Intersection types with subtyping by means of cut elimination

Olivier LAURENT

Laboratoire de l'Informatique du Parallélisme

ENS Lyon – Université de Lyon

UMR 5668 CNRS ENS-Lyon UCBL INRIA

46, allée d'Italie

69364 Lyon cedex 07 – FRANCE

`Olivier.Laurent@ens-lyon.fr`

March 13, 2012

Abstract

We give a purely syntactic proof (from scratch) of the subject equality property of the BCD intersection type system through a reformulation of the subtyping relation having a "cut-elimination" property.

Introduction

A key property of the BCD intersection type system introduced by Barendregt, Coppo and Dezani in [BCDC83] is the *subject equality property*: two λ-terms equal up to the β-equality admit the same types. This is the property proving that the set of all types which can be associated with a λ-term is an invariant of the β-reduction, thus leading to a λ-model (see also [CDCHL84, CDCZ87]).

The BCD system is based on typing rules and on a subtyping relation on types. We are not going to survey the huge literature on intersection type systems. The present paper should be readable without any specific knowledge in this topic. However we encourage the interesting reader to have a look at [vB95, RDRP04].

The purpose of this paper is to give an alternative proof (and completely self contained) of the subject equality result with a purely syntactic approach. The main novelty lies in the precise analysis of the subtyping relation based on a formulation of this relation which makes the transitivity rule superfluous.

If we focus on the subtyping relation as presented in [BCDC83], the transitivity rule obfuscates a lot the reasoning about subtyping. From a proof-theoretical point of view, the transitivity rule corresponds to the cut rule. The reason why cuts make reasoning about derivations complicated is often analysed as the fact that it violates the sub-formula property. The answer to this problem in proof theory is to define systems in which the cut rule is admissible (and thus can be eliminated in derivations), leading to the sub-formula property. Being able to eliminate cuts often requires to turn axioms into appropriate logical rules. This is what we are going to do with subtyping rules.

We have tried to make the structure of the subject equality proof as simple as possible, as summarized in Figure 1. An important consequence is the possibility to delineate the points where the results really depend on the subtyping relation. This allows us to make the proof modular: as soon as the CSR condition (*i.e.* core subtyping rules of Table 2 are valid) is satisfied as well as the arrow subtyping lemma (Lemma 5), the proof applies and the subject equality result holds.

The intermediary steps appearing in the proof, from the arrow subtyping lemma to the subject reduction and subject expansion properties are already used in many papers. If we look at syntactic proofs from the literature we can mention that: the arrow subtyping lemma (Lemma 5) is [BCDC83, Lemma 2.4], the variable typing lemma (Lemma 7) is equivalent to [CDCZ87, Lemma 1.7(i)], the application typing lemma (Lemma 8) is equivalent to [BCDC83, Lemma 2.8(i)], the arrow typing lemma (Lemma 9) is [RDRP04, Lemma 10.1.7(iv)], the arrow abstraction typing lemma (Lemma 10) is proved as an intermediary step for [BCDC83, Lemma 2.8(iii)] (and is necessary for subject equality to hold: [CDCHL84, Theorem 4.8] and [CDCZ87, Theorem 2.6]), the proof of the subject expansion property (Proposition 2) is a detailed version of the proof in [CDCZ87, Corollary 2.7(ii)]. More generally [RDRP04, Lemma 10.1.7] summarizes most of these results.

We can mention two specific points in our approach: first the notion of canonical derivation makes a bit more uniform and simpler the proofs of a few of the intermediary results, and second we develop our proofs with assuming the core subtyping rules of Table 2 to hold, while the previous references to the literature directly assume that the rules of Table 5 also hold (or at least the first two).

But the important novelty lies in the use of a cut-elimination property to prove the arrow subtyping lemma (Lemmas 5, 14 and 18). The idea of presenting the subtyping relation through a sequent calculus, and to deduce the arrow subtyping lemma from it, already appears in [IK02]. We give here a slightly different system and extend it with the Ω type and with an arbitrary number of type variables (we also take into account additional type inequations required for a subject equality property with respect to the η-reduction). The obtained system leads to the same provability relation as its (*trans*)-free version. If this (*trans*)-free version does not satisfies the sub-formula property, it allows us anyway to prove the arrow subtyping lemma in a completely direct way (no need to introduce more complex induction hypotheses).

We first present a complete development of our approach in Section 1. This allows us to present our method in a simple case and to introduce the core subtyping rules and the associated notion of canonical derivation. Section 2 is devoted to the extension of the subtyping system to a system equivalent to the one presented in [BCDC83]. The work of Section 1 allows us to obtain subject equality in Section 2 by only reproving the arrow subtyping lemma. The equivalence with the BCD system is explicitly proved in Section 3. Finally, Section 4 is devoted to the extension of the results to the extensional case: subject equality with respect to $\beta\eta$. This corresponds to the extension of the subtyping relation with the inequations $X \leq \Omega \to X$ and $\Omega \to X \leq X$ [CDCHL84, RDRP04].

1 The typing system with the core subtyping relation

Type variables are denoted by X, Y, ... and types are built from variables and the constant Ω by means of the two binary operations $\cap$ and $\to$:

$$A \quad ::= \quad X \mid \Omega \mid A \cap A \mid A \to A$$

In order to enhance readability, we use the notation $\bigcap_{i \in I} A_i$ for a type obtained *in some way* by applying $\cap$ connectives to the types in $(A_i)_{i \in I}$. If $I = \emptyset$, such an empty intersection is a notation for Ω. If I is a singleton $\{i\}$ then it is simply a notation for A_i.

$$
\begin{tikzcd}
 & & \begin{array}{c}\text{variable typing}\\ \text{(Lemma 7)}\end{array} \arrow[dr] & \\
\begin{array}{c}\boxed{\text{CSR}}\\ \text{(Table 2)}\end{array} \arrow[r] & \begin{array}{c}\text{canonical}\\ \text{derivations}\\ \text{(Lemma 6)}\end{array} \arrow[ur] \arrow[r] \arrow[dr] & \begin{array}{c}\text{application typing}\\ \text{(Lemma 8)}\end{array} \arrow[r] & \begin{array}{c}\text{subject reduction}\\ \text{(Proposition 1)}\end{array} \\
 & & \begin{array}{c}\text{arrow}\\ \text{abstraction typing}\\ \text{(Lemma 10)}\end{array} \arrow[ur] & \\
\begin{array}{c}\boxed{\boxed{\text{cut elimination}}}\\ \text{(Lemma 3)}\end{array} \arrow[r] & \begin{array}{c}\boxed{\begin{array}{c}\text{arrow}\\ \text{subtyping}\end{array}}\\ \text{(Lemma 5)}\end{array} \arrow[ur] & & \\
 & & \begin{array}{c}\boxed{\text{CSR}}\\ \text{(Table 2)}\end{array} \arrow[r] & \begin{array}{c}\text{subject expansion}\\ \text{(Proposition 2)}\end{array}
\end{tikzcd}
$$

Figure 1: Structure of the β subject equality proof

Terms are the usual λ-terms with λ as binder for λ-variables (x, y, ...):

$$t \quad ::= \quad x \mid \lambda x.t \mid t\,t$$

We use the notation $x \notin t$ for x *not free in* t. The *syntactic substitution* of x by u in t is denoted $t\{^u/_x\}$. It makes possible the capture of free variables of the substituting term u by λs of the substituted term t. Except when this syntactic substitution is directly involved (which will occur only in a few places in the paper), we consider λ-terms up to α-conversion of bound variables. We denote the *capture-free substitution* of x by u in t as $t[^u/_x]$.

As examples :

- Both $t\{^x/_x\}$ and $t[^x/_x]$ are always equal to t.
- $t\{^u/_x\}$ and $t[^u/_x]$ coincide if x is not bound in t and the free variables of u are not bound in t.
- $(\lambda y.x)\{^y/_x\}$ is $\lambda y.y$ while $(\lambda y.x)[^y/_x]$ is $\lambda z.y$ and they are not α-equivalent.
- $(\lambda x.\lambda y.x)\{^y/_x\}$ is $\lambda x.\lambda y.y$ while $(\lambda x.\lambda y.x)[^y/_x]$ is $\lambda x.\lambda y.x$ and they are not α-equivalent.

Typing judgments are of the shape $\Gamma \vdash t : A$ where Γ is a finite set of pairs of λ-variables and types $(x : A)$ in which each λ-variable occurs at most once. Concerning the typing rules, we first consider the core intersection type system given by the typing rules of Table 1 and the subtyping rules of Table 2. The (*trans*) rule is written with parentheses since a cornerstone of our approach will be to show that this rule is admissible (Lemmas 3, 13 and 17).

We start with some simple preliminary lemmas which do not depend on the particular choice of subtyping rules.

$$\frac{}{\Gamma, x : A \vdash x : A}\,var \qquad \frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x.t : A \to B}\,lam \qquad \frac{\Gamma \vdash t : A \to B \qquad \Gamma \vdash u : A}{\Gamma \vdash t\,u : B}\,app$$

$$\frac{\Gamma \vdash t : A \qquad \Gamma \vdash t : B}{\Gamma \vdash t : A \cap B}\,\cap \qquad \frac{}{\Gamma \vdash t : \Omega}\,\Omega \qquad \frac{\Gamma \vdash t : A \qquad A \leq B}{\Gamma \vdash t : B}\,\leq$$

Table 1: Typing rules

$$\frac{}{A \leq A}\,id \qquad \left(\frac{A \leq B \qquad B \leq C}{A \leq C}\,trans\right)$$

$$\frac{A \leq C}{A \cap B \leq C}\,\cap_l^1 \qquad \frac{B \leq C}{A \cap B \leq C}\,\cap_l^2 \qquad \frac{C \leq A \qquad C \leq B}{C \leq A \cap B}\,\cap_r \qquad \frac{}{C \leq \Omega}\,\Omega_r$$

Table 2: Core subtyping rules

Lemma 1 (Monotonicity)
If $\Gamma \vdash t : A$, $\Delta \leq \Gamma$ and $A \leq B$ then $\Delta \vdash t : B$ (where $\Delta \leq \Gamma$ means that for each typing declaration $x_i : A_i$ in Γ there is a declaration $x_i : A'_i$ with $A'_i \leq A_i$ in Δ).

Proof. We first prove the case $A = B$ by induction on the derivation of $\Gamma \vdash t : A$. We consider each possible last rule:

(***var***) If $t = x$, let A' be the type of x in Δ, we have $A' \leq A$ and:

$$\frac{\dfrac{}{\Delta \vdash x : A'}\,var \qquad A' \leq A}{\Delta \vdash x : A}\,\leq$$

(***lam***) If $t = \lambda x.t'$ with $A = A' \to A''$ and $\Gamma, x : A' \vdash t' : A''$, by induction hypothesis, we have $\Delta, x : A' \vdash t' : A''$ thus $\Delta \vdash \lambda x.t' : A$.

(***app***) If $t = t'\,t''$ with $\Gamma \vdash t' : A' \to A$ and $\Gamma \vdash t'' : A'$, by induction hypothesis, we have $\Delta \vdash t' : A' \to A$ and $\Delta \vdash t'' : A'$. So that $\Delta \vdash t'\,t'' : A$.

($\cap$) If $A = A' \cap A''$ with $\Gamma \vdash t : A'$ and $\Gamma \vdash t : A''$, by induction hypothesis, we have $\Delta \vdash t : A'$ and $\Delta \vdash t : A''$ thus $\Delta \vdash t : A$.

(Ω) If $A = \Omega$ then $\Delta \vdash t : \Omega$.

($\leq$) If $A' \leq A$ with $\Gamma \vdash t : A'$ then, by induction hypothesis, we have $\Delta \vdash t : A'$ thus $\Delta \vdash t : A$.

We conclude with:

$$\frac{\Delta \vdash t : A \qquad A \leq B}{\Delta \vdash t : B}\,\leq$$

$\square$

Lemma 2 (Non-free variables)
If $x \notin t$ and $\Gamma, x : B \vdash t : A$ then $\Gamma \vdash t : A$.

Proof. By induction on the derivation of $\Gamma, x : B \vdash t : A$. We consider each possible last rule:

(*var*) If $t = y \neq x$ then $y : A \in \Gamma$ and $\Gamma \vdash y : A$.

(*lam*) If $t = \lambda y.t'$ and $A = A' \to A''$ with $\Gamma, x : B, y : A' \vdash t' : A''$ then, by induction hypothesis, $\Gamma, y : A' \vdash t' : A''$ and thus $\Gamma \vdash \lambda y.t' : A$.

(*app*) If $t = t'\,t''$ with $\Gamma, x : B \vdash t' : A' \to A$ and $\Gamma, x : B \vdash t'' : A'$ then, by induction hypothesis, $\Gamma \vdash t' : A' \to A$ and $\Gamma \vdash t'' : A'$ thus $\Gamma \vdash t'\,t'' : A$.

($\cap$) If $A = A' \cap A''$ with $\Gamma, x : B \vdash t : A'$ and $\Gamma, x : B \vdash t : A''$ then, by induction hypothesis, $\Gamma \vdash t : A'$ and $\Gamma \vdash t : A''$ thus $\Gamma \vdash t : A$.

(Ω) We have $\Gamma \vdash t : \Omega$.

($\leq$) If $A' \leq A$ with $\Gamma, x : B \vdash t : A'$ then, by induction hypothesis, $\Gamma \vdash t : A'$ thus $\Gamma \vdash t : A$.

□

1.1 Properties of the core subtyping relation

We turn our attention to the subtyping relation and we take benefits from the presentation we have chosen to prove the cornerstone property of our approach: elimination of the (*trans*) rule. Our particular choice of rules is very natural from a proof-theoretic point of view since they correspond to the $\{\&, \top\}$ fragment of linear logic.

Lemma 3 (Cut elimination)
The (trans) rule is admissible in the core subtyping system without (trans).

Proof. Through a translation $\cap \leftrightarrow \&$ and $\Omega \leftrightarrow \top$, we exactly obtain the $\{\&, \top\}$ fragment of two-sided linear logic for which the cut-elimination property is well known. As a fragment of two-sided additive linear logic, this system has the property that if $\Gamma \vdash \Delta$ is derivable then Γ and Δ contain exactly one formula (see [Mar99] for related results and links with Whitman's work [Whi41] on free lattices).

The more general result given by Lemma 17 is proved in Appendix A. □

In the subtyping system without the (*trans*) rule, the arrow subtyping lemma (Lemma 5) becomes easy to prove. Moreover in the particular case of the subtyping rules used in this section, a proof can be obtained through a simplified property (Lemma 4) which is not valid in the more general cases addressed in the next sections.

Lemma 4 (Trivial arrow subtyping)
If $\bigcap_{i \in I}(A_i \to B_i) \leq A \to B$ then there exists $i \in I$ such that $A = A_i$ and $B_i = B$.

Proof. By induction on a derivation of $\bigcap_{i \in I}(A_i \to B_i) \leq A \to B$ without the (*trans*) rule (Lemma 3). The last rule must be (*id*) or ($\cap_l^k$) ($k \in \{1, 2\}$). The (*id*) case is immediate since $I = \{i\}$, $A = A_i$ and $B = B_i$. In the ($\cap_l^k$) cases, we have $I' \subseteq I$ such that $\bigcap_{i \in I'}(A_i \to B_i) \leq A \to B$ thus, by induction hypothesis, there exists $i \in I' \subseteq I$ such that $A = A_i$ and $B_i = B$. □

Lemma 5 (Arrow subtyping)
If $\bigcap_{i \in I}(A_i \to B_i) \leq A \to B$ *then there exists* $J \subseteq I$ *such that for all* $i \in J$*,* $A \leq A_i$ *and* $\bigcap_{i \in J} B_i \leq B$*.*

Proof. Immediate from Lemma 4 with $J = \{i\} \subseteq I$. □

In the statement of this lemma, J can be empty which means $\Omega \leq B$. It also contains the case I empty which entails that J is also necessarily empty. This last situation gives thus $\Omega \leq A \to B$ entails $\Omega \leq B$.

1.2 Canonical derivations

We now move towards the subject equality proof with some key lemmas. The typing system is not syntax directed as shown by the ($\cap$), (Ω) and ($\leq$) rules. However, by looking at the interaction between the typing rules and the core subtyping rules, it is possible to constrain the shape of derivations under consideration, as given by Definition 1 and Lemma 6.

Definition 1 (Canonical derivation)
The typing rules (*var*), (*lam*) and (*app*) are called the *term rules* (because they modify the term in the judgment). A *type block* is a sub-derivation containing any number (possibly 0) of ($\cap$) rules followed by a ($\leq$) rule.

Informally, a *canonical derivation* is a typing derivation such that the rules between two term rules are a type block and which ends with a type block. More precisely and more formally:

- An (Ω) rule followed by a ($\leq$) rule is a canonical derivation.
- n (*var*) rules followed by a type block (thus containing $n-1$ ($\cap$) rules) give a canonical derivation.
- n canonical derivations, each of which is used in a (*lam*) rule and then gathered through a type block give a canonical derivation.
- $2n$ canonical derivations used by pairs in (*app*) rules and then gathered through a type block give a canonical derivation.

Looking at a canonical derivation in a bottom up way gives a ($\leq$) rule and then either an (Ω) rule or ($\cap$) rules above which one finds a term rule, and then canonical derivations again.

Lemma 6 (Canonical derivation)
If $\Gamma \vdash t : A$ *is derivable, then it is derivable with a canonical derivation.*

Proof. By induction on the derivation of $\Gamma \vdash t : A$. We consider each possible last rule:

(*var*) or (Ω) We add a ($\leq$) rule to the derivation of $\Gamma \vdash t : A$ and we obtain a canonical one:

$$\dfrac{\Gamma \vdash t : A \qquad \dfrac{}{A \leq A}\,id}{\Gamma \vdash t : A}\,\leq$$

(*lam*) If $\Gamma, x : B \vdash u : C$ with $t = \lambda x.u$ and $A = B \to C$, by induction hypothesis we have a canonical derivation of $\Gamma, x : B \vdash u : C$. We turn it into a canonical derivation of $\Gamma \vdash t : A$ by:

$$\cfrac{\cfrac{\Gamma, x : B \vdash u : C}{\Gamma \vdash t : A}\,lam \qquad \cfrac{}{A \leq A}\,id}{\Gamma \vdash t : A}\,\leq$$

(***app***) If $\Gamma \vdash u : B \to A$ and $\Gamma \vdash v : B$ with $t = u\,v$, by induction hypothesis we have a canonical derivation of $\Gamma \vdash u : B \to A$ and a canonical derivation of $\Gamma \vdash v : B$. We turn them into a canonical derivation of $\Gamma \vdash t : A$ by:

$$\cfrac{\cfrac{\Gamma \vdash u : B \to A \qquad \Gamma \vdash v : B}{\Gamma \vdash t : A}\,app \qquad \cfrac{}{A \leq A}\,id}{\Gamma \vdash t : A}\,\leq$$

($\cap$) If $\Gamma \vdash t : B$ and $\Gamma \vdash t : C$ with $A = B \cap C$, by induction hypothesis we have a canonical derivation of $\Gamma \vdash t : B$ and a canonical derivation of $\Gamma \vdash t : C$. By definition they end with a ($\leq$) rule and thus they are of the following shapes:

$$\cfrac{\Gamma \vdash t : B' \qquad B' \leq B}{\Gamma \vdash t : B}\,\leq \qquad \text{and} \qquad \cfrac{\Gamma \vdash t : C' \qquad C' \leq C}{\Gamma \vdash t : C}\,\leq$$

If $\Gamma \vdash t : C'$ is obtained with an (Ω) rule thus $C' = \Omega$ (the case where $\Gamma \vdash t : B'$ is obtained with an (Ω) rule could be treated similarly), we build the following canonical derivation:

$$\cfrac{\Gamma \vdash t : B' \qquad \cfrac{B' \leq B \qquad \cfrac{\cfrac{}{B' \leq \Omega}\,\Omega_r \qquad \Omega \leq C}{B' \leq C}\,trans}{B' \leq B \cap C}\,\cap_r}{\Gamma \vdash t : A}\,\leq$$

If none of $\Gamma \vdash t : B'$ and $\Gamma \vdash t : C'$ is obtained with an (Ω) rule, we build the following canonical derivation:

$$\cfrac{\cfrac{\Gamma \vdash t : B' \qquad \Gamma \vdash t : C'}{\Gamma \vdash t : B' \cap C'}\,\cap \qquad \cfrac{\cfrac{B' \leq B}{B' \cap C' \leq B}\,\cap_l^1 \qquad \cfrac{C' \leq C}{B' \cap C' \leq C}\,\cap_l^2}{B' \cap C' \leq B \cap C}\,\cap_r}{\Gamma \vdash t : A}\,\leq$$

($\leq$) If $\Gamma \vdash t : B$ with $B \leq A$, by induction hypothesis we have a canonical derivation of $\Gamma \vdash t : B$. By definition it ends with a ($\leq$) rule and thus it is of the following shape:

$$\cfrac{\Gamma \vdash t : C \qquad C \leq B}{\Gamma \vdash t : B}\,\leq$$

We obtain a canonical derivation of $\Gamma \vdash t : A$ by:

$$\cfrac{\Gamma \vdash t : C \qquad \cfrac{C \leq B \qquad B \leq A}{C \leq A}\,trans}{\Gamma \vdash t : A}\,\leq$$

$\square$

Relying on canonical derivations and (*trans*)-free subtyping, we see what we can learn about the typing of each of the constructions of the term language (Lemmas 7, 8, 9 and 10) in this typing system which is not syntax directed.

Lemma 7 (Variable typing)
If $\Gamma, x : A \vdash x : B$ *then* $A \leq B$.

Proof. By Lemma 6, we consider a canonical derivation of $\Gamma, x : A \vdash x : B$. Its last rule is a $(\leq)$ rule:

$$\dfrac{\Gamma, x : A \vdash x : B' \qquad B' \leq B}{\Gamma, x : A \vdash x : B} \leq$$

If $B' = \Omega$, then:

$$\dfrac{\dfrac{}{A \leq \Omega}\,\Omega_r \qquad \Omega \leq B}{A \leq B}\, trans$$

Otherwise $B' = \bigcap_{i \in I} B_i$ with for all $i \in I$, $\Gamma, x : A \vdash x : B_i$ and the rules introducing these judgments are (*var*) rules thus $B_i = A$. We conclude:

$$\dfrac{\dfrac{\cdots \qquad \dfrac{i \in I}{A \leq A}\, id \qquad \cdots}{A \leq \bigcap_{i \in I} A}\,\cap_r \qquad \bigcap_{i \in I} A \leq B}{A \leq B}\, trans$$

□

Lemma 8 (Application typing)
If $\Gamma \vdash t\,u : B$, *there exist a set* I *and two families* $(A_i)_{i \in I}$ *and* $(B_i)_{i \in I}$ *such that* $\bigcap_{i \in I} B_i \leq B$ *and for all* $i \in I$, $\Gamma \vdash t : A_i \to B_i$ *and* $\Gamma \vdash u : A_i$.

Proof. According to Lemma 6, we can restrict ourselves to the case of a canonical derivation of $\Gamma \vdash t\,u : B$. Its last rule is a $(\leq)$ rule:

$$\dfrac{\Gamma \vdash t\,u : B' \qquad B' \leq B}{\Gamma \vdash t\,u : B} \leq$$

If $B' = \Omega$, we consider $I = \emptyset$ and we have $\Omega \leq B$. Otherwise, above this last $(\leq)$ rule, we have a (possibly empty) tree of $(\cap)$ rules, and the leaves of this tree are (*app*) rules. This means that, up to associativity of $\cap$, we have a set I with $B' = \bigcap_{i \in I} B_i \leq B$ and for all $i \in I$, $\Gamma \vdash t : A_i \to B_i$ and $\Gamma \vdash u : A_i$. □

Lemma 9 (Abstraction typing)
If $\Gamma \vdash \lambda x.t : A$, *there exist a set* I *and two families* $(A_i)_{i \in I}$ *and* $(B_i)_{i \in I}$ *such that* $\bigcap_{i \in I} A_i \to B_i \leq A$ *and for all* $i \in I$, $\Gamma, x : A_i \vdash t : B_i$.

Proof. According to Lemma 6, we can restrict ourselves to the case of a canonical derivation of $\Gamma \vdash \lambda x.t : A$. It ends with a $(\leq)$ rule:

$$\dfrac{\Gamma \vdash \lambda x.t : A' \qquad A' \leq A}{\Gamma \vdash \lambda x.t : A} \leq$$

If $A' = \Omega$, we have $\Omega \leq A$ and we can choose $I = \emptyset$. Otherwise, above this last $(\leq)$ rule, we have a (possibly empty) tree of $(\cap)$ rules, and the leaves of this tree are (*lam*) rules. This means that, up to associativity of $\cap$, $A' = \bigcap_{i\in I} A_i \to B_i \leq A$ with for all $i \in I$, $\Gamma, x : A_i \vdash t : B_i$. $\square$

Lemma 10 (Arrow abstraction typing)
If $\Gamma \vdash \lambda x.t : A \to B$, there exist a set I and two families $(A_i)_{i\in I}$ and $(B_i)_{i\in I}$ such that $\bigcap_{i\in I} B_i \leq B$ and for all $i \in I$, $A \leq A_i$ and $\Gamma, x : A_i \vdash t : B_i$

Proof. By Lemma 9, we have a set I with $\bigcap_{i\in I} A_i \to B_i \leq A \to B$ and for all $i \in I$, $\Gamma, x : A_i \vdash t : B_i$.
By Lemma 5, we have a subset J of I such that for all $i \in J$, $A \leq A_i$ and $\bigcap_{i\in J} B_i \leq B$. $\square$

1.3 Subject equality

After two substitution lemmas, we will go to subject reduction, subject expansion and subject equality.

Lemma 11 (General substitution)
Assume that $\Gamma \vdash t\{{}^{v}/_{x}\} : A$ and for all Δ and B, $\Gamma, \Delta \vdash v : B$ implies $\Gamma, \Delta \vdash u : B$, then $\Gamma \vdash t\{{}^{u}/_{x}\} : A$.

Proof. By induction on t and then on the derivation of $\Gamma \vdash t\{{}^{v}/_{x}\} : A$. If $t = x$, we have $t\{{}^{v}/_{x}\} = v$ with $\Gamma \vdash v : A$ and we conclude by hypothesis since $t\{{}^{u}/_{x}\} = u$. Otherwise we consider each possible last rule of the derivation of $\Gamma \vdash t\{{}^{v}/_{x}\} : A$:

(***var***) If $t = y \neq x$, we have $t\{{}^{v}/_{x}\} = y = t\{{}^{u}/_{x}\}$.

(***lam***) If $t = \lambda y.t'$ ($y = x$ or $y \neq x$) with $A = A' \to A''$ and $\Gamma, y : A' \vdash t'\{{}^{v}/_{x}\} : A''$ then, by induction hypothesis, $\Gamma, y : A' \vdash t'\{{}^{u}/_{x}\} : A''$ thus $\Gamma \vdash t\{{}^{u}/_{x}\} : A$.

(***app***) If $t = t'\,t''$ with $\Gamma \vdash t'\{{}^{v}/_{x}\} : A' \to A$ and $\Gamma \vdash t''\{{}^{v}/_{x}\} : A'$ then, by induction hypothesis, $\Gamma \vdash t'\{{}^{u}/_{x}\} : A' \to A$ and $\Gamma \vdash t''\{{}^{u}/_{x}\} : A'$ thus $\Gamma \vdash t\{{}^{u}/_{x}\} : A$.

$(\cap)$ If $A = A' \cap A''$ with $\Gamma \vdash t\{{}^{v}/_{x}\} : A'$ and $\Gamma \vdash t\{{}^{v}/_{x}\} : A''$ then, by induction hypothesis, $\Gamma \vdash t\{{}^{u}/_{x}\} : A'$ and $\Gamma \vdash t\{{}^{u}/_{x}\} : A''$ thus $\Gamma \vdash t\{{}^{u}/_{x}\} : A$.

(Ω) We have $\Gamma \vdash t\{{}^{u}/_{x}\} : \Omega$.

$(\leq)$ If $A' \leq A$ with $\Gamma \vdash t\{{}^{v}/_{x}\} : A'$ then, by induction hypothesis, $\Gamma \vdash t\{{}^{u}/_{x}\} : A'$ thus $\Gamma \vdash t\{{}^{u}/_{x}\} : A$.

$\square$

Lemma 12 (Substitution)
If $\Gamma, x : A \vdash t : B$ and $\Gamma \vdash u : A$ with $x \notin u$ then $\Gamma \vdash t[{}^{u}/_{x}] : B$.

Proof. Up to α-conversion in t, we can assume that x is not bound in t and that no free variable of u is bound in t. As a consequence $t[{}^{u}/_{x}] = t\{{}^{u}/_{x}\}$.

We have $\Gamma, x : A \vdash t\{{}^{x}/_{x}\} : B$. If $\Gamma, x : A, \Delta \vdash x : C$ then $A \leq C$ by Lemma 7, and by Lemma 1 we obtain $\Gamma, x : A, \Delta \vdash u : C$. It is thus possible to apply Lemma 11 to deduce $\Gamma, x : A \vdash t\{{}^{u}/_{x}\} : B$. Finally, since $t\{{}^{u}/_{x}\} = t[{}^{u}/_{x}]$ and x is not free in $t[{}^{u}/_{x}]$, we can apply Lemma 2 to conclude $\Gamma \vdash t[{}^{u}/_{x}] : B$. $\square$

Proposition 1 (Subject reduction)
$\Gamma \vdash (\lambda x.t)\, u : A \Longrightarrow \Gamma \vdash t[^u/_x] : A$.

Proof. By Lemma 8, there exists a set I with $\bigcap_{i \in I} A_i \leq A$ and for all $i \in I$, $\Gamma \vdash \lambda x.t : B_i \to A_i$ and $\Gamma \vdash u : B_i$.

If I is empty, we immediately have:

$$\dfrac{\dfrac{}{\Gamma \vdash t[^u/_x] : \Omega}\,\Omega \qquad \Omega \leq A}{\Gamma \vdash t[^u/_x] : A}\,\leq$$

Otherwise, given an $i \in I$, by Lemma 10, there exist a set J_i, $(C^i_j)_{j \in J_i}$ and $(D^i_j)_{j \in J_i}$ such that for all $j \in J_i$, $B_i \leq D^i_j$, $\Gamma, x : D^i_j \vdash t : C^i_j$ and $\bigcap_{j \in J_i} C^i_j \leq A_i$.

- If J_i is empty, we have $\Omega \leq A_i$ thus:

$$\dfrac{\dfrac{}{\Gamma \vdash t[^u/_x] : \Omega}\,\Omega \qquad \Omega \leq A_i}{\Gamma \vdash t[^u/_x] : A_i}\,\leq$$

- If J_i is not empty, for each $j \in J_i$, by Lemma 1, we have $\Gamma, x : B_i \vdash t : C^i_j$. Moreover $\Gamma \vdash u : B_i$, thus by Lemma 12, $\Gamma \vdash t[^u/_x] : C^i_j$. Then we can derive:

$$\dfrac{\dfrac{\cdots \qquad \overset{j \in J_i}{\Gamma \vdash t[^u/_x] : C^i_j} \qquad \cdots}{\Gamma \vdash t[^u/_x] : \bigcap_{j \in J_i} C^i_j}\,\cap \qquad \bigcap_{j \in J_i} C^i_j \leq A_i}{\Gamma \vdash t[^u/_x] : A_i}\,\leq$$

By a sequence of $(\cap)$ rules for $i \in I$, we finally get:

$$\dfrac{\dfrac{\cdots \qquad \overset{i \in I}{\Gamma \vdash t[^u/_x] : A_i} \qquad \cdots}{\Gamma \vdash t[^u/_x] : \bigcap_{i \in I} A_i}\,\cap \qquad \bigcap_{i \in I} A_i \leq A}{\Gamma \vdash t[^u/_x] : A}\,\leq$$

□

Proposition 2 (Subject expansion)
$\Gamma \vdash (\lambda x.t)\, u : A \Longleftarrow \Gamma \vdash t[^u/_x] : A$.

This result is easier than subject reduction. The syntactic proof we give here is a detailed presentation of the sketch presented in [CDCZ87, Corollary 2.7(ii)]. It makes precise the fact that some core rules from Table 2 are required.

Proof. We first prove by induction on the derivation of $\Gamma \vdash t[^u/_x] : A$ that there exists B such that $\Gamma, x : B \vdash t : A$ and $\Gamma \vdash u : B$. If $t = x$ then $t[^u/_x] = u$ and we choose $B = A$. We have $\Gamma, x : A \vdash x : A$ and $\Gamma \vdash u : A$. Otherwise we look at the last rule of the derivation of $\Gamma \vdash t[^u/_x] : A$:

(var) If we have $t = y \neq x$ and $t[^u/_x] = y$. With $B = \Omega$, we get $\Gamma, x : \Omega \vdash y : A$ (because $y : A \in \Gamma$) and $\Gamma \vdash u : \Omega$.

(*lam*) We have $t = \lambda y.t'$, $t[{}^{u}/_{x}] = \lambda y.(t'[{}^{u}/_{x}])$ and $A = A' \to A''$ with $\Gamma, y : A' \vdash t'[{}^{u}/_{x}] : A''$. By induction hypothesis, there exists B such that $\Gamma, x : B, y : A' \vdash t' : A''$ and $\Gamma \vdash u : B$. We then have $\Gamma, x : B \vdash \lambda y.t' : A$ and we conclude.

(*app*) If $t = t'\,t''$ with $\Gamma \vdash t'[{}^{u}/_{x}] : A' \to A$ and $\Gamma \vdash t''[{}^{u}/_{x}] : A'$ then, by induction hypothesis, there exist B' and B'' such that $\Gamma, x : B' \vdash t' : A' \to A$, $\Gamma \vdash u : B'$, $\Gamma, x : B'' \vdash t'' : A'$ and $\Gamma \vdash u : B''$. By Lemma 1, we have $\Gamma, x : B' \cap B'' \vdash t' : A' \to A$ $\left(\text{using } \dfrac{\dfrac{}{B' \leq B'}\,id}{B' \cap B'' \leq B'}\,\cap_l^1\right)$ and $\Gamma, x : B' \cap B'' \vdash t'' : A'$ $\left(\text{using } \dfrac{\dfrac{}{B'' \leq B''}\,id}{B' \cap B'' \leq B''}\,\cap_l^2\right)$ and we can derive:

$$\dfrac{\Gamma, x : B' \cap B'' \vdash t' : A' \to A \qquad \Gamma, x : B' \cap B'' \vdash t'' : A'}{\Gamma, x : B' \cap B'' \vdash t'\,t'' : A}\,app$$

and

$$\dfrac{\Gamma \vdash u : B' \qquad \Gamma \vdash u : B''}{\Gamma \vdash u : B' \cap B''}\,\cap$$

so that we choose $B = B' \cap B''$.

($\cap$) If $A = A' \cap A''$ with $\Gamma \vdash t[{}^{u}/_{x}] : A'$ and $\Gamma \vdash t[{}^{u}/_{x}] : A''$, by induction hypothesis, there exist B' and B'' such that $\Gamma, x : B' \vdash t : A'$, $\Gamma \vdash u : B'$, $\Gamma, x : B'' \vdash t : A''$ and $\Gamma \vdash u : B''$. By Lemma 1, we can build:

$$\dfrac{\Gamma, x : B' \cap B'' \vdash t : A' \qquad \Gamma, x : B' \cap B'' \vdash t : A''}{\Gamma, x : B' \cap B'' \vdash t : A}\,\cap$$

and

$$\dfrac{\Gamma \vdash u : B' \qquad \Gamma \vdash u : B''}{\Gamma \vdash u : B' \cap B''}\,\cap$$

so that we choose $B = B' \cap B''$.

(Ω) If $A = \Omega$, we choose $B = \Omega$ and we have $\dfrac{}{\Gamma, x : \Omega \vdash t : \Omega}\,\Omega$ and $\dfrac{}{\Gamma \vdash u : \Omega}\,\Omega$.

($\leq$) If $A' \leq A$ with $\Gamma \vdash t[{}^{u}/_{x}] : A'$ then, by induction hypothesis, there exists B such that $\Gamma, x : B \vdash t : A'$ and $\Gamma \vdash u : B$. We can derive:

$$\dfrac{\Gamma, x : B \vdash t : A' \qquad A' \leq A}{\Gamma, x : B \vdash t : A}\,\leq$$

We conclude with:

$$\dfrac{\dfrac{\Gamma, x : B \vdash t : A}{\Gamma \vdash \lambda x.t : B \to A}\,lam \qquad \Gamma \vdash u : B}{\Gamma \vdash (\lambda x.t)\,u : A}\,app$$

$$\frac{B \leq A}{A \to C \leq B \to C} \to_l \qquad \frac{C \leq A \to D \qquad D \leq B}{C \leq A \to B} \to_r$$

$$\frac{D \leq C \to A \qquad D \leq C \to B}{D \leq C \to (A \cap B)} \to\cap \qquad \frac{}{B \leq A \to \Omega} \to\Omega$$

Table 3: Additional subtyping rules

□

Theorem 1 (Subject equality)
If $t =_\beta u$ *then* $\Gamma \vdash t : A \iff \Gamma \vdash u : A$.

Proof. By Propositions 1 and 2, and we conclude with Lemma 11. □

A summary of the global structure of the proof of Theorem 1 is given in Figure 1 where CSR means that the subtyping system is required to contain the core subtyping rules of Table 2. The boxed properties are the only ones which depend on the subtyping rules. This shows that Theorem 1 is still valid for any extension of the core subtyping system satisfying Lemma 5 (and a natural way to prove it is Lemma 3). This important remark will be applied in the following sections.

2 Main system

In order to recover a system equivalent to the BCD [BCDC83] typing system, we enrich the $\leq$ relation with the rules of Table 3. The specific choice of rules made here is entirely driven by the cut-elimination property: one should be able to prove the (*trans*) rule to be admissible (Lemma 13), and by relying on (*trans*)-free proofs the arrow subtyping lemma (Lemma 14) should derive immediately.

We want to prove the subject equality property for this system. According to the remark after Theorem 1, we only have to prove the analogue of Lemma 5 and we are going to do so by means of a cut-elimination property (as given in Lemma 3).

Lemma 13 (Cut elimination)
The (trans) rule is admissible in the subtyping system without (trans).

Proof. The more general result given by Lemma 17 is proved in Appendix A. □

Lemma 14 (Arrow subtyping)
If $\bigcap_{i\in I}(A_i \to B_i) \leq A \to B$ *then there exists* $J \subseteq I$ *such that for all* $i \in J$, $A \leq A_i$ *and* $\bigcap_{i\in J} B_i \leq B$.

Proof. We prove the result by induction on a derivation without the (*trans*) rule (Lemma 13). The possible last rules are:

(*id*) We have $J = I = \{i\}$, $A = A_i$ and $B = B_i$.

$(\cap_l^1)$ There exists $I' \subseteq I$ such that $\bigcap_{i\in I'}(A_i \to B_i) \leq A \to B$ and, by induction hypothesis, there exists $J \subseteq I' \subseteq I$ such that for all $i \in J$, $A \leq A_i$ and $\bigcap_{i\in J} B_i \leq B$.

($\cap_l^2$) Idem.

($\to_l$) We have $J = I = \{i\}$, $A \leq A_i$ and $B = B_i$.

($\to_r$) We have $\bigcap_{i\in I}(A_i \to B_i) \leq A \to D$ and $D \leq B$. By induction hypothesis, there exists $J \subseteq I$ such that for all $i \in J$, $A \leq A_i$ and $\bigcap_{i\in J} B_i \leq D$, and we have:

$$\dfrac{\bigcap_{i\in J} B_i \leq D \qquad D \leq B}{\bigcap_{i\in J} B_i \leq B}\, trans$$

($\to\cap$) We have $\bigcap_{i\in I}(A_i \to B_i) \leq A \to B'$ and $\bigcap_{i\in I}(A_i \to B_i) \leq A \to B''$ with $B = B' \cap B''$. By induction hypothesis, there exist $J' \subseteq I$ and $J'' \subseteq I$ such that for all $i \in J'$, $A \leq A_i$ and $\bigcap_{i\in J'} B_i \leq B'$ and for all $i \in J''$, $A \leq A_i$ and $\bigcap_{i\in J''} B_i \leq B''$, we choose $J = J' \cup J'' \subseteq I$ and we get for all $i \in J$, $A \leq A_i$. If both J' and J'' are not empty, we have:

$$\dfrac{\dfrac{\bigcap_{i\in J'} B_i \leq B'}{\bigcap_{i\in J} B_i \leq B'}\,\cap_l \qquad \dfrac{\bigcap_{i\in J''} B_i \leq B''}{\bigcap_{i\in J} B_i \leq B''}\,\cap_l}{\bigcap_{i\in J} B_i \leq B' \cap B''}\,\cap_r$$

If J' is empty but and J'' is not, we have:

$$\dfrac{\dfrac{\dfrac{}{\bigcap_{i\in J''} B_i \leq \Omega}\,\Omega_r \qquad \Omega \leq B'}{\bigcap_{i\in J''} B_i \leq B'}\, trans \qquad \bigcap_{i\in J''} B_i \leq B''}{\bigcap_{i\in J''} B_i \leq B' \cap B''}\,\cap_r$$

with $J'' = J$ (and similarly if J'' is empty but J' is not). Finally if both J' and J'' are empty, then:

$$\dfrac{\Omega \leq B' \qquad \Omega \leq B''}{\Omega \leq B' \cap B''}\,\cap_r$$

($\to\Omega$) We have $B = \Omega$ and thus $J = \emptyset$ and $\Omega \leq B$.

□

Theorem 2 (Subject equality)
If $t =_\beta u$ *then* $\Gamma \vdash t : A \iff \Gamma \vdash u : A$.

Proof. As done for Theorem 1 and as explained in Figure 1 by applying Lemma 14 instead of Lemma 5. □

We have proved the main theorem for the β-equality. In the sequel we will also be interested in η-equality. The system presented here already satisfies the subject reduction property with respect to η-reduction (and this is what we prove in the last part of this section) but the subject expansion property for η is not valid and we will address this point in Section 4.

Proposition 3 (Extensional subject reduction)
If $x \notin t$, $\Gamma \vdash \lambda x.(t\,x) : A \Longrightarrow \Gamma \vdash t : A$.

Proof. By Lemma 9, there exists a set I with $\bigcap_{i \in I} A_i \to B_i \leq A$ and, for all $i \in I$, $\Gamma, x : A_i \vdash t\,x : B_i$. If I is empty, we have $\Omega \leq A$ and:

$$\dfrac{\dfrac{}{\Gamma \vdash t : \Omega}\,\Omega \qquad \Omega \leq A}{\Gamma \vdash t : A}\,\leq$$

Otherwise, for each $i \in I$, by Lemma 8 applied to $\Gamma, x : A_i \vdash t\,x : B_i$, there exists a set J_i with $\bigcap_{j \in J_i} C^i_j \leq B_i$ and for all $j \in J_i$, $\Gamma, x : A_i \vdash t : D^i_j \to C^i_j$ and $\Gamma, x : A_i \vdash x : D^i_j$.

- If J_i is empty then $\Omega \leq B_i$ thus:

$$\dfrac{\dfrac{}{\Gamma \vdash t : \Omega}\,\Omega \qquad \dfrac{\dfrac{}{\Omega \leq A_i \to \Omega}\,\to\Omega \qquad \Omega \leq B_i}{\Omega \leq A_i \to B_i}\,\to_r}{\Gamma \vdash t : A_i \to B_i}\,\leq$$

- If J_i is not empty, then for each $j \in J_i$, by Lemma 2, $\Gamma \vdash t : D^i_j \to C^i_j$ and by Lemma 7, $A_i \leq D^i_j$ thus:

$$\dfrac{\dfrac{\cdots \qquad \dfrac{\dfrac{\begin{matrix} j \in J_i \\ A_i \leq D^i_j \end{matrix}}{D^i_j \to C^i_j \leq A_i \to C^i_j}\,\to_l}{\bigcap_{j \in J_i} D^i_j \to C^i_j \leq A_i \to C^i_j}\,\cap_l \qquad \cdots}{\bigcap_{j \in J_i} D^i_j \to C^i_j \leq A_i \to \bigcap_{j \in J_i} C^i_j}\,\to\cap \qquad \bigcap_{j \in J_i} C^i_j \leq B_i}{\bigcap_{j \in J_i} D^i_j \to C^i_j \leq A_i \to B_i}\,\to_r$$

  and then we have:

$$\dfrac{\dfrac{\cdots \qquad \begin{matrix} j \in J_i \\ \Gamma \vdash t : D^i_j \to C^i_j \end{matrix} \qquad \cdots}{\Gamma \vdash t : \bigcap_{j \in J_i} D^i_j \to C^i_j}\,\cap \qquad \bigcap_{j \in J_i} D^i_j \to C^i_j \leq A_i \to B_i}{\Gamma \vdash t : A_i \to B_i}\,\leq$$

This proves $\Gamma \vdash t : A_i \to B_i$ for each $i \in I$, and we can conclude:

$$\dfrac{\dfrac{\cdots \qquad \begin{matrix} i \in I \\ \Gamma \vdash t : A_i \to B_i \end{matrix} \qquad \cdots}{\Gamma \vdash t : \bigcap_{i \in I}(A_i \to B_i)}\,\cap \qquad \bigcap_{i \in I}(A_i \to B_i) \leq A}{\Gamma \vdash t : A}\,\leq$$

□

$$\frac{}{A \leq A} \qquad \frac{A \leq B \qquad B \leq C}{A \leq C} \qquad \frac{}{A \leq \Omega}$$

$$\frac{}{A \cap B \leq A} \qquad \frac{}{A \cap B \leq B} \qquad \frac{}{A \leq A \cap A} \qquad \frac{A \leq C \qquad B \leq D}{A \cap B \leq C \cap D}$$

Table 4: Core BCD subtyping rules

$$\frac{C \leq A \qquad B \leq D}{A \to B \leq C \to D} \qquad \frac{}{(A \to B) \cap (A \to C) \leq A \to (B \cap C)} \qquad \frac{}{\Omega \leq \Omega \to \Omega}$$

Table 5: Additional BCD subtyping rules

3 Relation with BCD

We are going to show that our system is equivalent to BCD's one [BCDC83]. This gives a "new" proof of the subject equality property of the BCD system.

The BCD typing system is given by the typing rules of Table 1 and by the subtyping relation of Tables 4 and 5.

Lemma 15 (Equivalence of core subtypings)
Our core subtyping system is equivalent to the core BCD subtyping.

Proof. Derivations of BCD rules from ours:

$$\frac{\dfrac{}{A \leq A}\,id}{A \cap B \leq A}\,\cap_l^1 \qquad \frac{\dfrac{}{B \leq B}\,id}{A \cap B \leq B}\,\cap_l^2 \qquad \frac{\dfrac{}{A \leq A}\,id \qquad \dfrac{}{A \leq A}\,id}{A \leq A \cap A}\,\cap_r$$

$$\frac{\dfrac{A \leq C}{A \cap B \leq C}\,\cap_l^1 \qquad \dfrac{B \leq D}{A \cap B \leq D}\,\cap_l^2}{A \cap B \leq C \cap D}\,\cap_r$$

Derivations of our rules from BCD rules:

$$\frac{\dfrac{}{A \cap B \leq A} \qquad A \leq C}{A \cap B \leq C} \qquad \frac{\dfrac{}{A \cap B \leq B} \qquad B \leq C}{A \cap B \leq C}$$

$$\frac{\dfrac{}{C \leq C \cap C} \qquad \dfrac{C \leq A \qquad C \leq B}{C \cap C \leq A \cap B}}{C \leq A \cap B}$$

□

Note that both this lemma and the next one make a strong use of the transitivity of $\leq$ in BCD.

Lemma 16 (Equivalence of subtypings)
Our subtyping system is equivalent to the BCD subtyping.

Proof. We derive the three additional BCD rules from ours:

$$\dfrac{\dfrac{\dfrac{}{A \to B \le A \to B}\,id}{(A \to B) \cap (A \to C) \le A \to B}\,\cap_l^1 \qquad \dfrac{\dfrac{}{A \to C \le A \to C}\,id}{(A \to B) \cap (A \to C) \le A \to C}\,\cap_l^2}{(A \to B) \cap (A \to C) \le A \to (B \cap C)}\,\to\cap$$

and

$$\dfrac{\dfrac{C \le A}{A \to B \le C \to B}\,\to_l \qquad B \le D}{A \to B \le C \to D}\,\to_r \qquad\qquad \dfrac{}{\Omega \le \Omega \to \Omega}\,\to\Omega$$

For the converse:

$$\dfrac{B \le A \qquad \dfrac{}{C \le C}}{A \to C \le B \to C} \qquad\qquad \dfrac{C \le A \to D \qquad \dfrac{\dfrac{}{A \le A} \qquad D \le B}{A \to D \le A \to B}}{C \le A \to B}$$

$$\dfrac{\dfrac{\dfrac{}{D \le D \cap D} \qquad \dfrac{D \le C \to A \qquad D \le C \to B}{D \cap D \le (C \to A) \cap (C \to B)}}{D \le (C \to A) \cap (C \to B)} \qquad \dfrac{}{(C \to A) \cap (C \to B) \le C \to (A \cap B)}}{D \le C \to (A \cap B)}$$

$$\dfrac{\dfrac{\dfrac{}{B \le \Omega} \qquad \dfrac{}{\Omega \le \Omega \to \Omega}}{B \le \Omega \to \Omega} \qquad \dfrac{\dfrac{}{A \le \Omega} \qquad \dfrac{}{\Omega \le \Omega}}{\Omega \to \Omega \le A \to \Omega}}{B \le A \to \Omega}$$

□

As a consequence we obtain the subject equality property for the BCD system:

Proposition 4 (BCD subject equality)
The BCD typing system satisfies: if $t =_\beta u$ *then* $\Gamma \vdash t : A \iff \Gamma \vdash u : A$.

Proof. By Lemmas 15 and 16 and Theorem 2. □

4 Extensionality

In order to get the subject equality property also with respect to the η-equality, we extend once again the $\le$ relation (see Table 6 where X is any variable). This choice of rules answers two requirements: being equivalent with the BCD rules of Table 7 and satisfying the admissibility of the (*trans*) rule (Lemma 17).

The structure of the proof of the subject equality property for the η-reduction is similar to the schema used for Theorems 1 and 2. A summary is given in Figure 2 where FSR means that the subtyping system is required to contain the full subtyping rules of Table 3 and exact ESR means that formulas are exactly the ones considered in this paper and the subtyping relation contains the rules of Tables 2, 3 and 6.

We prove the cut elimination property and the arrow subtyping lemma in the presence of the new rules. The schema given in Figure 1 allows one to conclude that the subject equality property holds for β-reduction with the new subtyping system.

$$
\begin{tikzcd}
& & \text{variable typing (Lemma 7)} \arrow[dr] & \\
\boxed{\text{CSR}}\ \text{(Table 2)} \arrow[r] & \text{canonical derivations (Lemma 6)} \arrow[ur] \arrow[r] \arrow[dr] & \text{application typing (Lemma 8)} \arrow[r] & \eta\ \text{subject reduction (Proposition 3)} \\
& & \text{abstraction typing (Lemma 9)} \arrow[ur] & \\
& & \boxed{\text{FSR}}\ \text{(Table 3)} \arrow[uur] & \\
& \boxed{\text{exact ESR}}\ \text{(Tables 2, 3 and 6)} \arrow[r] & \boxed{\text{intersection arrow}}\ \text{(Lemma 19)} \arrow[dr] & \\
& & & \eta\ \text{subject expansion (Proposition 5)} \\
& & \boxed{\text{CSR}}\ \text{(Table 2)} \arrow[ur] &
\end{tikzcd}
$$

Figure 2: Structure of the η subject equality proof

$$
\frac{}{X \leq A \to X}\, X_l \qquad \frac{A \leq \Omega \to X}{A \leq X}\, X_r
$$

Table 6: Extensionality subtyping rules

Lemma 17 (Cut elimination)
The (trans) rule is admissible in the subtyping system without (trans).

Proof. The proof of this result is given in Appendix A. We decided to put this proof in appendix to stress the idea that it is somehow independent of the rest of the paper and that one may think about it as a result one could delegate to a proof-theorist friend. $\square$

Lemma 18 (Arrow subtyping)
If $\bigcap_{i\in I}(A_i \to B_i) \leq A \to B$ then there exists $J \subseteq I$ such that for all $i \in J$, $A \leq A_i$ and $\bigcap_{i\in J} B_i \leq B$.

Proof. As for Lemma 14, using the fact that $\bigcap_{i\in I}(A_i \to B_i) \leq A \to B$ cannot be conclusion of a (X_l) or of a (X_r) rule. $\square$

In order to prove the subject expansion property with respect to η-reduction, we go through the following key property allowed by the rules of Table 6 and used in [CDCHL84, Theorem 2.6(ii)].

Lemma 19 (Intersection arrow)
For any type A, there exist a non-empty set I and two families $(A_i)_{i\in I}$ and $(B_i)_{i\in I}$ of types such that $A \leq \bigcap_{i\in I} A_i \to B_i$ and $\bigcap_{i\in I} A_i \to B_i \leq A$.

Proof. By induction on the type A:

- If $A = X$, we choose $I = \{i\}$, $A_i = \Omega$ and $B_i = X$. We have:

$$\dfrac{}{X \leq \Omega \to X}\,X_l \qquad\text{and}\qquad \dfrac{\dfrac{}{\Omega \to X \leq \Omega \to X}\,id}{\Omega \to X \leq X}\,X_r$$

- If $A = \Omega$, we choose $I = \{i\}$, $A_i = \Omega$ and $B_i = \Omega$. We have:

$$\dfrac{}{\Omega \leq \Omega \to \Omega}\,{\to}\Omega \qquad\text{and}\qquad \dfrac{}{\Omega \to \Omega \leq \Omega}\,\Omega_r$$

- If $A = A' \to B'$, we choose $I = \{i\}$, $A_i = A'$ and $B_i = B'$.

- If $A = A' \cap A''$, by induction hypothesis, we have I', $(A'_i)_{i\in I'}$, $(B'_i)_{i\in I'}$, I'', $(A''_i)_{i\in I''}$ and $(B''_i)_{i\in I''}$ such that $A' \leq \bigcap_{i\in I'} A'_i \to B'_i$, $\bigcap_{i\in I'} A'_i \to B'_i \leq A'$, $A'' \leq \bigcap_{i\in I''} A''_i \to B''_i$ and $\bigcap_{i\in I''} A''_i \to B''_i \leq A''$. We choose $I = I' \cup I''$ and we have:

$$A' \cap A'' \leq \bigcap_{i\in I'} A'_i \to B'_i \cap \bigcap_{i\in I''} A''_i \to B''_i$$

  and

$$\bigcap_{i\in I'} A'_i \to B'_i \cap \bigcap_{i\in I''} A''_i \to B''_i \leq A' \cap A''$$

  (see Lemma 15 for a derivation of $C_1 \cap C_2 \leq D_1 \cap D_2$ from $C_1 \leq D_1$ and $C_2 \leq D_2$).

$\square$

Proposition 5 (Extensional subject expansion)
If $x \notin t$, $\Gamma \vdash \lambda x.(t\,x) : A \Longleftarrow \Gamma \vdash t : A$.

Proof. By Lemma 19, we have $A \leq \bigcap_{i \in I} A_i \to B_i$ and $\bigcap_{i \in I} A_i \to B_i \leq A$. We prove the result by induction on the size of the non-empty set I.

- If I is a singleton $\{i\}$, we have $A \leq A_i \to B_i$ and $A_i \to B_i \leq A$. By Lemma 1, $\Gamma, x : A_i \vdash t : A$ thus we can derive:

$$\dfrac{\dfrac{\dfrac{\dfrac{\Gamma, x : A_i \vdash t : A \qquad A \leq A_i \to B_i}{\Gamma, x : A_i \vdash t : A_i \to B_i}\leq \qquad \dfrac{}{\Gamma, x : A_i \vdash x : A_i}\mathit{var}}{\Gamma, x : A_i \vdash t\,x : B_i}\mathit{app}}{\Gamma \vdash \lambda x.(t\,x) : A_i \to B_i}\mathit{lam} \qquad A_i \to B_i \leq A}{\Gamma \vdash \lambda x.(t\,x) : A}\leq$$

- If I is not a singleton, we have $I = I' \cup I''$ (with both I' and I'' non-empty), $A \leq \bigcap_{i \in I'} A'_i \to B'_i \cap \bigcap_{i \in I''} A''_i \to B''_i$ and $\bigcap_{i \in I'} A'_i \to B'_i \cap \bigcap_{i \in I''} A''_i \to B''_i \leq A$. We can derive $A \leq \bigcap_{i \in I'} A'_i \to B'_i$ and $A \leq \bigcap_{i \in I''} A''_i \to B''_i$ by:

$$\dfrac{C \leq D \cap E \qquad \dfrac{\dfrac{}{D \leq D}\mathit{id}}{D \cap E \leq D}\cap^1_l}{C \leq D}\mathit{trans} \qquad \text{and} \qquad \dfrac{C \leq D \cap E \qquad \dfrac{\dfrac{}{E \leq E}\mathit{id}}{D \cap E \leq E}\cap^2_l}{C \leq E}\mathit{trans}$$

  and then:

$$\dfrac{\Gamma \vdash t : A \qquad A \leq \bigcap_{i \in I'} A'_i \to B'_i}{\Gamma \vdash t : \bigcap_{i \in I'} A'_i \to B'_i}\leq \qquad \text{and} \qquad \dfrac{\Gamma \vdash t : A \qquad A \leq \bigcap_{i \in I''} A''_i \to B''_i}{\Gamma \vdash t : \bigcap_{i \in I''} A''_i \to B''_i}\leq$$

  thus, by induction hypothesis, $\Gamma \vdash \lambda x.(t\,x) : \bigcap_{i \in I'} A'_i \to B'_i$ and $\Gamma \vdash \lambda x.(t\,x) : \bigcap_{i \in I''} A''_i \to B''_i$, so that:

$$\dfrac{\Gamma \vdash \lambda x.(t\,x) : \bigcap_{i \in I'} A'_i \to B'_i \qquad \Gamma \vdash \lambda x.(t\,x) : \bigcap_{i \in I''} A''_i \to B''_i}{\Gamma \vdash \lambda x.(t\,x) : \bigcap_{i \in I'} A'_i \to B'_i \cap \bigcap_{i \in I''} A''_i \to B''_i}\cap$$

  and $\Gamma \vdash \lambda x.(t\,x) : A$ since $\bigcap_{i \in I'} A'_i \to B'_i \cap \bigcap_{i \in I''} A''_i \to B''_i \leq A$.

□

Theorem 3 (Extensional subject equality)
If $t =_{\beta\eta} u$ *then* $\Gamma \vdash t : A \iff \Gamma \vdash u : A$.

Proof. As before, subject β-equality is a consequence of Lemma 18.
Subject η-reduction is given by Proposition 3 and subject η-expansion by Proposition 5.
We conclude with Lemma 11. □

As done in [RDRP04], once subject equality for β-reduction is known, one can obtain the subject equality for η-reduction by showing that:

$$\Gamma \vdash \lambda x.x : A \iff \Gamma \vdash \lambda x.\lambda y.(x\,y) : A$$

However this would not make the proof much simpler here.

We now prove that our choice of rules in this extensional case are equivalent to usual rules for extensionality in the BCD setting: X equivalent to $\Omega \to X$ (Table 7) [CDCHL84, RDRP04].

$$\frac{}{\Omega \to X \leq X} \qquad \frac{}{X \leq \Omega \to X}$$

Table 7: Extensionality BCD subtyping rules

Lemma 20 (Equivalence of extensional subtypings)
Our extensional subtyping system is equivalent to the BCD one.

Proof. The two rules (X_l) and (X_r) of Table 6 are equivalent (up to the other rules) to the rules of Table 7:

$$\dfrac{\dfrac{}{\Omega \to X \leq \Omega \to X}\,id}{\Omega \to X \leq X}\,X_r \qquad \dfrac{A \leq \Omega \to X \qquad \dfrac{}{\Omega \to X \leq X}}{A \leq X}$$

$$\dfrac{}{X \leq \Omega \to X}\,X_l \qquad \dfrac{\dfrac{}{X \leq \Omega \to X} \qquad \dfrac{\dfrac{}{A \leq \Omega} \qquad \dfrac{}{X \leq X}}{\Omega \to X \leq A \to X}}{X \leq A \to X}$$

□

As with Proposition 4, we can re-prove from these results the $\beta\eta$ subject equality property of the BCD extensional system.

Conclusion

By applying the idea of Figure 1, we have been able to prove the subject equality property with different subtyping relations. The key result is Lemma 5. All the variants of this lemma have been proved by means of a cut-elimination property.

While in Section 1, cut elimination entails the sub-formula property, a major defect of Sections 2 and 4 comes from the violation of the sub-formula property by the rules of Tables 3 and 6. From a proof-theoretical point of view, even if cut elimination allows us to prove Lemma 5 from the subtyping rules (which are precisely designed for this purpose), it would be much nicer and much more natural to go through a sub-formula property. Providing a presentation of the rules of Tables 3 and 6 which ensures cut elimination and the sub-formula property is still an open question.

This kind of questions could be addressed in relation with the proof theory of the relevant logic `B+` which is strongly related with the BCD system [DCGV97].

It would be interesting to see if our approach could also be developed with union types, with other intersection type systems and if it could be applied to the question of principal types.

A Proof of Lemma 17: the (*trans*) rule is admissible

We consider that each rule has size 1 except the (X_l) rule which has size 2. The size $|\pi|$ of a proof π is the sum of the sizes of the rules of π. As a consequence $|\pi|$ is the number of rules of π plus the number of (X_l) rules.

We prove by induction on $|\pi_1|+|\pi_2|$ that if π_1 is a derivation of $A \leq B$ and π_2 is a derivation of $B \leq C$ both without the (*trans*) rule, then there exists a derivation of $A \leq C$ without the (*trans*) rule. We consider each possible last rule for π_2 and in each case we look at the possible last rules for π_1. We then apply a transformation of the proof which allows us to use the induction hypothesis.

A lot of these transformations are very simple commutations of rules. We give here the main cases only. For the interested reader, all the possible cases are listed in the formal proof in Coq (`http://perso.ens-lyon.fr/olivier.laurent/BCDcutel.v`).

$$\dfrac{\dfrac{A \leq D \to E \qquad E \leq C}{A \leq D \to C}\,{\to_r} \qquad \dfrac{B \leq D}{D \to C \leq B \to C}\,{\to_l}}{A \leq B \to C}\,\mathit{trans}$$

$$\downarrow$$

$$\dfrac{\dfrac{A \leq D \to E \qquad \dfrac{B \leq D}{D \to E \leq B \to E}\,{\to_l}}{A \leq B \to E}\,\mathit{trans} \qquad E \leq C}{A \leq B \to C}\,{\to_r}$$

$$\dfrac{\dfrac{D \leq E \to A \qquad D \leq E \to B}{D \leq E \to (A \cap B)}\,{\to\cap} \qquad \dfrac{C \leq E}{E \to (A \cap B) \leq C \to (A \cap B)}\,{\to_l}}{D \leq C \to (A \cap B)}\,\mathit{trans}$$

$$\downarrow$$

$$\dfrac{\dfrac{D \leq E \to A \qquad \dfrac{C \leq E}{E \to A \leq C \to A}\,{\to_l}}{D \leq C \to A}\,\mathit{trans} \qquad \dfrac{D \leq E \to B \qquad \dfrac{C \leq E}{E \to B \leq C \to B}\,{\to_l}}{D \leq C \to B}\,\mathit{trans}}{D \leq C \to (A \cap B)}\,{\to\cap}$$

$$\dfrac{A \leq B \qquad \dfrac{B \leq C \to D \qquad B \leq C \to E}{B \leq C \to (D \cap E)}\,{\to\cap}}{A \leq C \to (D \cap E)}\,\mathit{trans}$$

$$\downarrow$$

$$\dfrac{\dfrac{A \leq B \qquad B \leq C \to D}{A \leq C \to D}\,\mathit{trans} \qquad \dfrac{A \leq B \qquad B \leq C \to E}{A \leq C \to E}\,\mathit{trans}}{A \leq C \to (D \cap E)}\,{\to\cap}$$

$$\dfrac{A \leq B \qquad \dfrac{}{B \leq C \to \Omega}\,{\to\Omega}}{A \leq C \to \Omega}\,\mathit{trans} \qquad \to \qquad \dfrac{}{A \leq C \to \Omega}\,{\to\Omega}$$

$$\dfrac{\dfrac{A \leq \Omega \to X}{A \leq X}\,X_r \qquad \dfrac{}{X \leq B \to X}\,X_l}{A \leq B \to X}\,trans \qquad \to \qquad \dfrac{A \leq \Omega \to X \qquad \dfrac{\dfrac{}{B \leq \Omega}\,\Omega_r}{\Omega \to X \leq B \to X}\to_l}{A \leq B \to X}\,trans$$

$$\dfrac{\dfrac{}{X \leq A \to X}\,X_l \qquad \dfrac{B \leq A}{A \to X \leq B \to X}\to_l}{X \leq B \to X}\,trans \qquad \to \qquad \dfrac{}{X \leq B \to X}\,X_l$$

We then deduce, by induction on the size of a proof π of $A \leq B$ possibly using the (*trans*) rule, that there exists a proof of $A \leq B$ without the (*trans*) rule.

One can check by looking to the proof step by step that if the derivations under consideration only use the rules of Table 2 (resp. of Table 2 and Table 3) then we do not need to use the other rules to get the result, so that one obtains a proof of Lemma 3 (resp. Lemma 13).

References

[BCDC83] Henk Barendregt, Mario Coppo, and Mariangiola Dezani-Ciancaglini. A filter lambda model and the completeness of type assignment. *Journal of Symbolic Logic*, 48:931–940, 1983.

[CDCHL84] Mario Coppo, Mariangiola Dezani-Ciancaglini, Furio Honsell, and Giuseppe Longo. Extended type structures and filter lambda models. In G. Lolli, G. Longo, and A. Marcja, editors, *Logic Colloquium 82*, volume 112 of *Studies in Logic and the Foundations of Mathematics*, pages 241–262. North-Holland, 1984.

[CDCZ87] Mario Coppo, Mariangiola Dezani-Ciancaglini, and Maddalena Zacchi. Type theories, normal forms and d_∞-lambda-models. *Information and Computation*, 72(2):85–116, 1987.

[DCGV97] Mariangiola Dezani-Ciancaglini, Silvia Ghilezan, and Betti Venneri. The "relevance" of intersection and union types. *Notre Dame Journal of Formal Logic*, 38(2):246–269, 1997.

[IK02] Hajime Ishihara and Toshihiko Kurata. Completeness of intersection and union type assignment systems for call-by-value lambda-models. *Theoretical Computer Science*, 272(1–2):197–221, 2002.

[Mar99] Jean-Yves Marion. From multiple sequent for additive linear logic to decision procedures for free lattices. *Theoretical Computer Science*, 224(1–2):157–172, 1999.

[RDRP04] Simona Ronchi Della Rocca and Luca Paolini. *The Parametric Lambda Calculus*. Texts in Theoretical Computer Science. Springer, 2004.

[vB95] Steffen van Bakel. Intersection type assignment systems. *Theoretical Computer Science*, 151(2):385–435, 1995.

[Whi41] Philip Whitman. Free lattices. *Annals of Mathematics*, 42(1):325–330, January 1941.

Acknowledgements

Thanks to Thierry Joly for motivating discussions on the topic of intersection types.
Thanks to Simona Ronchi Della Rocca for her important comments on preliminary versions of this paper.
Thanks to the anonymous referees for their useful pointers to bibliography.

Formal proofs

The interested reader can find a formalization of all the results which concern the subtyping relation only (including the admissibility of the (*trans*) rule) developed in the `Coq` proof system:

- The development: `http://perso.ens-lyon.fr/olivier.laurent/BCDcutel.v`
- The `Coq` proof system: `http://coq.inria.fr/`