \vdash t : A \rightarrow B \quad \Gamma \vdash t : A}{\Gamma \vdash tu : B}$
$\frac{\Gamma \vdash t : A}{\Gamma \vdash t : \forall X. A}^{(X \notin FV(\Gamma))}$	$\frac{\Gamma \vdash t : \forall X. A}{\Gamma \vdash t : A\{X := B\}}$	$\frac{}{\Gamma \vdash \mathbf{cc} : ((A \rightarrow B) \rightarrow A) \rightarrow A}$

**Fig. 1.** Second-order type system for the  $\lambda_c$ -calculus

It is well-known that these combinators can be given the following polymorphic types:

$$\begin{array}{l|l} \mathbf{i} : \forall X. X \Rightarrow X & \mathbf{s} : \forall XYZ. (X \Rightarrow Y \Rightarrow Z) \Rightarrow (X \Rightarrow Y) \Rightarrow X \Rightarrow Z \\ \mathbf{k} : \forall XY. X \Rightarrow Y \Rightarrow X & \mathbf{w} : \forall XY. (X \Rightarrow X \Rightarrow Y) \Rightarrow X \Rightarrow Y \end{array}$$

Through the interpretation these combinators are identified with their types:

**Proposition 18.** *The following equalities hold in any implicative structure  $\mathcal{A}$ :*

1.  $\mathbf{i}^{\mathcal{A}} = \bigwedge_{a \in \mathcal{A}} (a \rightarrow a)$
2.  $\mathbf{k}^{\mathcal{A}} = \bigwedge_{a, b \in \mathcal{A}} (a \Rightarrow b \Rightarrow a)$
3.  $\mathbf{s}^{\mathcal{A}} = \bigwedge_{a, b, c \in \mathcal{A}} ((a \rightarrow b \rightarrow c) \rightarrow (a \rightarrow b) \rightarrow a \rightarrow c)$
4.  $\mathbf{w}^{\mathcal{A}} = \bigwedge_{a, b, c \in \mathcal{A}} ((a \rightarrow a \rightarrow b) \rightarrow a \rightarrow b)$

*Proof.* The inequality from left to right are consequences of the adequacy. The converse inequalities are proved by hands, using the properties of application and abstraction in implicative structures (Propositions 11 and 14).

Finally, in the spirit of the previous equalities, we define the interpretation of  $\mathbf{cc}$  by the interpretation of its principal type, that is:

$$\mathbf{cc}^{\mathcal{A}} \triangleq \mathbf{cc} = \bigwedge_{a, b} (((a \rightarrow b) \rightarrow a) \rightarrow a)$$

**Remark 19.** *It is not always the case that a term is equal to its principal type. Consider for instance a dummy implicative structure  $\mathcal{A}$  where  $a \rightarrow b = \top$  for all elements  $a, b \in \mathcal{A}$ . Suppose in addition that  $\mathcal{A}$  has at least two distinct elements, so that  $\perp \neq \top$ . Then the following holds:*

1. For any  $a, b \in \mathcal{A}$ , we have  $ab = \bigwedge \{c : a \leq b \rightarrow c\} = \bigwedge \mathcal{A} = \perp$ .
2. For any  $f : \mathcal{A} \rightarrow \mathcal{A}$ , we have  $\lambda f = \bigwedge_{a \in \mathcal{A}} (a \rightarrow f(a)) = \bigwedge_{a \in \mathcal{A}} \top = \top$ .
3.  $\mathbf{ii} : \forall X. X \rightarrow X$ , yet  $(\mathbf{ii})^{\mathcal{A}} = \perp \neq \top = (\forall X. X \rightarrow X)^{\mathcal{A}}$ .
4.  $\mathbf{i}^{\mathcal{A}} = \top \neq \perp = (\mathbf{skk})^{\mathcal{A}}$ .

#### 4.4 The problem of consistency

The last remark shows us that not all implicative structures are suitable for interpreting intuitionistic or classical logic. We thus need to introduce a criterion of consistency:

**Definition 20. (Consistency)** We say that an implicative structure is:

- intuitionistically consistent if  $t^A \neq \perp$  for all closed  $\lambda$ -terms;
- classically consistent if  $t^A \neq \perp$  for all closed  $\lambda_c$ -terms.

We shall now relate the previous definition to the usual definition of consistency in classical realizability. Recall that any abstract Krivine structures  $\mathcal{K} = (\mathbf{A}, \mathbf{\Pi}, \mathbf{app}, \mathbf{push}, \mathbf{k}, \mathbf{s}, \mathbf{cc}, \mathbf{PL}, \perp)$  induces an implicative structure  $(\mathcal{A}, \preceq, \rightarrow)$  where  $\mathcal{A} = \mathcal{P}(\mathbf{\Pi})$ ,  $a \preceq b \Leftrightarrow a \supseteq b$  and  $a \rightarrow b = a^\perp \cdot b$ . A realizability model is said to be consistent when there is no proof-like term realizing  $\perp$ . In terms of abstract Krivine structures, the consistency can then be expressed by this simple criterion:

$$\mathcal{K} \text{ is consistent} \quad \text{if and only if} \quad \{\perp\}^\perp \cap \mathbf{PL} = \mathbf{\Pi}^\perp \cap \mathbf{PL} = \emptyset$$

We thus need to check that this criterion of consistency for the AKS implies the consistency of the induced implicative algebra, *i.e.* that if  $t$  is a closed  $\lambda_c$ -term, then  $t^A \neq \perp$ . By definition of the implicative algebra  $\mathcal{A}$  induced the AKS, we have that  $t^A \in \mathcal{A} = \mathcal{P}(\mathbf{\Pi})$ . Therefore,  $t^A$  is a falsity value from the point of view of the AKS. To ensure that it is not equal to  $\perp$  (*i.e.*  $\mathbf{\Pi}$ ), it is enough to find a realizer of  $t^A$  in the AKS. The consistency of the AKS precisely states that  $\perp$  does not have any realizer.

Our strategy to find a realizer for  $t^A$  in the AKS is to use  $t$  itself. First, we reduce the problem to the set of terms that are identifiable with the combinatory terms of the AKS. We call a *combinatory term* any term that is obtained by combination of the previous combinators. To each combinatory term  $t$  we associate a term  $t^A$  in  $\mathbf{A}$ , whose definition by induction is trivial:

$$\mathbf{k}^A \triangleq \mathbf{k} \quad \mathbf{s}^A \triangleq \mathbf{s} \quad \mathbf{cc}^A \triangleq \mathbf{cc} \quad (tu)^A \triangleq \mathbf{app}(t^A, u^A)$$

Since the set  $\mathbf{PL}$  is closed under application, for any combinatory term  $t$ , its interpretation  $t^A$  is in  $\mathbf{PL}$ . The combinatory completeness of  $(\mathbf{k}, \mathbf{s}, \mathbf{cc})$  with respect to closed  $\lambda_c$ -terms ensures us that there exists a combinatory term  $t_0$  (viewed as a  $\lambda$ -term) such that  $t_0 \rightarrow_\beta t$ . By Proposition 15, we thus have  $t_0^A \preceq t^A$ . It is thus enough to show that  $t_0^A \neq \perp$ : we reduced the original problem for closed  $\lambda_c$ -terms to combinatory terms.

It thus only remains to show that for any combinatory term  $t_0$ , its interpretation  $t_0^A$  is not  $\perp$ . For the reason detailed above, it is sufficient to prove that  $t_0^A$  is realized. We prove that  $t_0^A$  is in fact realized by  $t_0^A$ :

**Lemma 21.** For any combinatory term  $t$ ,  $t^A$  realizes  $t^A$ , *i.e.*  $t^A \Vdash t^A$

*Proof.* By induction on the structure of  $t$ , by combining usual results of classical realizability and properties of the implicative structures.

We can thus conclude that the consistency of the AKS induces the one (in the sense of Definition 20) of the associated implicative structures:

**Proposition 22.** If  $\mathcal{K}$  is a consistent abstract Krivine structure, then the implicative structure it induces is classically consistent.

*Proof.* Let  $t$  be any closed  $\lambda_c$ -term. We want to show that  $t^A \neq \perp = \mathbf{II}$ . We show that  $t^A$ , which belongs to  $\mathcal{P}(\mathbf{II})$  is realized by a proof-like term

It is worth noting that the criterion of consistency is defined with respect to the set  $\mathbf{PL}$  together with the pole. These sets are already at the heart of the definition of Krivine's realizability models, where valid formulas are precisely the formulas realized by a proof-like term. We shall then introduce the corresponding ingredient for implicative structures.

## 5 Implicative algebras

### 5.1 Separation

**Definition 23. (Separator)** Let  $(\mathcal{A}, \preceq, \rightarrow)$  be an implicative structure. We call a separator over  $\mathcal{A}$  any set  $\mathcal{S} \subseteq \mathcal{A}$  such that for all  $a, b \in \mathcal{A}$ , the following conditions hold:

1.  $\mathbf{k}^A \in \mathcal{S}$ , and  $\mathbf{s}^A \in \mathcal{S}$ . (Combinators)
2. If  $a \in \mathcal{S}$  and  $a \preceq b$ , then  $b \in \mathcal{S}$ . (Upwards closure)
3. If  $(a \rightarrow b) \in \mathcal{S}$  and  $a \in \mathcal{S}$ , then  $b \in \mathcal{S}$ . (Closure under modus ponens)

A separator  $\mathcal{S}$  is said to be classical if besides  $\mathbf{cc}^A \in \mathcal{S}$  and consistent if  $\perp \notin \mathcal{S}$ .

**Remark 24. (Alternative definition)** In presence of condition (2), it is easy to show that condition (3) is equivalent to the following condition:

- (3') If  $a \in \mathcal{S}$  and  $b \in \mathcal{S}$  then  $ab \in \mathcal{S}$  (Closure under application)

Intuitively, thinking of elements of an implicative structure as truth values, a separator should be understood as the set which distinguishes the valid formulas. Considering the elements as terms, it should rather be viewed as the set of valid realizers. Indeed, conditions (1) and (3') ensure that all closed  $\lambda$ -terms are in any separator. Reading  $a \preceq b$  as “the formula  $a$  is a subtype of the formula  $b$ ”, condition (2) ensures the validity of semantic subtyping. Thinking of the ordering as “ $a$  is a realizer of the formula  $b$ ”, condition (2) states that if a formula is realized, then it is in the separator.

**Definition 25. (Implicative algebra)** We call implicative algebra any quadruple  $(\mathcal{A}, \preceq, \rightarrow, \mathcal{S})$  where  $(\mathcal{A}, \preceq, \rightarrow)$  is an implicative structure and  $\mathcal{S}$  is a separator over  $\mathcal{A}$ . We say that an implicative algebra is classical if its separator is.

**Example 26. (Complete Boolean algebras)** It is easy to verify that for any complete Boolean algebra  $\mathcal{B}$ , combinators are interpreted by the maximal element in the induced implicative structure:  $\mathbf{k}^{\mathcal{B}} = \mathbf{s}^{\mathcal{B}} = \mathbf{cc}^{\mathcal{B}} = \top$ . Therefore, the singleton  $\{\top\}$  is a classical separator for the induced implicative structure. Any non-degenerated complete Boolean algebra thus induces a classically consistent implicative algebra.

**Example 27. (Abstract Krivine structure)** Recall that any AKS induces an implicative structure  $(\mathcal{A}, \preceq, \rightarrow)$  where  $\mathcal{A} = \mathcal{P}(\mathbf{II})$ ,  $a \preceq b \Leftrightarrow a \supseteq b$  and  $a \rightarrow b = a^\perp \cdot b$ . The sets of realized formulas, namely  $\mathcal{S} = \{a \in \mathcal{A} : a^\perp \cap \mathbf{PL} \neq \emptyset\}$ , defines a valid separator.

## 5.2 $\lambda_c$ -terms

The first property that we shall state about classical separators is that they contain the interpretation of all closed  $\lambda_c$ -terms. This follows again from the combinatory completeness of the basis  $(\mathbf{k}, \mathbf{s}, \mathbf{cc})$  for the  $\lambda_c$ -calculus<sup>12</sup>. Indeed, if  $\mathcal{S}$  is a classical separator over an implicative structure  $(\mathcal{A}, \preceq, \rightarrow)$ , it is clear that any combinatory term is in the separator. Again, by combinatory completeness, if  $t$  is a closed  $\lambda_c$ -term, there exists a combinatory term  $t_0$  such that  $t_0 \rightarrow_\beta t$ , and therefore  $t_0^A \preceq t^A$  (by Proposition 15). By upward closure of separators, we deduce that:

**Proposition 28.** *If  $(\mathcal{A}, \preceq, \rightarrow, \mathcal{S})$  is a (classical) implicative algebra and  $t$  is a closed  $\lambda$ -term (resp.  $\lambda_c$ -term), then  $t^A \in \mathcal{S}$ .*

From the previous proposition and the adequacy of second-order typing rules for the  $\lambda_c$ -calculus (Theorem 16), we obtain that:

**Corollary 29.** *If  $(\mathcal{A}, \preceq, \rightarrow, \mathcal{S})$  is a (classical) implicative algebra,  $t$  is a closed  $\lambda$ -term (resp.  $\lambda_c$ -term) and  $A$  is a formula such that  $\vdash t : A$ , then  $A^A \in \mathcal{S}$ .*

**Remark 30.** *The latter corollary provides us with a methodology for proving that an element of a given implicative algebra is in the separator. In the spirit of realizability, where the standard methodology to prove that a formula is realized consists in using typed terms and adequacy as much as possible, we can use typed terms to prove automatically that the corresponding formulas belongs to the separator. We shall use this methodology abundantly in the sequel. In the Coq development, this corresponds to a tactic called *realizer* which allows us to prove that an element belongs to the separator simply by furnishing a realizer:*

*Lemma composition:*  $\forall a b c, (a \mapsto b) \mapsto (b \mapsto c) \mapsto a \mapsto c \in \mathcal{S}$   
*Proof. intros. realizer (( $\lambda^+ \lambda^+ \lambda^+ ([\$1] ([\$2] \$0))$ )). Qed. (\*\*  $\lambda xyz.y(xz)$  \*)*

## 5.3 Internal logic

In order to be able to define triposes from implicative algebras, the first step is to equip them with a structure of Heyting algebra. To this end, we begin with defining an entailment relation in the spirit of filtered OCAs [12]. We then define quantifiers and connectives as usual in classical realizability (see [13]), and we verify that they satisfy the usual logical rules. In the rest of this section, we work within a fixed implicative algebra  $(\mathcal{A}, \preceq, \rightarrow, \mathcal{S})$ .

**Definition 31. (Entailment)** *For all  $a, b \in \mathcal{A}$ , we say that  $a$  entails  $b$  and write  $a \vdash_{\mathcal{S}} b$  if  $a \rightarrow b \in \mathcal{S}$ . We say that  $a$  and  $b$  are equivalent and write  $a \cong_{\mathcal{S}} b$  if  $a \vdash_{\mathcal{S}} b$  and  $b \vdash_{\mathcal{S}} a$ .*

**Proposition 32. (Properties of  $\vdash_{\mathcal{S}}$ )** *For any  $a, b, c \in \mathcal{A}$ , the following holds:*

<sup>12</sup> In order to avoid the certification of the corresponding compilation function, we state this well-known fact as an axiom (the only one) in our development.

1.  $a \vdash_{\mathcal{S}} a$  (Reflexivity)
2. if  $a \vdash_{\mathcal{S}} b$  and  $b \vdash_{\mathcal{S}} c$  then  $a \vdash_{\mathcal{S}} c$  (Transitivity)
3. if  $a \preceq b$  then  $a \vdash_{\mathcal{S}} b$  (Subtyping)
4. if  $a \cong_{\mathcal{S}} b$  then  $a \in \mathcal{S}$  if and only if  $b \in \mathcal{S}$  (Closure under  $\cong_{\mathcal{S}}$ )
5. if  $a \vdash_{\mathcal{S}} b \rightarrow c$  then  $a \wedge b \vdash_{\mathcal{S}} c$  (Half-adjunction property)
6.  $\perp \vdash_{\mathcal{S}} a$  (Ex falso quod libet)
7.  $a \vdash_{\mathcal{S}} \top$  (Maximal element)

*Proof.* Straightforward from the definitions, using  $\lambda xyz.y(xz)$  to realize the second item and  $\lambda xy.xyy$  to realize the fifth.

Besides, the entailment relation behaves like Heyting's arrow with respect to the preorder relation  $\vdash_{\mathcal{S}}$  in terms of monotonicity:

**Proposition 33. (Compatibility with  $\rightarrow$ )** For all  $a, a', b, b' \in \mathcal{A}$ , we have:

1. If  $b \vdash b'$  then  $a \rightarrow b \vdash a \rightarrow b'$
2. If  $a \vdash a'$  then  $a' \rightarrow b \vdash a \rightarrow b$

*Proof.* Direct using  $\lambda xyz.x(yz)$  and  $\lambda xyz.y(xz)$  as realizers.

**Negation** Recall that the negation is defined by  $\neg a \triangleq a \rightarrow \perp$ . If additionally the separator is classical, we can prove that for any  $a \in \mathcal{A}$ , we have:

**Proposition 34. (Double negation)** If  $\mathcal{S}$  is a classical separator, for any  $a \in \mathcal{A}$  we have: 1.  $a \vdash_{\mathcal{S}} \neg\neg a$  2.  $\neg\neg a \vdash_{\mathcal{S}} a$

*Proof.* The first item is realized by  $\lambda xk.kx$ , while the second follows from the inequality  $((a \rightarrow \perp) \rightarrow a) \rightarrow a \preceq ((a \rightarrow \perp) \rightarrow \perp) \rightarrow a$ , whose left member is realized by **cc**.

**Quantifiers** Following the usual definition in classical realizability (see [13,19]), the universal quantification of a family of truth values is naturally defined as its meet while the existential quantification is defined through a negative encoding:

$$\bigvee_{i \in I} a_i \triangleq \bigwedge_{i \in I} a_i \qquad \bigexists_{i \in I} a_i \triangleq \bigwedge_{c \in \mathcal{A}} \left( \bigwedge_{i \in I} (a_i \rightarrow c) \rightarrow c \right)$$

While it could have seemed more natural to define existential quantifiers through joins, we should recall that the arrow does not commute with joins in general<sup>13</sup>. It is clear that these definitions are compatible with the expected semantic rules:

**Proposition 35. (Universal quantifier)** The following semantic typing rules are valid in any implicative structures:

$$\frac{\Gamma \vdash t : a_i \text{ for all } i \in I}{\Gamma \vdash t : \bigvee_{i \in I} a_i} \qquad \frac{\Gamma \vdash t : \bigvee_{i \in I} a_i \quad i_0 \in I}{\Gamma \vdash t : a_{i_0}}$$

<sup>13</sup> When it does, the realizability tripes actually collapses to a forcing tripes, see [18,19]

**Proposition 36. (Existential quantifier)** *The following semantic typing rules are valid in any implicative structures:*

$$\frac{\Gamma \vdash t : a_{i_0} \quad i_0 \in I}{\Gamma \vdash \lambda x.xt : \exists_{i \in I} a_i} \qquad \frac{\Gamma \vdash t : \exists_{i \in I} a_i \quad \Gamma, x : a_i \vdash u : c \quad (\text{for all } i \in I)}{\Gamma \vdash t(\lambda x.u) : c}$$

*Proof.* Straightforward using the adjunction of the application (Proposition 11).

**Sum and product** We define it by the usual encodings in System F:

$$a \times b \triangleq \bigwedge_{c \in \mathcal{A}} ((a \rightarrow b \rightarrow c) \rightarrow c) \qquad a + b \triangleq \bigwedge_{c \in \mathcal{A}} ((a \rightarrow c) \rightarrow (b \rightarrow c) \rightarrow c)$$

Recall that the pair  $\langle a, b \rangle$  is encoded by the  $\lambda$ -term  $\lambda x.xab$ , while first and second projection are respectively defined by  $\pi_1 \triangleq \lambda xy.x$  and  $\pi_2 \triangleq \lambda xy.y$ . We can check that the expected semantic typing rules are valid

**Proposition 37. (Product)** *The following semantic typing rules are valid:*

$$\frac{\Gamma \vdash t : a \quad \Gamma \vdash u : b}{\Gamma \vdash \lambda z.ztu : a \times b} \qquad \frac{\Gamma \vdash t : a \times b}{\Gamma \vdash t\pi_1 : a} \qquad \frac{\Gamma \vdash t : a \times b}{\Gamma \vdash t\pi_2 : b}$$

**Proposition 38. (Sum)** *The following semantic typing rules are valid:*

$$\frac{\Gamma \vdash t : a}{\Gamma \vdash \lambda r.lt : a + b} \qquad \frac{\Gamma \vdash t : b}{\Gamma \vdash \lambda r.rt : a + b} \qquad \frac{\Gamma \vdash t : a_1 + a_2 \quad \Gamma, x_i : a_i \vdash u_i : c}{\Gamma \vdash t(\lambda x_1.u_1)(\lambda x_2.u_2) : c}$$

*Proof.* Straightforward lattice manipulation, similar to the proof for the existential quantifier.

The natural candidate to computationally represents a “meet” of  $a$  and  $b$  is the product type  $a \times b$ . We can verify that it satisfies the expected property (in Heyting algebras) w.r.t. to the arrow:

**Proposition 39. (Adjunction)** *For any  $a, b, c \in \mathcal{A}$ , we have  $a \vdash_{\mathcal{S}} b \rightarrow c$  if and only if  $a \times b \vdash_{\mathcal{S}} c$ .*

*Proof.* Both directions are proved using the expected realizer and subtyping: from left to right, we use  $\lambda xy.yx$  to realize  $(a \rightarrow b \rightarrow c) \rightarrow a \times b \rightarrow c$ ; from right to left, we realize  $(a \times b \rightarrow c) \rightarrow a \rightarrow b \rightarrow c$  with  $\lambda pxy.p(\lambda z.zxy)$ .

## 5.4 Implicative tripos

It is clear from the properties of implicative algebras presented in the last sections that the entailment relation together with the sum and products induce a structure of Heyting prealgebra (indeed, the entailment relation only defines a preorder). By considering the quotient  $\mathcal{A}/\cong_{\mathcal{S}}$  of the former Heyting prealgebra by the relation  $\cong_{\mathcal{S}}$ , and lifting the previous definitions of connectives and quantifiers

to equivalence classes, we thus obtain a Heyting algebra<sup>14</sup>. This construction is actually the main step towards the definition of the implicative tripos [18,19], which allows us to recover the usual categorical interpretation of realizability models. In particular, it provides us with a framework in which simple criteria allows us to compare classical realizability and forcing models.

## 6 Conclusion & future work

### 6.1 Conclusion

We presented in this paper Miquel’s concept of *implicative algebra* [18], that relies on the primitive notion of implicative structure. These structures are defined as a particular class of meet-complete lattices equipped with an arrow, where this arrow satisfies commutations with arbitrary meets which are the counterpart of the logical commutation between the universal quantification and the implication. We showed that implicative structures are a generalization Streicher’s AKSs [24] and Ferrer *et al.*’s  $\mathcal{K}$ OCAAs [6,7]. Besides, they provide us with a framework in which both  $\lambda_c$ -terms and their types can be interpreted. This has the nice consequence that we really consider the elements of the implicative structure as  $\lambda_c$ -terms and that we can compute with truth values. Through the formalization, this is reflected by a tactic allowing us to prove that elements belong to the separator by simply furnishing realizers.

### 6.2 Future work

For future work, it would be interesting to push the formalization further to be able to represent implicative triposes. However, this poses the challenge of manipulating quotients and equivalent classes. The safe definition of quotients within CIC (and thus Coq) is indeed a tricky question [11,3,4], and as for now, we do not know which technical solution (reasoning modulo setoids, quotient as types classes, etc.) would be the more adapted to our situation.

In a more theoretic perspective, implicative algebras take position on a presentation of logic through universal quantification and the implication. The computational counterpart of this choice is that the presentation relies on the call-by-name  $\lambda_c$ -calculus. This raises the question of knowing whether it is possible to have alternative presentations with similar structures based on different connectives (and thus different calculi). We partially undertook<sup>15</sup> this investigation in [19] by studying different presentations based on disjunctive and conjunctive connectives and related Munch-Maccagnoni’s system L [20]. Yet, the equivalence between all presentations still remains to prove.

*Acknowledgments* The author wishes to thank Assia Mahboubi for pushing him to write the current paper.

<sup>14</sup> If the implicative algebra is classical, for all  $a \in \mathcal{A}$  we saw that  $\neg\neg a \cong_{\mathcal{S}} a$ . Through the same quotient, this implies that  $\neg\neg[a] = [a]$  for all  $a \in \mathcal{A}$ . and that the induced Heyting algebra is actually a Boolean algebra.

<sup>15</sup> The present formalization was particularly useful to this purpose.

## References

1. The poplmark challenge. URL: <https://www.seas.upenn.edu/~plclub/poplmark/>.
2. Arthur Charguéraud. The locally nameless representation. *Journal of Automated Reasoning*, 49(3):363–408, Oct 2012. doi:10.1007/s10817-011-9225-2.
3. Laurent Chicli, Loïc Pottier, and Carlos Simpson. Mathematical quotients and quotient types in coq. In Herman Geuvers and Freek Wiedijk, editors, *Types for Proofs and Programs*, pages 95–107, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.
4. Cyril Cohen. Types quotients en coq. In Hermann, editor, *Actes des 21ème journées francophones des langages applicatifs (JFLA 2010)*, Vieux-Port La Ciotat, France, 2010. INRIA. URL: <http://jfla.inria.fr/2010/actes/PDF/cyrilcohen.pdf>.
5. W. Ferrer and O. Malherbe. The category of implicative algebras and realizability. *ArXiv e-prints*, December 2017. arXiv:1712.06043.
6. W. Ferrer Santos, M. Guillermo, and O. Malherbe. Realizability in OCAs and AKSs. *ArXiv e-prints*, 2015. arXiv:1512.07879.
7. Walter Ferrer Santos, Jonas Frey, Mauricio Guillermo, Octavio Malherbe, and Alexandre Miquel. Ordered combinatory algebras and realizability. *Mathematical Structures in Computer Science*, 27(3):428–458, 2017. doi:10.1017/S0960129515000432.
8. Jonas Frey. Realizability Toposes from Specifications. In Thorsten Altenkirch, editor, *13th International Conference on Typed Lambda Calculi and Applications (TLCA 2015)*, volume 38 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 196–210, Dagstuhl, Germany, 2015. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. URL: <http://drops.dagstuhl.de/opus/volltexte/2015/5164>, doi:10.4230/LIPIcs.TLCA.2015.196.
9. Jonas Frey. Classical realizability in the cps target language. *Electronic Notes in Theoretical Computer Science*, 325(Supplement C):111 – 126, 2016. The Thirty-second Conference on the Mathematical Foundations of Programming Semantics (MFPS XXXII). doi:<https://doi.org/10.1016/j.entcs.2016.09.034>.
10. Timothy G. Griffin. A formulae-as-type notion of control. In *Proceedings of the 17th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '90, pages 47–58, New York, NY, USA, 1990. ACM. URL: <http://doi.acm.org/10.1145/96709.96714>, doi:10.1145/96709.96714.
11. M. Hofmann. *Extensional Concepts in Intensional Type Theory*. PhD thesis, University of Edinburgh, 1995.
12. Pieter Hofstra and Jaap Van Oosten. Ordered partial combinatory algebras. *Mathematical Proceedings of the Cambridge Philosophical Society*, 134(3):445–463, 2003. doi:10.1017/S0305004102006424.
13. J.-L. Krivine. Realizability in classical logic. In interactive models of computation and program behaviour. *Panoramas et synthèses*, 27, 2009.
14. J.-L. Krivine. Realizability algebras: a program to well order r. *Logical Methods in Computer Science*, 7(3), 2011.
15. J.-L. Krivine. Realizability algebras II : new models of ZF + DC. *Logical Methods in Computer Science*, 8(1):10, February 2012. 28 p.
16. J.-L. Krivine. Quelques propriétés des modèles de réalisabilité de ZF, February 2014. URL: <http://hal.archives-ouvertes.fr/hal-00940254>.

17. Alexandre Miquel. Existential witness extraction in classical realizability and via a negative translation. *Logical Methods in Computer Science*, 7(2):188–202, 2011. URL: [http://dx.doi.org/10.2168/LMCS-7\(2:2\)2011](http://dx.doi.org/10.2168/LMCS-7(2:2)2011), doi:10.2168/LMCS-7(2:2)2011.
18. Alexandre Miquel. Implicative algebras. Unpublished manuscript, 2018. URL: <https://www.fing.edu.uy/~amiquel/impalg.pdf>.
19. Étienne Miquey. *Classical realizability and side-effects*. Theses, Univ.é Paris Diderot ; Univ. de la República, Uruguay, November 2017. URL: <https://hal.inria.fr/tel-01653733>.
20. Guillaume Munch-Maccagnoni. Focalisation and Classical Realisability. In Erich Grädel and Reinhard Kahle, editors, *Computer Science Logic '09*, volume 5771 of *Lecture Notes in Computer Science*, pages 409–423. Springer, Heidelberg, 2009.
21. Andrew M. Pitts. Tripos theory in retrospect. *Mathematical Structures in Computer Science*, 12(3):265–279, 2002. doi:10.1017/S096012950200364X.
22. Frédéric Ruyer. *Proofs, Types and Subtypes*. PhD thesis, Université de Savoie, November 2006. URL: <https://tel.archives-ouvertes.fr/tel-00140046>.
23. Matthieu Sozeau and Nicolas Oury. First-class type classes. In Otmame Ait Mohamed, César Muñoz, and Sofène Tahar, editors, *Theorem Proving in Higher Order Logics*, pages 278–293, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.
24. Thomas Streicher. Krivine’s classical realisability from a categorical perspective. *Mathematical Structures in Computer Science*, 23(6):1234–1256, 2013. doi:10.1017/S0960129512000989.