Orthogonality and Boolean Algebras for Deduction Modulo

Aloïs Brunel[1], Olivier Hermant[2], and Clément Houtmann[3]

[1] ENS de Lyon, Alois.Brunel@ens-lyon.org
[2] ISEP, Olivier.Hermant@isep.fr
[3] INRIA Saclay, Clement.Houtmann@inria.fr

Abstract. Originating from automated theorem proving, *deduction modulo* removes computational arguments from proofs by interleaving rewriting with the deduction process. From a proof-theoretic point of view, deduction modulo defines a generic notion of cut that applies to any first-order theory presented as a rewrite system. In such a setting, one can prove cut-elimination theorems that apply to many theories, provided they verify some generic criterion. *Pre-Heyting algebras* are a generalization of Heyting algebras which are used by Dowek to provide a semantic intuitionistic criterion called *superconsistency* for generic cut-elimination. This paper uses pre-Boolean algebras (generalizing Boolean algebras) and biorthogonality to prove a generic cut-elimination theorem for the classical sequent calculus modulo. It gives this way a novel application of reducibility candidates techniques, avoiding the use of proof-terms and simplifying the arguments.

1 Introduction

In the usual models of predicate logic (Boolean algebras, Heyting algebras, Kripke models), the interpretations of logically equivalent formulæ are always equal. In particular, valid formulæ are all interpreted by one unique truth value representing truthness. This is adequate for the study of purely logical systems but insufficient for the study of deduction modulo [DHK03]: indeed, in order to remove irrelevant computational arguments from proofs, deduction modulo interleaves rewriting with the deduction process and therefore defines a computational equivalence which is usually strictly weaker than logical equivalence and that appeals to a distinction at the semantical level too. For example, Euclid's algorithm can be specified in deduction modulo: in particular when $a < b$ and $b \bmod a \neq 0$, the gcd of a and b is equal to the gcd of ($b \bmod a$) and a. Propositions "2 *is the gcd of* 4 *and* 6" and "2 *is the gcd of* 2 *and* 4" are then computationally and logically equivalent (because $2 = 6 \bmod 4$). These two propositions are also logically equivalent to Fermat's Last Theorem (all of them are valid), but they are not computationally equivalent to it. Indeed reducing this theorem to a trivial assertion such as "2 *is the gcd of* 4 *and* 6" involves *proving* the theorem. Such a proof hardly qualifies as a *computation*.

Introduced by Dowek [Dow06], *pre-Heyting algebras* are a generalization of Heyting algebras which take into account such a distinction between computational and logical equivalences. Interestingly, they provide a semantic intuitionistic criterion called *superconsistency* for generic cut-elimination in deduction modulo. A theory is superconsistent if it has an interpretation in any pre-Heyting algebra. Since reducibility candidates in deduction modulo [DW03] are a remarkable example of a pre-Heyting algebra, any superconsistent theory can be interpreted in this algebra and consequently verifies the generic notion of cut-elimination provided by deduction modulo. Therefore pre-Heyting algebras are adequate for deduction modulo in intuitionistic logic.

In this paper, we propose a similar notion of model for deduction modulo in *classical logic* that we call *pre-Boolean algebras*. We show that these models lead to a classical version of superconsistency which implies cut-elimination in classical sequent calculus modulo. Our approach significantly differs on two points from the original use of reducibility candidates in deduction modulo [DW03]. First, we do not use original Girard's reducibility candidates [Gir72] or Tait's saturated sets [Tai75], but rather orthogonality which easily adapts to classical sequent calculi: This technique has first been introduced to define reducibility candidates for proofnets and to prove strong normalization of a fragment of linear logic [Gir87] and has since been used many times for various linear logic fragments [Oka99,Gim09] but also for the classical version of system F_ω [LM08] and is the basis of Krivine's classical realizability [Kri09]. Second, we only prove cut-elimination instead of normalization, hence our proof is considerably simplified. Our technique is related to the proofs of cut-elimination for linear logic that use phase semantics [Oka02,Abr91,CT06], but whereas those cut-elimination models can be seen as projections of typed reducibility candidates models [Oka99], ours is crucially designed in a untyped fashion: superconsistency forecloses the degree of freedom to choose the interpretation of atomic formulæ, and the truth values must be forced to contain all the axioms, in order to be able to conclude.

This paper is organized as follows: Deduction modulo, impersonated by a classical sequent calculus, is presented in Section 2. In Section 3, we define pre-Boolean algebras, our generalization of Boolean algebra which acknowledge the distinction between computational and logical equivalences. Section 4 introduces orthogonality for classical deduction modulo using sets of pointed sequents, which allows us to construct a pre-Boolean algebra of sequents and prove adequacy (*i.e.* cut-elimination) in Section 5. Finally in Section 6, we extract a Boolean algebra from the pre-Boolean algebra of sequents presented in Section 5.

2 Classical sequent calculus modulo

We suppose given a signature containing a set of variables $(x, y, z \dots)$, a set of function symbols and a set of predicate symbols. Each function symbol and each predicate symbol has a fixed arity. Terms $(t, u, v \dots)$ and atomic formulæ $(a, b, c \dots)$ are constructed as usual. Formulæ $(A, B, C \dots)$ are constructed from atomic formulæ, negated atomic formulæ ($\bar{a}, \bar{b}, \bar{c} \dots$), conjunctions ($\wedge$), disjunctions ($\vee$), universal quantification ($\forall$) and existential quantification ($\exists$).

$$A, B ::= a \mid \bar{a} \mid \top \mid \bot \mid A \wedge B \mid A \vee B \mid \forall x.A \mid \exists x.A$$

Negation is the involutive function $(.)^\perp$ recursively defined as

$$\begin{array}{lll} a^\perp = \bar{a} & \bot^\perp = \top & (A \wedge B)^\perp = A^\perp \vee B^\perp & (\forall x.A)^\perp = \exists x.A^\perp \\ \bar{a}^\perp = a & \top^\perp = \bot & (A \vee B)^\perp = A^\perp \wedge B^\perp & (\exists x.A)^\perp = \forall x.A^\perp \end{array}$$

Capture avoiding substitutions are denoted $[t/x]$. Sequents are finite multisets of formulæ (denoted $\vdash A_1, A_2 \dots$). If $\equiv$ is a congruence relation on formulæ, the (one-sided) sequent calculus LK modulo $\equiv$ is described in Figure 1.

$$\frac{}{\vdash A, A^\perp}\ (\text{Axiom}) \qquad \frac{\vdash A, \Delta_1 \qquad \vdash A^\perp, \Delta_2}{\vdash \Delta_1, \Delta_2}\ (\text{Cut}) \qquad \frac{\vdash A, \Delta \qquad A \equiv B}{\vdash B, \Delta}\ (\text{Conv})$$

$$\frac{\vdash A, A, \Delta}{\vdash A, \Delta}\ (\text{Contr}) \qquad \frac{\vdash \Delta}{\vdash A, \Delta}\ (\text{Weak}) \qquad \frac{}{\vdash \top}\ (\top) \qquad (\text{no rule for } \bot)$$

$$\frac{\vdash A, \Delta_1 \qquad \vdash B, \Delta_2}{\vdash A \wedge B, \Delta_1, \Delta_2}\ (\wedge) \qquad \frac{\vdash A, B, \Delta}{\vdash A \vee B, \Delta}\ (\vee)$$

$$\frac{\vdash A[t/x], \Delta}{\vdash \exists x.A, \Delta}\ (\exists) \qquad \frac{\vdash A, \Delta \qquad x \text{ fresh in } \Delta}{\vdash \forall x.A, \Delta}\ (\forall)$$

Fig. 1. Sequent calculus LK modulo $\equiv$

3 A generalized semantics

Definition 1 (pre-Boolean algebra). *A pre-Boolean algebra is a structure $\langle \mathcal{B}, \top, \bot, \wedge, \vee, (.)^\perp, \forall, \exists \rangle$ where $\mathcal{B}$ is a set, $\top$ and $\bot$ are elements of $\mathcal{B}$, $\wedge$ and $\vee$ are functions from $\mathcal{B} \times \mathcal{B}$ to $\mathcal{B}$, $(.)^\perp$ is a function from $\mathcal{B}$ to $\mathcal{B}$, and $\forall$ and $\exists$ are (partial) functions from $\wp(\mathcal{B})$ to $\mathcal{B}$. Finally, we require the function $(.)^\perp$ to be involutive.*

A pre-Boolean algebra is said full if $\forall$ and $\exists$ are total functions. It is ordered if it can be equipped with an order relation $\sqsubseteq$ such that $\wedge, \vee, \forall, \exists$ are monotonous, $(.)^\perp$ is antimonotonous. If greatest lower bounds for $\sqsubseteq$ are defined for any $X \subseteq \mathcal{B}$, the pre-Boolean algebra is said complete.

The order relation of the above Definition 1 shall not be confused with the order relation of Boolean algebras. The terminology pre-Boolean algebra has been chosen because it is possible to equip our structure with an additional *pre*-order relation $\leq$ together with axioms on $\leq$ that are a weakening to pre-orders of the definition of a distributive complemented lattice: $\wedge$ and $\vee$ build a[1]

[1] and no more *the*

binary greatest lower bound and *a* least upper bound, respectively, and they obey distributivity laws for the pre-order; $\top$ and $\bot$ are *a* greatest element and *a* least element, respectively; $(.)^\perp$ is a complement operation; $\forall$ and $\exists$ build arbitrary greatest lower bounds and lowest upper bounds, respectively. Of course, when $\leq$ is an order, the notion of pre-Boolean algebras boils down to Boolean algebras.

The presentation of pre-Boolean algebras with a pre-order has the advantage to make a straightforward analogy with Boolean algebras, as Dowek did when generalizing Heyting algebras to pre-Heyting algebras (also known as Truth Values algebras) [Dow06]. Loosening $\leq$ into a pre-order follows the intention to separate computational and logical equivalences: to the first correspond strict equality and to the second the equivalence relation generated by $\leq \cup \geq$. Notice that the pre-order relation is necessary to show that soundness and completeness still hold for this extended notion of model as it is the case for pre-Heyting algebras and intuitionistic natural deduction modulo [Dow06].

Except for the restriction on the involutivity of $(.)^\perp$, this matches exactly the pre-Boolean algebra definition of [Dow10], if we define, as usual, $a \Rightarrow b$ as $a^\perp \vee b$ (conversely, define $a^\perp$ as $a \Rightarrow \bot$).

Since in this paper, the pre-order $\leq$ does not play any role, we chose to get rid of it, just as Cousineau does [Cou09]. Indeed, the main concern is the computational equivalence, and not the logical one.

In doing this, we do not get more structures: any algebra can always be equipped with the trivial pre-order, for which $a \leq b$ whatever a and b are, and all the axioms for $\leq$ are obviously satisfied. In fact, we even have a strictly smaller class of models, by imposing the involutivity of $(.)^\perp$, leading to a potentially larger class of super-consistent theories.

Interpretations in pre-Boolean algebra are partial functions defined as usual. Note that our instances of pre-Boolean algebras ensure the totality of interpretations.

Definition 2 (Interpretation). *Let $\langle \mathcal{B}, \leq, \top, \bot, \wedge, \vee, (.)^\perp, \forall, \exists \rangle$ be a pre-Boolean algebra and $(.)^*$ be a function from n-ary atomic predicates P to functions in $M^n \to \mathcal{B}$ and from n-ary function symbols to functions in $M^n \to M$, for some chosen domain M. Let ϕ be a valuation assigning to each variable a value in M. If C is a formula and t is a term, then their respective interpretations C^*_ϕ and t^*_ϕ are defined inductively as:*

$$f(t_1, \dots, t_n)^*_\phi = f^*((t_1)^*_\phi, \dots, (t_n)^*_\phi) \qquad x^*_\phi = \phi(x)$$
$$P(t_1, \dots, t_n)^*_\phi = P^*((t_1)^*_\phi, \dots, (t_n)^*_\phi)$$

$$(\top)^* = \top \qquad (A \wedge B)^*_\phi = A^*_\phi \wedge B^*_\phi \qquad (\forall x.A)^*_\phi = \forall\{\ (A)^*_{\phi+(d/x)} \mid d \in M\ \}$$
$$(\bot)^* = \bot \qquad (A \vee B)^*_\phi = A^*_\phi \vee B^*_\phi \qquad (\exists x.A)^*_\phi = ((\forall x.(A^\perp))^*_\phi)^\perp$$

where $\phi + (d/x)$ is the valuation assigning d to x and $\phi(y)$ to any $y \neq x$.

Lemma 1 (Substitution). *For any formula A, terms t and u, and valuation ϕ, $(u[t/x])^*_\phi = u^*_{\phi+(t^*_\phi/x)}$ and $(A[t/x])^*_\phi = A^*_{\phi+(t^*_\phi/x)}$.*

Proof. By structural induction on u (resp. A).

Definition 3 (Model interpretation). *Let $\equiv$ be a congruence on terms and formulæ. An interpretation $(.)^*$ is said to be a model interpretation for $\equiv$ if and only if for any valuation ϕ, any terms $t \equiv u$ and formulæ $A \equiv B$, $t^*_\phi = u^*_\phi$ and $A^*_\phi = B^*_\phi$.*

The usual definition of consistency states that a theory is consistent if it can be interpreted in a non-trivial model (*i.e.* where $\bot \neq \top$). In particular, a congruence $\equiv$ is consistent if there exists a model interpretation $(.)^*$ for $\equiv$ in *some non-trivial* model, *i.e.* in some non-trivial pre-Boolean algebra. Such a definition is modified to define *superconsistency* [Dow06] as follows.

Definition 4 (Superconsistency). *A congruence $\equiv$ is superconsistent if* for all *full, ordered and complete pre-Boolean algebra D, an interpretation can be found for $\equiv$ in D.*

4 Behaviours

We dedicate the following sections to a proof that superconsistency is a criterion which entails cut-elimination in our one-sided classical sequent calculus: if $\equiv$ is superconsistent, then cut-elimination holds in LK modulo $\equiv$. To establish such a cut-elimination result, we use orthogonality to design a pre-Boolean algebra of pointed sequents and demonstrate adequacy which in turn implies cut-elimination. The technique used here to prove cut-elimination differs from Dowek and Werner's approach [DW03] because we do not prove strong normalization but cut-elimination (*i.e.* admissibility of the Cut rule) and by the use of orthogonality. However the philosophy remains: in the process of proving cut-elimination, we demonstrate that a pre-Boolean algebra is constructed. Therefore we finally obtain a superconsistency criterion, based on our definition of pre-Boolean algebra, for cut-elimination in our classical sequent calculus modulo.

The notion of orthogonality that we will use in Section 5 relies on sets of *pointed sequents*. These are usual sequents where one formula is distinguished.

Definition 5 (Pointed Sequents). *We define pointed sequents as sequents of the form $\vdash \Delta$ where exactly one formula A of Δ is distinguished*[2]*: a pointed sequent is a pair consisting of a non-empty sequent and a pointer to some specific formula of the sequent. We denote this formula by A°. The set of pointed sequents is the set of sequents of the form $\vdash A^\circ, \Delta$ and is noted P°. The set of usual sequents is the set of sequents of the form $\vdash \Delta$ with no distinguished formula and is noted P. Pointed sequents are represented by letters $t, u, s \ldots$ Moreover, the subset of P° which contains exactly all the sequents whose distinguished formula is A is denoted by $P^\circ(A)$. If $X \subseteq P^\circ$ we pose $X(A) = X \cap P^\circ(A)$.*

[2] In other words, the formula A is in the *stoup*.

Pointed sequents are meant to interact through *cuts*, and therefore define *orthogonality*.

Definition 6 (Cut). *If $t = (\vdash A^\circ, \Delta_1)$ and $u = (\vdash B^\circ, \Delta_2)$ are pointed sequents with $B \equiv A^\perp$, then the sequent $t \star u$ is defined by $t \star u = (\vdash \Delta_1, \Delta_2)$. Obviously $t \star u \in P$. Notice that if $B \not\equiv A^\perp$, $t \star u$ is undefined.*

We denote by Ax the set of all axioms, that is the sequents $\vdash A^\perp, A$ for every A. Ax° is the set of pointed axioms.

Definition 7 (Orthogonal). *In what follows, we pose*

$$\perp\!\!\!\perp = \{ \vdash \Delta \mid \vdash \Delta \text{ has a cut-free proof in LK modulo } \equiv \} .$$

We will write $\perp\!\!\!\perp^\circ$ for the set of pointed sequents which have a cut-free proof. If $X \subseteq P^\circ$, then we define the orthogonal of X as

$$X^\perp = \bigcup_B \{ u \in P^\circ(B) \mid \forall t \in X(C) \text{ with } B \equiv C^\perp, t \star u \in \perp\!\!\!\perp \}$$

Lemma 2. *The usual properties on orthogonality hold:*

$$X \subseteq X^{\perp\perp}, \qquad X \subseteq Y \text{ implies } Y^\perp \subseteq X^\perp, \qquad X^{\perp\perp\perp} = X^\perp .$$

Definition 8 (Behaviour). *A set of sequents X is said to be a behaviour when $X^{\perp\perp} = X$.*

Lemma 3. *Behaviours are always stable by conversion of the distinguished formula through $\equiv$. In other words, if X is a behaviour, if $\vdash A^\circ, \Delta$ is in X and if $A \equiv B$, then $\vdash B^\circ, \Delta$ is in X.*

Proof. Let us prove first that any orthogonal $X^\perp$ is stable by conversion: *if* $(\vdash A^\circ, \Delta) \in X^\perp$ *and* $A \equiv B$, *then* $(\vdash B^\circ, \Delta) \in X^\perp$. Let us assume that $(\vdash C^\circ, \Delta') \in X$ with $C \equiv B^\perp$. Then $C \equiv A^\perp$ (since $B^\perp \equiv A^\perp$) and since $(\vdash A^\circ, \Delta) \in X^\perp$, there exists a cut-free proof of $\vdash \Delta, \Delta'$. We just proved that $(\vdash B^\circ, \Delta) \in X^\perp$.

Now, any behaviour $X = X^{\perp\perp}$ is the orthogonal of $X^\perp$ and therefore is stable by conversion through $\equiv$. □

Lemma 4. *The set of behaviours is closed under unrestricted intersection.*

Proof. If $\mathcal{S}$ is a set of behaviours, then we show that

$$\left(\bigcap_{X \in \mathcal{S}} X \right)^{\perp\perp} \subseteq \bigcap_{X \in \mathcal{S}} X .$$

Let us take an element $t \in (\bigcap \mathcal{S})^{\perp\perp}$. Let X be an element of $\mathcal{S}$. Let $u \in X^\perp$. Because $\bigcap \mathcal{S} \subseteq X$, we have $X^\perp \subseteq (\bigcap \mathcal{S})^\perp$. Hence $u \in (\bigcap \mathcal{S})^\perp$ and so $t \star u \in \perp\!\!\!\perp$. That means $t \in X^{\perp\perp}$, but X is a behaviour, so $t \in X$. This is true for every $X \in \mathcal{S}$ so finally $t \in \bigcap_{X \in \mathcal{S}} X$. □

Definition 9 (Behaviours Operations). *if X and Y are behaviours and $\mathcal{S}$ is a set of behaviours, then $X \wedge Y$ and $\forall \mathcal{S}$ are respectively defined as $X \wedge Y = ((X.Y) \cup Ax^\circ)^{\perp\perp}$ where $X.Y$ is*

$$\{ \vdash (A \wedge B)^\circ, \Delta_A, \Delta_B \mid (\vdash A^\circ, \Delta_A) \in X \text{ and } (\vdash B^\circ, \Delta_B) \in Y \}$$

and

$$\forall \mathcal{S} = (\{ \vdash (\forall x A)^\circ, \Delta \mid \text{ for any } t \in \mathcal{T}, X \in \mathcal{S}, (\vdash (A[t/x])^\circ, \Delta) \in X \} \cup Ax^\circ)^{\perp\perp}$$

where $\mathcal{T}$ is the set of open terms of the language.

By definition and by Lemma 2, $X^\perp$, $X \wedge Y$ and $\forall \mathcal{S}$ are always behaviours.

5 The pre-Boolean algebra of sequents

The next step towards cut-elimination is the construction of a pre-Boolean algebra whose elements are behaviours. The base set of our algebra is

$$D = \{ X \mid Ax^\circ \subseteq X \subseteq \perp\!\!\!\perp^\circ \text{ and } X = X^{\perp\perp} \}$$

Let us construct a pre-Boolean algebra from D using operators $(.)^\perp$, $\wedge$ and $\forall$.

Lemma 5. *If $S \subseteq D$ then $\bigcap S$ is the greatest lower bound of S in D (for the inclusion order $\subseteq$).*

Proof. Since the base set D is closed under unrestricted intersection (Lemma 4), $\bigcap S \in D$. Now if $C \in D$ is a lower bound of S, then $C \subseteq \bigcap S$. Hence $\bigcap S$ is the greatest lower bound of S in D. □

Lemma 6. *For all $X \in D$, $X^\perp \in D$.*

Proof. Let us notice that $(Ax^\circ)^\perp = \perp\!\!\!\perp^\circ$. Then $Ax^\circ \subseteq X \subseteq \perp\!\!\!\perp^\circ$ (since $X \in D$) and Lemma 2 imply $Ax^\circ \subseteq (Ax^\circ)^{\perp\perp} = (\perp\!\!\!\perp^\circ)^\perp \subseteq X^\perp \subseteq (Ax^\circ)^\perp = \perp\!\!\!\perp^\circ$. □

Lemma 7. *If $X, Y \in D$, then for every C, $(\vdash (C^\perp)^\circ, C) \in (X.Y \cup Ax^\circ)^\perp$.*

Proof. We prove equivalently that for all $(\vdash C^\circ, \Delta) \in (X.Y \cup Ax^\circ)$, the sequent $((\vdash (C^\perp)^\circ, C) \star (\vdash C^\circ, \Delta)) = (\vdash C, \Delta)$ has a cut-free proof.

- If $(\vdash C^\circ, \Delta) \in Ax^\circ$, then $\Delta = C^\perp$. Therefore $(\vdash (C^\perp)^\circ, C) \star (\vdash C^\perp, C^\circ) = (\vdash C^\perp, C)$ has obviously a cut-free proof.
- If $(\vdash C^\circ, \Delta) \in X.Y$, then $C = A \wedge B$, $\Delta = \Delta_1, \Delta_2$ and both $\vdash A, \Delta_1$ and $\vdash B, \Delta_2$ have cut-free proofs. By application of the $(\wedge)$ rule, $\vdash A \wedge B, \Delta_1, \Delta_2$ has a cut-free proof. □

Theorem 1. *D is stable under $(.)^\perp$, $\wedge$ and $\forall$.*

Proof. First, Lemma 6 implies stability under $(.)^\perp$.

Let us prove stability under $\wedge$: let us assume $X, Y \in D$ and prove $X \wedge Y \in D$.

– $X \wedge Y$ is a behaviour by definition.
– $Ax^\circ \subseteq X \wedge Y$ since $Ax^\circ \subseteq (X.Y \cup Ax^\circ) \subseteq (X.Y \cup Ax^\circ)^{\perp\perp} = X \wedge Y$.
– Now, let us prove that $X \wedge Y \subseteq \perp\!\!\!\perp^\circ$. We take $(\vdash C^\circ, \Delta) \in X \wedge Y$ and we show that it has a cut-free proof. First, we can notice that $(\vdash (C^\perp)^\circ, C) \in (X.Y \cup Ax^\circ)^\perp$ (Lemma 7). Hence, $(\vdash C^\circ, \Delta) \star (\vdash (C^\perp)^\circ, C) = (\vdash C, \Delta) \in \perp\!\!\!\perp$ and so $(\vdash C, \Delta)$ has a cut-free proof: $(\vdash C^\circ, \Delta) \in \perp\!\!\!\perp^\circ$.

Finally let us prove stability under $\forall$: let us assume that $\mathcal{S}$ is a subset of D and prove that $\forall\mathcal{S} \in D$.

– $\forall\mathcal{S}$ is a behaviour by definition.
– The definition of $\forall\mathcal{S}$ shows that it is the biorthogonal $X^{\perp\perp}$ of a set X containing Ax°. Therefore $Ax^\circ \subseteq X \subseteq X^{\perp\perp} = \forall\mathcal{S}$.
– Finally to prove $\forall\mathcal{S} \subseteq \perp\!\!\!\perp^\circ$, it suffices to show that

$$(\{\ \vdash (\forall x A)^\circ, \Delta \mid \text{ for any } t \in \mathcal{T}, X \in \mathcal{S}, (\vdash (A[t/x])^\circ, \Delta) \in X\ \} \cup Ax^\circ) \subseteq \perp\!\!\!\perp^\circ$$

because $\perp\!\!\!\perp^\circ$ is a behaviour. $Ax^\circ \subseteq \perp\!\!\!\perp^\circ$ obviously. Now, we assume that for any $t \in \mathcal{T}$ and any $X \in \mathcal{S}, (\vdash (D[t/x])^\circ, \Gamma) \in X$. Let us prove that $(\vdash (\forall x.D)^\circ, \Gamma) \in \perp\!\!\!\perp^\circ$. It suffices to take a fresh variable $y \in \mathcal{T}$: then $(\vdash (D[y/x]^\circ, \Gamma))$ is cut-free and by the $\forall$ rule, we obtain that $(\vdash \forall x.D, \Gamma)$ is cut-free too. □

Remark 1. We need to inject the axioms in the construction of the operation $X \wedge Y$, because otherwise, we could not prove the stability of D with respect to this operation. Indeed, to show that $X \wedge Y \in D$ given $X, Y \in D$ we need to prove equivalently that all the sequents in $(X.Y)^\perp$ are cut-free, which is generally not true because $X.Y$ does not contain all the axioms.

Theorem 2. *The structure $\langle D, \leq, \top, \perp, \wedge, \vee, (.)^\perp, \forall, \exists \rangle$, where*

– *$\leq$ be the trivial pre-order on D,*
– *$\top$ is $\perp\!\!\!\perp^\circ$ and $\perp$ is $\perp\!\!\!\perp^{\circ\perp}$,*
– *the operators $\wedge, (.)^\perp, \forall$ are those defined in Definition 9 and 7*
– *and the operators $\vee$ and $\exists$ are the respective boolean dual of $\wedge$ and $\forall$,* i.e. *$X \vee Y = (X^\perp \wedge Y^\perp)^\perp$ and $\exists S = (\forall S^\perp)^\perp$ where $S^\perp = \{\ X^\perp \mid X \in S\ \}$,*

is a pre-Boolean algebra.

Proof. Since we chose a trivial pre-order, there is nothing to check but the stability of D under all the operators, that holds by the above lemmata. □

Remark 2. It should be noted that the pre-Boolean algebra D we have defined is not a monoid when equipped with the operation $\star$ (since when t and u are pointed sequents, $t \star u$ is not a pointed sequent) and so cannot be seen as a classical phase space.

Finally we can state our main result.

Theorem 3 (Adequacy). *Let $\equiv$ be a congruence on terms and formulæ and $(.)^*$ be a model interpretation for $\equiv$ in D. Let $\vdash C_1, ..., C_k$ be a provable sequent in LK modulo $\equiv$, let σ be a substitution whose domain does not contain any bounded variable in $C_1, ..., C_k$, ϕ be a valuation and let $(\vdash (\sigma C_1^\perp)^\circ, \Delta_1) \in ((C_1)^*_\phi)^\perp, \dots, (\vdash (\sigma C_k^\perp)^\circ, \Delta_k) \in ((C_k)^*_\phi)^\perp$. Then $\vdash \Delta_1, ..., \Delta_k \in \perp\!\!\!\perp$.*

Proof. The proof is done by induction on the last rule of the proof of $\vdash C_1, \dots, C_k$.

Axiom For simplicity we suppose that the axiom is performed on C_1 and $C_2 = C_1^\perp$. Therefore $(C_2)^*_\phi = ((C_1)^*_\phi)^\perp$ and since $(\vdash (\sigma C_1^\perp)^\circ, \Delta_1) \in ((C_1)^*_\phi)^\perp = (C_2)^*_\phi$ and $(\vdash (\sigma C_2^\perp)^\circ, \Delta_2) \in ((C_2)^*_\phi)^\perp$, then $\vdash \Delta_1, \Delta_2 \in \perp\!\!\!\perp$.

Conjunction We assume that the derivation is

$$\frac{\vdash A_1, C_2, \dots, C_k \qquad \vdash A_2, C_{k+1}, \dots, C_n}{\vdash \underbrace{A_1 \wedge A_2}_{C_1}, C_2, \dots, C_k, C_{k+1}, \dots, C_n} (\wedge)$$

Let us assume $(\vdash (\sigma C_i^\perp)^\circ, \Delta_i) \in ((C_i)^*_\phi)^\perp$ for all $i > 1$. By induction hypothesis, $\vdash \sigma A_1^\circ, \Delta_2, \dots, \Delta_k$ is in $((A_1)^*_\phi)^{\perp\perp} = (A_1)^*_\phi$ and $\vdash \sigma A_2^\circ, \Delta_{k+1}, \dots, \Delta_n$ is in $((A_2)^*_\phi)^{\perp\perp} = (A_2)^*_\phi$. Therefore $\vdash \sigma C_1^\circ, \Delta_2, \dots, \Delta_n$ is in

$$\begin{aligned}(A_1)^*_\phi.(A_2)^*_\phi \subseteq ((A_1)^*_\phi.(A_2)^*_\phi)^{\perp\perp} &\subseteq ((A_1)^*_\phi.(A_2)^*_\phi \cup Ax^\circ)^{\perp\perp} \\ &= (C_1)^*_\phi = ((C_1)^*_\phi)^{\perp\perp} .\end{aligned}$$

Then $\vdash \Delta_1, \dots, \Delta_n \in \perp\!\!\!\perp$.

Disjunction We assume that the derivation is

$$\frac{\vdash A_1, A_2, C_2, \dots, C_k}{\vdash \underbrace{A_1 \vee A_2}_{C_1}, C_2, \dots, C_k} (\vee)$$

Let us assume that $(\vdash (\sigma C_i^\perp)^\circ, \Delta_i)$ is in $((C_i)^*_\phi)^\perp$ for all $i > 1$ and let us prove that for all $(\vdash (\sigma C_1^\perp)^\circ, \Delta_1) \in ((C_1)^*_\phi)^\perp$, the sequent $\vdash \Delta_1, \dots, \Delta_k$ is in $\perp\!\!\!\perp$. It is equivalent to prove that $\vdash \sigma C_1^\circ, \Delta_2, \dots, \Delta_k$ is in

$$\begin{aligned}((C_1)^*_\phi)^{\perp\perp} &= ((A_1)^*_\phi \vee (A_2)^*_\phi)^{\perp\perp} = (((A_1)^*_\phi)^\perp \wedge ((A_2)^*_\phi)^\perp)^{\perp\perp\perp} \\ &= (((A_1)^*_\phi)^\perp \wedge ((A_2)^*_\phi)^\perp)^\perp = (((A_1)^*_\phi)^\perp.((A_2)^*_\phi)^\perp \cup Ax^\circ)^{\perp\perp\perp} \\ &= (((A_1)^*_\phi)^\perp.((A_2)^*_\phi)^\perp \cup Ax^\circ)^\perp\end{aligned}$$

or equivalently to prove that for all sequent $(\vdash (\sigma C_1^\perp)^\circ, \Delta_1)$ in the set $((A_1)^*_\phi)^\perp.((A_2)^*_\phi)^\perp \cup Ax^\circ$, the sequent $\vdash \Delta_1, \dots, \Delta_k$ is in $\perp\!\!\!\perp$.

- if $(\vdash (\sigma C_1^\perp)^\circ, \Delta_1) \in Ax^\circ$, then $\Delta_1 = \sigma C_1$. Since $\vdash (\sigma A_1^\perp)^\circ, \sigma A_1$ and $\vdash (\sigma A_2^\perp)^\circ, \sigma A_2$ are respectively in $((A_1)^*_\phi)^\perp$ and $((A_2)^*_\phi)^\perp$, then by induction hypothesis, $\vdash \sigma A_1, \sigma A_2, \Delta_2, \dots, \Delta_k \in \perp\!\!\!\perp$. Using $(\vee_R)$,

$$\vdash A_1 \vee A_2, \Delta_2, \dots, \Delta_k \quad = \quad \vdash \Delta_1, \dots, \Delta_k \quad \in \perp\!\!\!\perp .$$

– if $(\vdash (\sigma C_1^\perp)^\circ, \Delta_1) \in ((A_1)^*_\phi)^\perp.((A_2)^*_\phi)^\perp$, then there exist sequents with $\vdash (\sigma A_1^\perp)^\circ, \Delta_a$ and $\vdash (\sigma A_2^\perp)^\circ, \Delta_b$ respectively in $((A_1)^*_\phi)^\perp$ and $((A_2)^*_\phi)^\perp$ such that Δ_1 is Δ_a, Δ_b. Then by induction hypothesis,

$$\vdash \Delta_a, \Delta_b, \Delta_2, \ldots, \Delta_k \quad = \quad \vdash \Delta_1, \Delta_2, \ldots, \Delta_k \quad \in \perp\!\!\!\perp .$$

Universal quantifier We assume that the derivation is

$$\frac{\vdash A, C_2, \ldots, C_k \qquad x \text{ is fresh in each } C_i}{\vdash \underbrace{\forall x.A}_{C_1}, C_2, \ldots, C_k} (\forall)$$

Let us assume that $(\vdash (\sigma C_i^\perp)^\circ, \Delta_i)$ is in $((C_i)^*_\phi)^\perp$ for all $i > 1$ and that the sequent $(\vdash ((\sigma \forall x.A)^\perp)^\circ, \Gamma)$ is in $((\forall x A)^*_\phi)^\perp$. We now want to prove that the sequent $(\vdash \Delta_2, \ldots, \Delta_k, \Gamma)$ is in $\perp\!\!\!\perp$. It is sufficient to prove that the sequent $(\vdash \Delta_2, \ldots, \Delta_k, (\sigma(\forall x.A))^\circ)$ is in $(\forall x.A)^*_\Phi$. By noticing that σ only substitutes variables that are free in $\forall x.A$, we get that $\sigma(\forall x.A) = \forall x.(\sigma A)$. It remains to prove that if $t \in \mathcal{T}$ and $d \in M$, then $(\vdash (\sigma A[t/x])^\circ, \Gamma) \in (A^*_{\phi+[d/x]})$. But, because x is fresh in C_i,

$$(\vdash ((\sigma + [t/x])C_i^\perp)^\circ, \Delta_i) = (\vdash (\sigma C_i^\perp)^\circ, \Delta_i)$$

for each $i > 1$. Again since x is fresh in each C_i, it is easy to see that $((C_i)^*_\phi)^\perp = ((C_i)^*_{\phi+[d/x]})^\perp$ for each $i > 1$. Hence the induction hypothesis applies to $(\sigma + [t/x])$ and $(\phi + [d/x])$. We then know that

$$\vdash \Delta_1, \ldots, \Delta_k, ((\sigma + [t/x])A)^\circ \in A^*_{\phi+[d/x]}$$

which is what we wanted.

Existential quantifier We assume that the derivation is

$$\frac{\vdash A[t/x], C_2, \ldots, C_k}{\vdash \underbrace{\exists x.A}_{C_1}, C_2, \ldots, C_k} (\exists)$$

Let us assume that $(\vdash (\sigma C_i^\perp)^\circ, \Delta_i)$ is in $((C_i)^*_\phi)^\perp$ for all $i > 1$ and that $(\vdash ((\sigma \exists x.A)^\perp)^\circ, \Gamma) \in ((\exists x.A)^*_\phi)^\perp = (\forall x.A^\perp)^*_\phi$. Since x is not in the domain of σ (because x is bounded in $\exists x.A$), and by definition of $(.)^\perp$, we have $(\sigma \exists x.A)^\perp = \forall x.(\sigma A)^\perp$. Hence we know that $(\vdash (\forall x.(\sigma A)^\perp)^\circ, \Gamma) \in \forall\{\ (A^\perp)^*_{\phi+[d/x]} \mid \forall d \in M\ \}$. In particular, we have $(\vdash (\sigma A[t/x])^\perp, \Gamma) \in (A^\perp)^*_{\phi+[t^*_\phi/x]}$. By Lemma 1, $(A^\perp)^*_{\phi+[t^*_\phi/x]} = (A[t/x]^\perp)^*_\phi$, so we can apply the induction hypothesis and finally obtain that $\vdash \Delta_1, \ldots, \Delta_k, \Gamma \in \perp\!\!\!\perp$.

Cut The derivation is

$$\frac{\vdash A, C_1, \ldots, C_p \qquad \vdash A^\perp, C_{p+1}, \ldots, C_k}{\vdash C_1, \ldots, C_k} (\text{Cut})$$

for some $1 \leqslant p \leqslant k$. Let us suppose that $(\vdash (\sigma C_i^\perp)^\circ, \Delta_i)$ is in $((C_i)^*_\phi)^\perp$ for all i. Then by induction hypothesis,

– if $\vdash (\sigma A^{\perp})^{\circ}, \Delta$ is in $(A^*_\phi)^{\perp}$, then $\vdash \Delta, \Delta_1, \ldots, \Delta_p \in \perp\!\!\!\perp$
– and if $\vdash \sigma A^{\circ}, \Delta$ is in A^*_ϕ, then $\vdash \Delta, \Delta_{p+1}, \ldots, \Delta_k \in \perp\!\!\!\perp$.

Therefore $\vdash \sigma A^{\circ}, \Delta_1, \ldots, \Delta_p$ is in A^*_ϕ and $\vdash (\sigma A^{\perp})^{\circ}, \Delta_{p+1}, \ldots, \Delta_k$ is in $(A^{\perp})^*_\phi = (A^*_\phi)^{\perp}$. Then $\vdash \Delta_1, \ldots, \Delta_k, \Gamma_1, \ldots, \Gamma_n \in \perp\!\!\!\perp$.

Weakening We assume that the derivation is

$$\frac{\vdash \quad C_2, \ldots, C_k}{\vdash C_1, C_2 \ldots, C_k}\,(\text{Weak})$$

Let us suppose that $(\vdash (\sigma C_i^{\perp})^{\circ}, \Delta_i)$ is in $((C_i)^*_\phi)^{\perp}$ for all $i > 1$. Then by induction hypothesis, $\vdash \Delta_2, \ldots, \Delta_k \in \perp\!\!\!\perp$. Therefore by weakening in cut-free proofs, $\vdash \Delta_1, \ldots, \Delta_k \in \perp\!\!\!\perp$.

Contraction We assume that the derivation is

$$\frac{\vdash C_1, C_1, \ldots, C_k}{\vdash \quad C_1, \ldots, C_k}\,(\text{Contr})$$

Let us suppose that $(\vdash (\sigma C_i^{\perp})^{\circ}, \Delta_i)$ is in $((C_i)^*_\phi)^{\perp}$ for all $i > 0$. Then by induction hypothesis, $\vdash \Delta_1, \Delta_1, \ldots, \Delta_k \in \perp\!\!\!\perp$. Therefore by contraction in cut-free proofs, $\vdash \Delta_1, \ldots, \Delta_k \in \perp\!\!\!\perp$.

Conversion We assume that the derivation is

$$\frac{\vdash A, C_2, \ldots, C_k \qquad A \equiv C_1}{\vdash C_1, C_2, \ldots, C_k}\,(\equiv)$$

and since $A \equiv C_1$, we know that $A^*_\phi = (C_1)^*_\phi$ and $(A^*_\phi)^{\perp} = ((C_1)^*_\phi)^{\perp}$. Let us suppose that $\vdash (\sigma C_i^{\perp})^{\circ}, \Delta_i$ is in $((C_i)^*_\phi)^{\perp}$ for all $i > 1$. Then since $\sigma C_1^{\perp} \equiv \sigma A^{\perp}$, the sequent $\vdash \sigma A^{\perp}, \Delta$ is also in $((C_i)^*_\phi)^{\perp} = (A^*_\phi)^{\perp}$. Finally by induction hypothesis, $\vdash \Delta_1, \ldots, \Delta_k \in \perp\!\!\!\perp$. □

Cut-elimination is a corollary of our adequacy result.

Corollary 1 (Superconsistency implies cut-elimination). *If $\equiv$ is a superconsistent theory, then cut-elimination holds for LK modulo $\equiv$,* i.e. *any sequent $\vdash \Delta$ derivable in LK modulo $\equiv$ has a cut-free proof in LK modulo $\equiv$.*

Proof. Superconsistency of $\equiv$ implies that there exists a model interpretation $(.)^*$ for $\equiv$ in the pre-Boolean algebra of sequents D (corresponding to $\equiv$). Let $\vdash C_1, \ldots, C_k$ be some provable sequent in LK modulo $\equiv$. Let us remark that $(\vdash (C_i^{\perp})^{\circ}, C_i) \in ((C_i)^*_\phi)^{\perp}$ for each C_i (where ϕ is the empty valuation). Then by our adequacy result (Theorem 3), $(\vdash C_1, \ldots, C_k) \in \perp\!\!\!\perp$. In other words, this sequent has a cut-free proof in LK modulo $\equiv$. □

Remark 3. To prove cut-elimination, we crucially rely on the fact that for each formula A and whatever the model interpretation $(.)^*$ given by the superconsistency is, A^*_ϕ contains all the axioms of the form $\vdash B^{\perp}, B^{\circ}$, including $\vdash A^{\perp}, A^{\circ}$. Otherwise, the interpretation of an atom A which is given by the superconsistency criterion would not necessarily contain all the provable sequents of the form $\vdash \Gamma, A^{\circ}$.

This property does not hold in usual phase semantics based cut-elimination models: in these settings, the elements of A^*_ϕ represent sequents of the form $\vdash \Gamma, A$. Whereas phase semantics cut-elimination models can be seen as projections of typed reducibility candidates models [Oka99], our model can be seen as the projection of a untyped reducibility candidates model.

6 An underlying Boolean algebra

We exhibit a (non-trivial) Boolean algebra, similar but simpler than the one of [DH07], extracted from the pre-Boolean algebra of sequents of section 5.

Definition 10 (Context Extraction). *Let A be a formula, we define $\lfloor A \rfloor$ to be the set of contexts $\Gamma = A_1, \cdots, A_n$ such that for any valuation ϕ, substitution σ, and any sequence of contexts Δ_i such that $\vdash \Delta_i, ((\sigma A_i)^\perp)^\circ \in {(A_i)^*_\phi}^\perp$, $\vdash \Delta_1, \cdots, \Delta_n, (\sigma A)^\circ \in A^*_\phi$.*

Equivalently, one may impose that for any context Δ such that $\vdash \Delta, ((\sigma A)^\perp)^\circ \in {A^*_\phi}^\perp$, we have $\vdash \Delta_1, \cdots, \Delta_n, \Delta \in \perp\!\!\!\perp$.

Definition 11 (Boolean algebra). *We define $\langle \mathcal{B}, \leq, \top, \bot, \wedge, \vee, .^\perp, \forall, \exists \rangle$ as follows. $\mathcal{B}$ is the set containing $\lfloor A \rfloor$ for any A. The order is inclusion, and the operations are*

$$\top = \lfloor \top \rfloor \qquad \lfloor A \rfloor \wedge \lfloor B \rfloor = \lfloor A \wedge B \rfloor \qquad \lfloor A \rfloor^\perp = \lfloor A^\perp \rfloor$$
$$\bot = \lfloor \bot \rfloor \qquad \lfloor A \rfloor \vee \lfloor B \rfloor = \lfloor A \vee B \rfloor$$

$\forall$ and $\exists$ are defined only on sets of the form $\{ \lfloor A[t/x] \rfloor \mid t \in \mathcal{T} \}$, where $\mathcal{T}$ is the set of equivalence classes modulo $\equiv$ of open terms:

$$\forall \{ \lfloor A[t/x] \rfloor \mid t \in \mathcal{T} \} = \lfloor \forall x A \rfloor \qquad \exists \{ \lfloor A[t/x] \rfloor \mid t \in \mathcal{T} \} = \lfloor \exists x A \rfloor$$

Notice that $\lfloor A[t/x] \rfloor$ for $t \in \mathcal{T}$ does not depend of the chosen representative of the equivalence class t since as soon as $t_1 \equiv t_2$, $\lfloor A[t_1/x] \rfloor = \lfloor A[t_2/x] \rfloor$.

Lemma 8. *Let A and B be two formulæ. Then:*

- *$A^\perp \in \lfloor A \rfloor$*
- *if $A_1, ..., A_n \in \lfloor A \rfloor$ then $\vdash A_1, ..., A_n, A$ has a cut-free proof.*
- *$\vdash A^\perp, B$ has a cut-free proof if, and only if, $\lfloor A \rfloor \subseteq \lfloor B \rfloor$*

Proof.

- $\vdash \Delta, (\sigma A)^{\perp\perp\circ} \in {(A^\perp)^*_\phi}^\perp$ and $\vdash \Delta, \sigma A^\circ \in A^*_\phi$ are the same statement.
- $\vdash (A_i^\perp)^\circ, A_i \in {A_i^*}_\phi^\perp$ for each A_i and ϕ. By Definition 10, $\vdash A_1, ..., A_n, A \in \perp\!\!\!\perp$.
- the if part follows from the two previous points: $A^\perp \in \lfloor A \rfloor \subseteq \lfloor B \rfloor$ and therefore $\vdash A^\perp, B$ has a proof. For the only if part, let $A_1, ..., A_n \in \lfloor A \rfloor$, σ be a substitution and ϕ be a valuation. Let Δ_i such that $\vdash \Delta_i, ((\sigma A_i)^\perp)^\circ \in {(A_i)^*_\phi}^\perp$. By hypothesis $\vdash \Delta_1, ..., \Delta_n, (\sigma A)^\circ \in A^*_\phi$, so Theorem 3 applied to the proof of $\vdash A^\perp, B$ implies that $\vdash \Delta_1, ..., \Delta_n, (\sigma B)^\circ \in B^*_\phi$. Therefore $A_1, ..., A_n \in \lfloor B \rfloor$.

Proposition 1. *$\langle \mathcal{B}, \leq, \top, \bot, \wedge, \vee, .^{\bot}, \forall, \exists \rangle$ is a boolean algebra, and $\lfloor . \rfloor$ is a model interpretation in this algebra, where the domain for terms is $\mathcal{T}$.*

Proof. This proposition is a consequence of the adequacy Theorem 3. Let us check the points of Definition 11:

1. $\lfloor A \rfloor \wedge \lfloor B \rfloor$ is the greatest lower bound of $\lfloor A \rfloor$ and $\lfloor B \rfloor$.
   – $\lfloor A \wedge B \rfloor \subseteq \lfloor A \rfloor$: by Lemma 8 since $\vdash (A \wedge B)^{\bot}, A$ has a two-step proof.
   – $\lfloor A \wedge B \rfloor \subseteq \lfloor B \rfloor$: by Lemma 8 since $\vdash (A \wedge B)^{\bot}, B$ has a two-step proof.
   – $\lfloor C \rfloor \subseteq \lfloor A \rfloor$ and $\lfloor C \rfloor \subseteq \lfloor B \rfloor$ implies $\lfloor C \rfloor \subseteq \lfloor A \wedge B \rfloor$: by hypothesis and Lemma 8, $C^{\bot} \in \lfloor C \rfloor \subseteq \lfloor A \rfloor \cap \lfloor B \rfloor$, and we have two proofs of $\vdash C^{\bot}, A$ and $\vdash C^{\bot}, B$. We combine them to form a proof of $\vdash C^{\bot}, A \wedge B$ and conclude by Lemma 8.
2. $\lfloor A \rfloor \vee \lfloor B \rfloor$ is the least upper bound of $\lfloor A \rfloor$ and $\lfloor B \rfloor$.
   – $\lfloor A \rfloor \subseteq \lfloor A \vee B \rfloor$: by Lemma 8 since $\vdash A^{\bot}, A \vee B$ has a two-step proof.
   – $\lfloor B \rfloor \subseteq \lfloor A \vee B \rfloor$: by Lemma 8 since $\vdash B^{\bot}, A \vee B$ has a two-step proof.
   – $\lfloor A \rfloor \subseteq \lfloor C \rfloor$ and $\lfloor B \rfloor \subseteq \lfloor C \rfloor$ implies $\lfloor A \vee B \rfloor \subseteq \lfloor C \rfloor$: by hypothesis and Lemma 8, $A^{\bot} \in \lfloor A \rfloor \subseteq \lfloor C \rfloor$ and $\vdash A^{\bot}, C$ has a proof. By a similar argument $\vdash B^{\bot}, C$ has also a proof. We combine them to form a proof of $\vdash (A \vee B)^{\bot}, C$ and conclude by Lemma 8.
3. properties of greatest and least elements.
   – $\lfloor C \rfloor \subseteq \lfloor \top \rfloor$: by Lemma 8 since $\vdash C^{\bot}, \top$ has a two-step proof.
   – $\lfloor \bot \rfloor \subseteq \lfloor C \rfloor$: by Lemma 8 since $\vdash \bot^{\bot}, C$ has a two-step proof.
4. distributivity of $\wedge$ and $\vee$ follow from the same laws in the logic, through Lemma 8: if two formulæ A and B are equivalent then $\lfloor A \rfloor = \lfloor B \rfloor$.
5. $\lfloor A^{\bot} \rfloor$ is a complement of $\lfloor A \rfloor$.
   – $\lfloor \top \rfloor \subseteq \lfloor A^{\bot} \vee A \rfloor$: by Lemma 8 since $\vdash \top^{\bot}, A^{\bot} \vee A$ has a two-step proof.
   – $\lfloor A^{\bot} \wedge A \rfloor \subseteq \lfloor \bot \rfloor$: by Lemma 8 since $\vdash (A^{\bot} \wedge A)^{\bot}, \bot$ has a two-step proof.
6. idempotency of $(.)^{\bot}$: $\lfloor A \rfloor^{\bot\bot} = \lfloor A^{\bot\bot} \rfloor = \lfloor A \rfloor$.

Lastly, we check that the operators $\forall$ and $\exists$ define a greatest lower bound and a least upper bound, respectively. Notice that although the order is set inclusion, those operators are *not* set intersection and union[3]: $\mathcal{B}$ is neither complete, nor closed under arbitrary union and intersection and it misses many sets.

– $\lfloor \forall x A \rfloor \subseteq \bigcap \{ \lfloor A[t/x] \rfloor \mid t \in \mathcal{T} \}$: by Lemma 8 since for any t, $\vdash (\forall x A)^{\bot}, A[t/x]$ has a one-step proof.
– $\lfloor C \rfloor \subseteq \bigcap \{ \lfloor A[t/x] \rfloor \mid t \in \mathcal{T} \}$ implies $C \subseteq \lfloor \forall x A \rfloor$: assume without loss of generality that x does not appear freely in C. By hypothesis and Lemma 8, $C^{\bot} \in \lfloor C \rfloor \subseteq \bigcap \{ \lfloor A[t/x] \rfloor \mid t \in \mathcal{T} \} \subseteq \lfloor A[x/x] \rfloor$ and $\vdash C^{\bot}, A$ has a proof. Adding a $(\forall)$ rule yields a proof of $\vdash C^{\bot}, \forall x A$. We conclude by Lemma 8.
– $\bigcup \{ \lfloor A[t/x] \rfloor \mid t \in \mathcal{T} \} \subseteq \lfloor \exists x A \rfloor$: by Lemma 8 since for any t, $\vdash A[t/x]^{\bot}, \exists x A$ has a one-step proof.
– $\bigcup \{ \lfloor A[t/x] \rfloor \mid t \in \mathcal{T} \} \subseteq \lfloor C \rfloor$ implies $\lfloor \exists x A \rfloor \subseteq \lfloor C \rfloor$: assume without loss of generality that x does not appear freely in C. By hypothesis and Lemma 8, $A^{\bot} \in \lfloor A[x/x] \rfloor \subseteq C$ and $\vdash A^{\bot}, C$ has a proof. Adding a $(\forall)$ rule yields a proof of $\vdash (\exists x A)^{\bot}, C$. We conclude by Lemma 8.

[3] so, for instance, the greatest lower bound is allowed to be smaller than set intersection

Definition 10 ensures that $\lfloor . \rfloor$ is an interpretation (Definition 2), provided that terms are interpreted by their equivalence class modulo $\equiv$. Lastly, if $A \equiv B$ then they are logically equivalent and by Lemma 8 $\lfloor A \rfloor = \lfloor B \rfloor$.

A direct proof of Proposition 1, bypassing Theorem 3, is possible. In this option, each of its case uses the same arguments than the corresponding case of Theorem 3. Such a proof would be made easier by considering the definition of [Dow10] for pre-Boolean algebra where one has conditions on $\Rightarrow$ rather than distributivity laws.

The benefits of a direct proof would be an alternative proof of the cut-elimination theorem, as it is done in [DH07], through the usual soundness theorem with respect to Boolean Algebras and strong completeness with respect to the particular Boolean Algebra we presented here.

7 Conclusion

We have generalized Boolean algebras into pre-Boolean algebras, a notion of model for classical logic which acknowledges the distinction between computational and logical equivalences. We also have demonstrated how superconsistency —a semantic criterion for generic cut-elimination in (intuitionistic) deduction modulo— adapts to classical logic: We have proposed a classical version of superconsistency based on pre-Boolean algebras. Using orthogonality, we have constructed a pre-Boolean algebra of sequents which allows to prove that our classical superconsistency criterion implies cut-elimination in classical sequent calculus modulo. In the last section, we have explained how a non-trivial Boolean algebra of contexts can be extracted from the pre-Boolean algebra of sequents, therefore relating our orthogonality cut-elimination proof with the usual semantics of classical logic (*i.e.* Boolean algebras). Finally we have proved that the same cut-elimination result can be obtained from this particular Boolean algebra, without going through the proof of adequacy for the pre-Boolean algebra.

Let us notice that any pre-Boolean algebra is also a pre-Heyting algebra. Therefore a theory which is superconsistent on pre-Heyting algebras is automatically superconsistent on pre-Boolean algebras. (The converse does not hold in general and pre-Heyting algebras are not always pre-Boolean algebras.) Dowek has proved [Dow06] that several theories of interest are superconsistent on pre-Heyting algebras: arithmetic, simple type theory, the theories defined by a confluent, terminating and quantifier free rewrite system, the theories defined by a confluent, terminating and positive rewrite system and the theories defined by a positive rewrite system such that each atomic formula has at most one one-step reduct. We automatically obtain that these theories are also superconsistent on pre-Boolean algebras, and therefore that cut-elimination holds in classical sequent calculus modulo these theories.

Using pre-Boolean algebras is not the unique way of connecting the superconsistency criterion with classical logic. For instance, one can use double-negation translations and prove that superconsistency (on pre-Heyting algebras) of a theory implies superconsistency (still on pre-Heyting algebras) of its double-negation translation which in turn implies cut-elimination in classical logic, using [DW03]. Superconsistency of double-negated theories on pre-Heyting algebras and superconsistency on pre-Boolean algebras remain to be compared. Both are implied by superconsistency on pre-Heyting algebras, and in both cases, no counterexample of the inverse has been found yet.

References

[Abr91] V.M. Abrusci. Phase semantics and sequent calculus for pure noncommutative classical linear propositional logic. *Journal of Symbolic Logic*, 56(4):1403–1451, 1991.

[Cou09] Denis Cousineau. Complete reducibility candidates. In *PSTT09*, 2009.

[CT06] A. Ciabattoni and K. Terui. Towards a semantic characterization of cut-elimination. *Studia Logica*, 82(1):95–119, 2006.

[DH07] Gilles Dowek and Olivier Hermant. A simple proof that super-consistency implies cut elimination. In *RTA*, pages 93–106, 2007.

[DHK03] Gilles Dowek, Thérèse Hardin, and Claude Kirchner. Theorem proving modulo. *Journal of Automated Reasoning*, 31(1):33–72, Nov 2003.

[Dow06] Gilles Dowek. Truth values algebras and proof normalization. In *TYPES*, pages 110–124, 2006.

[Dow10] Gilles Dowek. Fondements des systèmes de preuve. Course notes, 2010.

[DW03] Gilles Dowek and Benjamin Werner. Proof normalization modulo. *Journal of Symbolic Logic*, 68(4):1289–1316, 2003.

[Gim09] Stéphane Gimenez. *Programmer, Calculer et Raisonner avec les Réseaux de la Logique Linéaire*. PhD thesis, Université Paris 7, 2009.

[Gir72] Jean-Yves Girard. *Interprétation Fonctionnelle et Élimination des Coupures de l'Arithmétique dOrdre Supérieur*. PhD thesis, Université Paris 7, 1972.

[Gir87] Jean-Yves Girard. Linear logic. *Theor. Comput. Sci.*, 50:1–102, 1987.

[Kri09] Jean-Louis Krivine. Realizability in classical logic. *Panoramas et synthèses*, 27:197–229, 2009.

[LM08] S. Lengrand and A. Miquel. Classical F [omega], orthogonality and symmetric candidates. *Annals of Pure and Applied Logic*, 153(1-3):3–20, 2008.

[Oka99] M. Okada. Phase semantic cut-elimination and normalization proofs of first- and higher-order linear logic. *Theoretical Computer Science*, 227(1-2):333–396, 1999.

[Oka02] M. Okada. A uniform semantic proof for cut-elimination and completeness of various first and higher order logics. *Theoretical Computer Science*, 281(1-2):471–498, 2002.

[Tai75] W.W. Tait. A realizability interpretation of the theory of species. In R.J. Parikh, editor, *Logic Colloquium*, pages 240–251. Springer, 1975.