Normalisation by Completeness with Heyting Algebras

Gaëtan Gilbert[1,2] and Olivier Hermant[3]

[1] ENS Lyon, France
gaetan.gilbert@ens-lyon.fr
[2] Inria Paris, France
[3] MINES ParisTech, PSL Research University, France
olivier.hermant@mines-paristech.fr

1 Introduction

In logic, a restriction to cut-free proofs makes analysis of a theory and proof search significantly simpler.
On the programming side, β reduction allows computation. Then normalisation of β reduction provides termination of the program and allows the production of a result.

Under the Curry Howard correspondence, a proof in natural deduction is cut-free when the associated term is normal.

Normalisation by Evaluation uses features of the meta level, like reduction when the meta level is a programming language, to compute on syntactic objects. Berger and Schwichtenberg used this method to define an efficient normalisation algorithm for λ calculus [2], and Altenkirch, Dybjer, Hofmann and Scott extended it to λ calculus with strong sums [1]. Coquand noted the similarity to completeness proofs [3].

Hugo Herbelin and his students then developed this principle of strong completeness.
The logical systems considered are syntactic systems, like natural deduction NJ, and are also associated with semantic systems like Boole algebras. Syntax and semantics are linked by soundness theorems, taking derivations in the former to valid statements in the later, and completeness, making derivations from valid statements.
Completeness can be enhanced so as to obtain a theorem of cut admissibility, and therefore cut elimination. Additionally, if all theorems are constructive then a cut elimination theorem can be extracted.
This extraction work has been accomplished by Herbelin in [4] using Kripke structures for semantics and extracting the algorithm from a formalisation of the proof in the Coq proof assistant.

Based on work by Hermant [5] itself inspired by Okada's contributions to linear logic [6], we know that Heyting algebras provide another sound and complete semantics to natural logic.
If the proof is constructive, the extracted normalisation algorithm should be compared with that from Kripke based normalisation by evaluation, regarding their complexities and the values they produce.

In this manuscript we begin to answer these questions by developing a Coq formalisation of the soundness and strong completeness proofs with Heyting algebras allowing algorithm extraction and testing. Additionally we study the links between Heyting algebras and Kripke structures to try to link the Heyting based algorithms with the Kripke based algorithms.

In the first section we recall definitions and basic lemmas about natural deduction and cut-free proofs.
In the second, we study the strong completeness of Heyting algebras.
In the third we recall basic properties of Kripke structures.
In the fourth we develop a transformations between Heyting algebras and Kripke structures.

The Coq sources are available at `https://github.com/SkySkimmer/NormalisationByCompleteness`.

2 Natural deduction

In this section, we recall the basic definitions and lemmas of natural deduction.

Definition 1 (Terms and formulas). *Let $\mathcal{V}$ infinite set of variables and $\mathcal{S}$ a set of function symbols. The set of terms $\mathcal{T}$ is defined by*

$$t ::= x | f(t_1 ... t_n)$$

for $x \in \mathcal{V}$ and $f \in \mathcal{S}$ with arity n.
Let $\mathcal{P}$ set of predicate symbols. Formulas $\mathcal{F}$ are defined by

$$A ::= P(t_1 ... t_n) \mid A \wedge B \mid A \vee B \mid A \Rightarrow B \mid \top \mid \bot \mid \forall x.A \mid \exists x.A$$

where $P \in \mathcal{P}$ with arity n.

At the time of this writing the Coq development is for the propositional fragment, i.e. $A ::= P \mid A \wedge B \mid A \vee B \mid A \Rightarrow B \mid \top \mid \bot$.

Remark 1. Formulas are considered modulo α-conversion.

Definition 2 (Substitutions). *A substitution is a partial function σ from variables to terms.*
We expand it inductively to a function from terms to terms and formulas to formulas, taking $\sigma(x) = x$ for x not in the domain of σ.
Notably for $Q \in \{\forall, \exists\}, \sigma(Q\ x.A) \coloneqq Q\ x.\sigma(A)$, assuming x fresh w.r.t. the image of σ by α-conversion. This is always possible since $dom(\sigma)$ is finite, and so the image of σ is also finite.

Definition 3 (Updated substitution). *For σ substitution, $x \in \mathcal{V} \backslash dom(\sigma)$ and $t \in \mathcal{T}$, $\sigma[x \mapsto t]$ is the substitution with domain $dom(\sigma) \cup \{x\}$ such that $\forall y \in dom(\sigma), \sigma[x \mapsto t](y) = \sigma(y)$ and $\sigma[x \mapsto t](x) = t$.*

Definition 4 (Empty substitution and single variable substitution). *The empty substitution $\emptyset$ is the substitution with the empty set as domain.*
For t term (resp. A formula), for x variable and u term, we define $t[u/x] \coloneqq \emptyset[x \mapsto u](t)$ (resp. $A[t/x] \coloneqq \emptyset[x \mapsto u](A)$).

Definition 5 (Context). *A context Γ is a list of formulas: $\Gamma = [A_1, ..., A_n], n \geq 0$.*
For $\Gamma = [A_1, ..., A_n]$ context and A formula, $\Gamma, A \coloneqq [A_1, ..., A_n, A]$.
For $\Gamma = [A_1, ..., A_n]$ context and B formula, we let $B \in \Gamma$ if and only if B is one of the A_i for some i. Then we can define a binary relation on contexts $\subseteq$ such that $\Gamma \subseteq \Sigma$ when any formula in Γ is also in Σ.

Remark 2. The $\subseteq$ relation is more general than the notion of contraction: $\Gamma, A, A \subseteq \Gamma, A$.
This also shows that while it is a preorder, it is not an order.

Definition 6 (Cut free proofs). *The following figure 1 defines the rules of natural deduction as well as relations $\vdash_{ne}$ (neutral proof) and $\vdash^*$ (cut-free proof) by mutual induction. Rules on the left are introduction rules which produce cut-free proofs, while rules on the right are elimination rules and produce neutral proofs.*

Definition 7 (Natural deduction NJ). *The judgement $\Gamma \vdash A$ has the same rules as both $\Gamma \vdash^* A$ and $\Gamma \vdash_{ne} A$.*
Then trivially if $\Gamma \vdash^* A$ then $\Gamma \vdash A$ and if $\Gamma \vdash_{ne} A$ then $\Gamma \vdash A$.

Lemma 1 (Weakening). *For Γ context and A formula, if $\Gamma \vdash^* A$ (resp. $\Gamma \vdash_{ne} A$, resp. $\Gamma \vdash A$) is derivable, then for any Σ context with $\Gamma \subseteq \Sigma$, $\Sigma \vdash^* A$ (resp. $\Sigma \vdash_{ne} A$, resp. $\Sigma \vdash A$) is derivable.*

Fig. 1. Rules of Natural Deduction

$$\frac{\Gamma \vdash_{ne} A}{\Gamma \vdash^{*} A}\ coerce \qquad \frac{A \in \Gamma}{\Gamma \vdash_{ne} A}\ ax$$

$$\frac{\Gamma \vdash^{*} A \qquad \Gamma \vdash^{*} B}{\Gamma \vdash^{*} A \wedge B}\ \wedge_I \qquad \frac{\Gamma \vdash_{ne} A \wedge B}{\Gamma \vdash_{ne} A}\ \wedge_{E_l} \qquad \frac{\Gamma \vdash_{ne} A \wedge B}{\Gamma \vdash_{ne} B}\ \wedge_{E_r}$$

$$\frac{\Gamma \vdash^{*} A}{\Gamma \vdash^{*} A \vee B}\ \vee_{I_l} \quad \frac{\Gamma \vdash^{*} B}{\Gamma \vdash^{*} A \vee B}\ \vee_{I_r} \qquad \frac{\Gamma \vdash_{ne} A \vee B \qquad A, \Gamma \vdash^{*} C \qquad B, \Gamma \vdash^{*} C}{\Gamma \vdash_{ne} C}\ \vee_E$$

$$\frac{\Gamma, A \vdash^{*} B}{\Gamma \vdash^{*} A \Rightarrow B}\ \Rightarrow_I \qquad \frac{\Gamma \vdash_{ne} A \Rightarrow B \qquad \Gamma \vdash^{*} A}{\Gamma \vdash_{ne} B}\ \Rightarrow_E$$

$$\frac{}{\Gamma \vdash^{*} \top}\ \top_I \qquad \frac{\Gamma \vdash_{ne} \bot}{\Gamma \vdash_{ne} A}\ \bot_E$$

$$\frac{\Gamma \vdash^{*} A \qquad x \notin FV(\Gamma)}{\Gamma \vdash^{*} \forall x.A}\ \forall_I \qquad \frac{\Gamma \vdash_{ne} \forall x.A}{\Gamma \vdash_{ne} A[t/x]}\ \forall_E$$

$$\frac{\Gamma \vdash^{*} A[t/x]}{\Gamma \vdash^{*} \exists x.A}\ \exists_I \qquad \frac{\Gamma \vdash_{ne} \exists x.A \qquad A, \Gamma \vdash^{*} C \qquad x \notin FV(C, \Gamma)}{\Gamma \vdash_{ne} C}\ \exists_E$$

Proof. By mutual induction on the derivation of $\Gamma \vdash^{*} A$ and $\Gamma \vdash_{ne} A$ (resp. by induction on $\Gamma \vdash A$).

Remark 3. Since the notion of contraction of a context is included in the $\subseteq$ relation, the weakening lemma can also be used as a contraction lemma.

Neutral proofs are such that they can replace axioms in cut-free proofs without introducing cuts.

Lemma 2 (Axiom replacement). *Let Γ and Σ contexts, if for each formula $C \in \Gamma$ we can derive $\Sigma \vdash_{ne} C$ ($\Sigma \vdash C$ if we admit cuts),*
Then for any A formula, if $\Gamma \vdash^{*} A$ (resp. $\Gamma \vdash_{ne} A$, resp. $\Gamma \vdash A$) we can derive $\Sigma \vdash^{*} A$ (resp. $\Sigma \vdash_{ne} A$, resp. $\Sigma \vdash A$).

Proof. By mutual induction on $\Gamma \vdash^{*} A$ and $\Gamma \vdash_{ne} A$ (resp. by induction on $\Gamma \vdash A$). We need the weakening lemma when the context is modified in a premise of a rule.

Lemma 3 (Kleene's inversion lemma). *Let Γ context, A and B formulas.*
If $\Gamma \vdash_{ne} A \Rightarrow B$ then $\Gamma, A \vdash_{ne} B$.
If $\Gamma \vdash^{*} A \Rightarrow B$ then $\Gamma, A \vdash^{*} B$.

Proof. If $\Gamma \vdash_{ne} A \Rightarrow B$, by weakening $\Gamma, A \vdash_{ne} A \Rightarrow B$ and $\Gamma, A \vdash^{*} A$ by axiom and coercion. then $\Gamma, A \vdash_{ne} B$ by $\Rightarrow_E$.

If $\Gamma \vdash^* A \Rightarrow B$, the final rule may be the coercion, in which case we have $\Gamma \vdash_{ne} A \Rightarrow B$ then $\Gamma, A \vdash_{ne} B$ and by coercion $\Gamma, A \vdash^* B$, otherwise it is the $\Rightarrow_I$ rule with premise $\Gamma, A \vdash^* B$.

3 Strong completeness by Heyting algebras

3.1 Heyting algebra

Definition 8 (Complete lattice). *A complete lattice is a tuple*

$$\mathcal{A} = (A, \leq, \wedge, \vee, \top, \bot, \bigwedge, \bigvee)$$

such that $(A, \leq)$ is a partial order with binary meet $\wedge$ and join $\vee$, arbitrary meet $\bigwedge$ and join $\bigvee$ and global maximum $\top$ and minimum $\bot$.

Definition 9 (Heyting algebra). *A Heyting algebra is a structure $\mathcal{H} = (H, \leq, \wedge, \vee, \Rightarrow, \top, \bot, \bigwedge, \bigvee)$ such that $(H, \leq, \wedge, \vee, \top, \bot, \bigwedge, \bigvee)$ is a complete lattice and verifies the implication property*

$$\forall a\ b\ c, a \leq b \Rightarrow c \text{ if and only if } a \wedge b \leq c$$

When working with propositional logic we forget $\bigwedge$ and $\bigvee$ and the conditions involving them.

Lemma 4. *In a Heyting algebra, binary meet and join distribute over each other.*

Proof. Let $a, b, c \in H$

- $a \wedge (b \vee c) \leq (a \wedge b) \vee (a \wedge c)$:
  $a \wedge b \leq (a \wedge b) \vee (a \wedge c)$ and $a \wedge c \leq (a \wedge b) \vee (a \wedge c)$.
  By the implication property, $b \leq a \Rightarrow ((a \wedge b) \vee (a \wedge c))$ and $c \leq a \Rightarrow ((a \wedge b) \vee (a \wedge c))$.
  Then $b \vee c \leq a \Rightarrow ((a \wedge b) \vee (a \wedge c))$ and we conclude by the implication property.
- $(a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c)$: true in all lattices
- $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$: true in all lattices
- $(a \vee b) \wedge (a \vee c) \leq a \vee (b \wedge c)$:
  By the implication property, equivalent to $a \vee b \leq (a \vee c) \Rightarrow (a \vee (b \wedge c))$
  $\iff a \leq (a \vee c) \Rightarrow (a \vee (b \wedge c))$ and $b \leq (a \vee c) \Rightarrow (a \vee (b \wedge c))$
  $\iff a \wedge (a \vee c) \leq a \vee (b \wedge c)$ (true) and $b \wedge (a \vee c) \leq a \vee (b \wedge c)$
  $\iff a \vee c \leq b \Rightarrow (a \vee (b \wedge c))$
  $\iff a \leq b \Rightarrow (a \vee (b \wedge c))$ and $c \leq b \Rightarrow (a \vee (b \wedge c))$
  $\iff a \wedge b \leq a \vee (b \wedge c)$ (true) and $c \wedge b \leq a \vee (b \wedge c)$ (true)

3.2 Interpretations and soundness

Definition 10 (Interpretation of a formula for propositional logic). *An interpretation in a Heyting algebra $\mathcal{H}$ is a function $[\![\_]\!]$ from atomic formulas to elements of $\mathcal{H}$, which is extended to propositional formulas in the natural way.*
If Γ is a context, we let $[\![\Gamma]\!] \coloneqq \bigwedge_{A\in\Gamma}[\![A]\!]$.
$[\![\Gamma]\!] = [\![\bigwedge_{A\in\Gamma} A]\!]$ by definition of $[\![\_]\!]$.

Theorem 1 (Soundness of Heyting algebras for propositional logic). *For Γ context and A formula, if $\Gamma \vdash A$ is derivable then for any Heyting algebra $\mathcal{H}$ and interpretation $[\![\_]\!]$,*

$$[\![\Gamma]\!] \leq [\![A]\!]$$

Proof. Trivial by induction on the derivation of $\Gamma \vdash A$.

Definition 11 (Interpretation of a first order formula). *A first order model on a Heyting algebra $\mathcal{H}$ is a set $\mathcal{D}$ called domain, with for each $f \in \mathcal{S}$ function symbol of arity n a function $[\![f]\!] : \mathcal{D}^n \to D$ and for each predicate symbol $P \in \mathcal{P}$ of arity n a function $[\![P]\!] : D^n \to H$.*
Then a valuation into the model is a partial function $\sigma : \mathcal{V} \to D$ with finite domain. The syntax for updating valuations is the same as that for substitutions.
For σ valuation and t term, if $FV(t) \subseteq dom(\sigma)$ we define $[\![t]\!]_\sigma$ in the usual inductive way.
For σ valuation and A formula, if $FV(A) \subseteq dom(\sigma)$ we define $[\![A]\!]_\sigma$ inductively on A.
Notably:

- $[\![P(t_1...t_k)]\!]_\sigma \coloneqq [\![P]\!]([\![t_1]\!]_\sigma...[\![t_k]\!]_\sigma)$
- $[\![\forall x.A]\!]_\sigma \coloneqq \bigwedge_{v\in\mathcal{D}}\{[\![A]\!]_{\sigma[x\mapsto v]}\}$
- $[\![\exists x.A]\!]_\sigma \coloneqq \bigvee_{v\in\mathcal{D}}\{[\![A]\!]_{\sigma[x\mapsto v]}\}$

Theorem 2 (Soundness of Heyting algebras for first order logic). *For Γ context and A formula, if $\Gamma \vdash A$ is derivable in NJ then for any Heyting algebra $\mathcal{H}$, for any model on $\mathcal{H}$ and valuation σ, $[\![\Gamma]\!]_\sigma \leq [\![A]\!]_\sigma$.*

Proof. Standard induction.

3.3 Completeness

Definition 12 (Extraction). *The extraction of a formula A is*

$$\lfloor A \rfloor \coloneqq \{\Gamma, \Gamma \vdash^* A\}$$

Definition 13 (Universal Heyting algebra). *The universal Heyting algebra Ω also called context algebra has the underlying set $\{\bigcap_{i\in I}\lfloor A_i\rfloor, (A_i)_{i\in I}$ family of formulas$\}$. Its operations are defined as*

- $\leq := \subseteq$
- $\wedge := \cap$
- $\bigwedge := \bigcap$
- $a \vee b := \bigcap\{\omega \in \Omega, a \cup b \subseteq \omega\}$
- $\bigvee A := \bigcap\{\omega \in \Omega, \bigcup A \subseteq \omega\}$
- $a \Rightarrow b := \bigcap\{\omega \in \Omega, \bigcup\{c \in \Omega, a \wedge c \subseteq b\} \subseteq \omega\} = \bigvee\{c \in \Omega, a \wedge c \subseteq b\}$
- $\top := \{\Gamma, \Gamma \textit{ context}\} = \lfloor\top\rfloor$
- $\bot := \{\Gamma, \forall A, \Gamma \vdash A\} = \lfloor\bot\rfloor$

Lemma 5. *The following identities are true:*

- $a \vee b = \bigcap\{\lfloor D\rfloor, a \cup b \subseteq \lfloor D\rfloor, D \textit{ formula}\}$
- $\bigvee A = \bigcap\{\lfloor D\rfloor, \bigcup A \subseteq \lfloor D\rfloor, D \textit{ formula}\}$
- $a \Rightarrow b = \bigcap\{\lfloor D\rfloor, \bigcup\{c \in \Omega, a \wedge c \subseteq b\} \subseteq \lfloor D\rfloor, D \textit{ formula}\}$

Proof.
- For any D, $\lfloor D\rfloor \in \Omega$ so $a \vee b \subseteq \bigcap\{\lfloor D\rfloor, a \cup b \subseteq \lfloor D\rfloor, D \text{ formula}\}$
  Then let Γ such that $\forall \lfloor D\rfloor$, if $a \cup b \subseteq \lfloor D\rfloor$ then $\Gamma \in \lfloor D\rfloor$ and let $\omega \in \Omega$ such that $a \cup b \subseteq \omega$.
  $\omega = \bigcap_{i\in I}\lfloor C_i\rfloor$ for some $(C_i)_{i\in I}$. Let $i \in I$. We have $a \vee b \subseteq \lfloor C_i\rfloor$ so $\Gamma \in \lfloor C_i\rfloor$.
  Then $\Gamma \in \omega$.
- Same as above.
- By viewing $a \Rightarrow b$ as $\bigvee\{c \in \Omega, a \wedge c \subseteq b\}$ and using the result for $\bigvee$.

Lemma 6. *Ω forms a Heyting algebra.*

Proof. Ω is closed by arbitrary intersection and $\forall A, \lfloor A\rfloor \in \Omega$, so the operations all produce values in Ω.
Then we need to verify

- $\leq$ is an order: trivial
- $\wedge$ and $\bigwedge$ are greatest lower bounds: trivial
- $\vee$ and $\bigvee$ are lowest upper bounds: consider the $\vee$ case.
  For a and b in Ω, let $d \in \Omega$. If $a \cup b \subseteq d$ then $a \subseteq d$ and $b \subseteq d$. Then $a \subseteq a \vee b$ and $b \subseteq a \vee b$.
  For $c \in \Omega$ with $a \subseteq c$ and $b \subseteq c$, we have $a \cup b \subseteq c$ so $a \vee b \subseteq c$.
- $\Rightarrow$ verifies the implication property

- If $a \leq b \Rightarrow c$ with $c = \bigcap_{k \in K} \lfloor C_k \rfloor$, let $\Gamma \in a \wedge b$. Let $k \in K$, we want $\Gamma \in \lfloor C_k \rfloor$.
  $\Gamma \in a$ so $\Gamma \in b \Rightarrow c$ and we have for any D, if $\bigcup \{e \in \Omega, b \wedge e \subseteq c\} \subseteq \lfloor D \rfloor$ then $\Gamma \in \lfloor D \rfloor$.
  Consider $D \coloneqq \Gamma \Rightarrow C_k$ (where $\Gamma \Rightarrow B \coloneqq A_1 \Rightarrow ... \Rightarrow A_n \Rightarrow B$ with $\Gamma = A_1 ... A_n$ and B formula).
  Let $e \in \Omega$ with $b \wedge e \subseteq c$. Let $\Delta \in e$, $\{\Delta, \Gamma\} \in b \wedge e$ by the weakening lemma, then $\Delta, \Gamma \in c$.
  Then $\Delta, \Gamma \vdash^* C_k$ and $\Delta \vdash^* \Gamma \Rightarrow C_k$ which is $\Delta \vdash^* D$. This for any such Δ, so $e \subseteq \lfloor D \rfloor$.
  $\Gamma \vdash^* \Gamma \Rightarrow C_k$ then by repeated application of Kleene's lemma $\Gamma, \Gamma \vdash^* C_k$ and by the weakening lemma $\Gamma \vdash^* C_k$.
  Finally $\Gamma \in c$.
- If $a \wedge b \leq c$, let $\Gamma \in a$. We want for any $d \in \Omega$, if $\bigcup \{e \in \Omega, b \wedge e \subseteq c\} \subseteq d$ then $\Gamma \in d$.
  Let d such, since $a \wedge b = b \wedge a \subseteq c$, $a \subseteq d$ then $\Gamma \in d$.

– $\top$ is the greatest element of Ω and $\bot$ the least element: trivial.

Definition 14 (Interpretation in the propositional context algebra). *Let $[\![A]\!] \coloneqq \lfloor A \rfloor$ for A atomic formula.*

Definition 15 (Interpretation in the first order context algebra). *The model on Ω has:*

– *the set of terms as domain*
– *for f function symbol of arity n, $[\![f]\!] \coloneqq (t_1, ..., t_n) \mapsto f(t_1 ... t_n)$*
– *for P predicate symbol of arity n, $[\![P]\!] \coloneqq (t_1, ..., t_n) \mapsto \lfloor P(t_1, ..., t_n) \rfloor$*

Then for any t and σ, $[\![t]\!]_\sigma = \sigma(t)$.

Definition 16 (Closure). *For any A formula, let $cl(A) \coloneqq \bigcap \{d \in \Omega, [A] \in d\}$.*

Lemma 7. *For any A, $cl(A) \in \Omega$.*

Proof. Ω is stable by arbitrary intersection.

Lemma 8. *For any A, $cl(A) = \bigcap \{\lfloor D \rfloor, [A] \in \lfloor D \rfloor\}$.*

Proof. – $cl(A) \subseteq \bigcap \{\lfloor D \rfloor, [A] \in \lfloor D \rfloor\}$:
Easily since $\lfloor D \rfloor \in \Omega$ for any D.

– $\bigcap\{\lfloor D\rfloor, [A] \in \lfloor D\rfloor\} \subseteq cl(A)$:
  Let Γ such that for any D, if $[A] \in \lfloor D\rfloor$ then $\Gamma \in \lfloor D\rfloor$ and let $\omega \in \Omega$ such that $[A] \in \omega$.
  $\omega = \bigcap_{i\in I} \lfloor C_i\rfloor$ for some $(C_i)_{i\in I}$. For $i \in I$, $[A] \in \lfloor C_i\rfloor$ so $\Gamma \in \lfloor C_i\rfloor$.
  Then $\Gamma \in \omega$.

Then $\Gamma \in cl(A)$ means $[A]$ can be replaced by Γ to the left of any sequent in a derivation. This is similar to the axiom replacement lemma, except this operation does not necessarily follow the structure of the derivation.

Lemma 9. *For Γ context and A formula, if $\Gamma \vdash_{ne} A$ then $\Gamma \in cl(A)$.*

Proof. By axiom replacement, considering the previous lemma.

DBLP:conf/csl/Coquand93

Theorem 3 (Key theorem (propositional case)).

$$\forall A, cl(A) \subseteq [\![A]\!] \subseteq \lfloor A\rfloor$$

Proof. By induction on A:

– A atomic: $cl(A) \subseteq \lfloor A\rfloor = [\![A]\!]$
  Let Γ such that for any D if $A \vdash^* D$ then $\Gamma \vdash^* D$. Then $\Gamma \vdash^* A$ with $D := A$.
– $cl(A \wedge B) \subseteq [\![A \wedge B]\!]$: by induction we only need $cl(A \wedge B) \subseteq cl(A) \cap cl(B)$.
  Let $\Gamma \in cl(A \wedge B)$ and D such that $A \vdash^* D$ (resp. $B \vdash^* D$). Since $A \wedge B \vdash_{ne} A$ (resp. $A \wedge B \vdash_{ne} B$) by the axiom replacement lemma we have $A \wedge B \vdash^* D$.

  $[\![A \wedge B]\!] \subseteq \lfloor A \wedge B\rfloor$: by the induction hypotheses we have $[\![A \wedge B]\!] \subseteq \lfloor A\rfloor \cap \lfloor B\rfloor$. Then the $\wedge$-intro rule concludes the proof.
– $cl(A \vee B) \subseteq [\![A \vee B]\!]$: consider C such that $[\![A]\!] \cup [\![B]\!] \subseteq \lfloor C\rfloor$.
  Then by the induction hypotheses $cl(A) \subseteq \lfloor C\rfloor$ and $cl(B) \subseteq \lfloor C\rfloor$.
  We have to show $[A \vee B] \in \lfloor C\rfloor$.
  Since $[A] \in cl(A) \subseteq \lfloor C\rfloor$ (resp. $[B] \in cl(B) \subseteq \lfloor C\rfloor$) we have $A \vdash^* C$ (resp. $B \vdash^* C$). Then by $\vee$-elim and *coerce* we have $A \vee B \vdash^* C$.

  $[\![A \vee B]\!] \subseteq \lfloor A \vee B\rfloor$: by definition of $[\![A]\!] \vee [\![B]\!]$, we need to show that $[\![A]\!] \cup [\![B]\!] \subseteq \lfloor A \vee B\rfloor$.
  $[\![A]\!] \cup [\![B]\!] \subseteq \lfloor A\rfloor \cup \lfloor B\rfloor$, then the $\vee$-intro rules concludes the proof.

– $cl(A \Rightarrow B) \subseteq [\![A \Rightarrow B]\!]$: by the implication rule we need $cl(A \Rightarrow B) \wedge [\![A]\!] \subseteq [\![B]\!]$, then with the induction hypotheses $cl(A \Rightarrow B) \wedge \lfloor A \rfloor \subseteq cl(B)$ suffices.
Let $\Gamma \in cl(A \Rightarrow B) \wedge \lfloor A \rfloor$.

$$\Gamma \vdash^* A \text{ and for any } C, \text{ if } A \Rightarrow B \vdash^* C \text{ then } \Gamma \vdash^* C$$

Let D such that $B \vdash^* D$. We need $\Gamma \vdash^* D$.
By weakening this is equivalent to $\Gamma, \Gamma \vdash^* D$ and then by Kleene's lemma $\Gamma \vdash^* \Gamma \Rightarrow D$ suffices.
We can prove this if $A \Rightarrow B \vdash^* \Gamma \Rightarrow D$, and by $\Rightarrow$-intro this boils down to showing $A \Rightarrow B, \Gamma \vdash^* D$.
$A \Rightarrow B, \Gamma \vdash_{ne} B$ by $\Rightarrow$-elim and $B \vdash^* D$ so by the axiom replacement lemma $A \Rightarrow B, \Gamma \vdash^* D$.

$[\![A \Rightarrow B]\!] \subseteq \lfloor A \Rightarrow B \rfloor$: by the induction hypotheses $cl(A) \Rightarrow \lfloor B \rfloor \subseteq \lfloor A \Rightarrow B \rfloor$ suffices.
DBLP:conf/csl/Coquand93 Let $\Gamma \in cl(A) \Rightarrow \lfloor B \rfloor$. We need $\Gamma \vdash^* A \Rightarrow B$. We have

$$\forall D, (\forall c \in \Omega, cl(A) \cap c \subseteq \lfloor B \rfloor \rightarrow c \subseteq \lfloor D \rfloor) \rightarrow \Gamma \vdash^* D$$

Take $D \coloneqq A \Rightarrow B$. Let $c \in \Omega$ such that $cl(A) \cap c \subseteq \lfloor B \rfloor$ then let $\Sigma \in c$.
By weakening $A, \Sigma \in cl(A) \wedge c$. Then $A, \Sigma \vdash^* B$ and $\Sigma \vdash^* A \Rightarrow B$.
This for any $\Sigma \in c$ so $c \subseteq \lfloor A \Rightarrow B \rfloor$
Then $\Gamma \vdash^* A \Rightarrow B$.
– $\top$ and $\bot$ are trivial cases.

Theorem 4 (Key theorem (first order case)). *For any A formula and σ valuation into Ω, σ is also a substitution and*

$$cl(\sigma(A)) \subseteq [\![A]\!]_\sigma \subseteq \lfloor \sigma(A) \rfloor$$

Proof. By induction on A. Cases $A \wedge B, A \vee B, A \Rightarrow B$ and atomic case work the same as in the propositional case.

– $cl(\sigma(\forall x.A)) \subseteq [\![\forall x.A]\!]_\sigma$:
$\sigma(\forall x.A) = \forall x.\sigma[x \mapsto x](A)$ (we can assume that x does not appear free in the image of $FV(\forall x.A)$ by σ). Note $\sigma' \coloneqq \sigma[x \mapsto x]$.
Let $\Gamma \in cl(\sigma(\forall x.A))$. That means for any D, if $[\forall x.\sigma'(A)] \vdash^* D$ then $\Gamma \vdash^* D$.
We need to prove that for all d term, $\Gamma \in [\![A]\!]_{\sigma[x \mapsto d]}$. Let d a term.

$\Gamma \in cl(\sigma[x \mapsto d](A))$ suffices.
Let D such that $\sigma[x \mapsto d](A) \vdash^* D$, we need to prove $\Gamma \vdash^* D$ which follows from $[\forall x.\sigma'(A)] \vdash^* D$.
$\sigma[x \mapsto d](A) = (\sigma'(A))[d/x]$ so $[\forall x.\sigma'(A)] \vdash_{ne} \sigma[x \mapsto d](A)$.
Then by axiom replacement $[\forall x.\sigma'(A)] \vdash^* D$.

$[\![\forall x.A]\!]_\sigma \subseteq \lfloor \sigma(\forall x.A) \rfloor$:
Let Γ such that $\Gamma \in [\![\forall x.A]\!]_\sigma$. By α-conversion we can assume x fresh.
$\forall d, \Gamma \in [\![A]\!]_{\sigma[x \mapsto d]}$. Then $\Gamma \in [\![A]\!]_{\sigma[x \mapsto x]} \subseteq \lfloor \sigma[x \mapsto x](A) \rfloor$.
Then by the $\forall_I$ rule $\Gamma \vdash^* \forall x.\sigma[x \mapsto x](A)$, and since $\forall x.\sigma[x \mapsto x](A) = \sigma(\forall x.A)$, $\Gamma \in \lfloor \sigma(\forall x.A) \rfloor$.

– $cl(\sigma(\exists x.A)) \subseteq [\![\exists x.A]\!]_\sigma$:
Let $\Gamma \in cl(\sigma(\exists x.A))$, assume x fresh, pose $\sigma' \coloneqq \sigma[x \mapsto x]$.
For D any formula, if $[\exists x.\sigma'(A)] \vdash^* D$ then $\Gamma \vdash^* D$
$\Gamma \in [\![\exists x.A]\!]_\sigma$ if and only if for all D, if for each d term $[\![A]\!]_{\sigma[x \mapsto d]} \subseteq \lfloor D \rfloor$ then $\Gamma \vdash^* D$.
Consider D such that $\forall d, [\![A]\!]_{\sigma[x \mapsto d]} \subseteq \lfloor D \rfloor$. We need to prove $[\exists x.\sigma'(A)] \vdash^* D$.

$$\frac{\exists x.\sigma'(A), \sigma'(A) \vdash^* D \qquad \exists x.\sigma'(A) \vdash_{ne} \exists x.\sigma'(A)}{\exists x.\sigma'(A) \vdash_{ne} D}\ \exists_E$$

$[\sigma'(A)] \in cl(\sigma'(A)) \subseteq [\![A]\!]_{\sigma'}$ by the induction hypothesis, then by the hypothesis on D we have $[\sigma'(A)] \in \lfloor D \rfloor$ for the first premise. The second is trivial with the *ax* rule and the *coerce* rule completes the derivation.

$[\![\exists x.A]\!]_\sigma \subseteq \lfloor \sigma(\exists x.A) \rfloor$:
Let $\Gamma \in [\![\exists x.A]\!]_\sigma$: for all D formula, if for each d term $[\![A]\!]_{\sigma[x \mapsto d]} \subseteq \lfloor D \rfloor$ then $\Gamma \vdash^* D$.
We show that $D \coloneqq \sigma(\exists x.A) = \exists x.\sigma[x \mapsto x](A)$ fulfils this condition.
Let d, Σ such that $\Sigma \in [\![A]\!]_{\sigma[x \mapsto d]}$. Then by the induction hypothesis $\Sigma \in \lfloor \sigma[x \mapsto d](A) \rfloor$.
$\sigma[x \mapsto d](A) = (\sigma[x \mapsto x](A))[d/x]$ so $\Sigma \vdash^* (\sigma[x \mapsto x](A))[d/x]$
Then $\Sigma \vdash^* \exists x.\sigma[x \mapsto x](A)$ i.e. $\Sigma \vdash^* \sigma(\exists x.A)$.

Theorem 5 (Completeness). *Propositional version: for Γ context and A formula, if in any Heyting algebra $[\![\Gamma]\!] \subseteq [\![A]\!]$ then $\Gamma \vdash^* A$.*
First order version: for Γ context and A formula, if in any Heyting algebra with model and for any σ valuation $[\![\Gamma]\!]_\sigma \subseteq [\![A]\!]_\sigma$ then $\Gamma \vdash^* A$.

Proof. We work in the universal algebra.
$\Gamma \vdash^* A$ is $\Gamma \in \lfloor A \rfloor$. In the first order case, let σ the substitution taking each variable of $FV(\Gamma, A)$ to itself. then $A = \sigma(A)$ (by induction on the structure of A).
Then it is enough to prove $\Gamma \in [\![A]\!] \supseteq [\![\Gamma]\!]$.
$[\![\Gamma]\!] = \bigwedge_{C \in \Gamma} [\![C]\!]$. Consider $C \in \Gamma$.
$\Gamma \vdash_{ne} C$ so $\Gamma \in cl(C) \subseteq [\![C]\!]$.
Then $\Gamma \in [\![\Gamma]\!] \subseteq \lfloor A \rfloor$.
$\Gamma \vdash^* A$.

Theorem 6 (Cut elimination). *For Γ context and A formula, if $\Gamma \vdash A$ then $\Gamma \vdash^* A$.*

Proof. By completeness since Heyting algebras are sound for natural deduction.

Some derivations of $\Gamma \vdash A$ will be transformed into cut-free derivations where the last rule is *coerce*. Trying to characterise them may be useful.

3.4 Formalisation

If we define Ω as $\{\{\Gamma : context, \forall A, P\ A \to \Gamma \vdash^* A\} | P : form \to Type\}$ (the naive definition for arbitrary intersections of extractions of formulas), arbitrary intersections of elements of Ω cannot be defined due to universe inconsistencies.
If we replace $Type$ by $Prop$, the loss of information means we need to have $\Gamma \vdash^* A$ live in $Prop$ also, and we cannot extract the algorithm to ocaml code. However, the whole proof can then be formalised.
Using the *Eval compute* command on the algorithm applied to a derivation we can obtain the result of the algorithm. However, since formulas are processed by the key lemma which does case analysis, computation blocks if the derivation involves formula variables.
We can also relax the universe constraints in Coq, deliberately working in an inconsistent system to get extraction.

Conclusion

Strong completeness of Heyting algebras produces an algorithm for proof normalisation. The algorithm can be studied by evaluating it on specific derivations and by *Print*ing the Coq function to study the generated code. It would be interesting to compare the normalisation with the one

formalised by Danko Ilik.

The transformations between Heyting algebras and Kripke structures are not a new result, but their formalisation should be helpful when studying their semantics.

A key direction in future work is additional study of the constructed normalisation algorithm. The effect of the model transformations when applied to the universal algebra are also of interest.
Strong completion for higher order logic should also be possible.

Annex

3.5 Atomic axiom

We apply the algorithm to

$$\frac{}{A \vdash A}\, ax$$

with A atomic.

Term name	Term definition	Term value	Term type	Term evaluated type
d_A	$*$	$\frac{}{A \vdash A}\, ax$	$A \vdash A$	$A \vdash A$
S_A	$soundness(d_A)$	$\lambda\ \Gamma\ d.d$	$[\![A]\!] \leq [\![A]\!]$	$\forall \Gamma, \Gamma \vdash^* A \to \Gamma \vdash^* A$
v_A	Weakening using $A \in [A]$	$\lambda\ D\ d.d$	$[A] \in cl(A)$	$\forall D, A \vdash^* D \to A \vdash^* D$
Kcl_A	Key lemma for A	$\lambda\ \Gamma\ H.H\ A\ \frac{\frac{}{A \vdash_{ne} A}\, ax}{A \vdash^* A}\, coerce$	$cl(A) \subseteq [\![A]\!]$	$\forall \Gamma, (\forall D, A \vdash^* D \to \Gamma \vdash^* D) \to$
	$Kcl_A\ [A]\ v_A$	$\frac{\frac{}{A \vdash_{ne} A}\, ax}{A \vdash^* A}\, coerce$	$[A] \in [\![A]\!]$	$A \vdash^* A$
	$S_A\ (Kcl_A\ [A]\ v_A)$	$\frac{\frac{}{A \vdash_{ne} A}\, ax}{A \vdash^* A}\, coerce$	$[A] \in [\![A]\!]$	$A \vdash^* A$
Kex_A	Key lemma for A	$\lambda\ \Gamma\ d.d$	$[\![A]\!] \subseteq \lfloor A \rfloor$	$\forall \Gamma, \Gamma \vdash^* A \to \Gamma \vdash^* A$
	$Kex_A\ [A]\ (S_A(Kcl_A\ [A]\ v_A))$	$\frac{\frac{}{A \vdash_{ne} A}\, ax}{A \vdash^* A}\, coerce$	$[A] \in \lfloor A \rfloor$	$A \vdash^* A$

The last term is the result of the algorithm.

3.6 Disjunction axiom

We apply the algorithm to

$$\frac{}{A \vee B \vdash A \vee B}\, ax$$

with A and B atomic.

References

1. Thorsten Altenkirch, Peter Dybjer, Martin Hofmann, and Phil Scott. Normalization by evaluation for typed lambda calculus with coproducts. In *16th Annual IEEE Symposium on Logic in Computer Science*, pages 303–310, 2001.
2. Ulrich Berger and Helmut Schwichtenberg. An inverse of the evaluation functional for typed λ–calculus. In R. Vemuri, editor, *Proceedings of the Sixth Annual IEEE Symposium on Logic in Computer Science*, pages 203–211. IEEE Computer Society Press, Los Alamitos, 1991.
3. Catarina Coquand. From semantics to rules: A machine assisted analysis. In *CSL*, pages 91–105, 1993.
4. Hugo Herbelin and Gyesik Lee. Formalizing logical metatheory: Semantical cut-elimination using kripke models for first-order predicate logic. *http://formal.hknu.ac.kr/Kripke/*, 2014. [Online, accessed 2014-06-11].
5. Olivier Hermant. Sequent calculus, completeness and cut elimination. [Lesson notes], 2013.
6. Mitsuhiro Okada. *An Introduction to Linear Logic: Expressiveness and Phase Semantics*, volume Volume 2 of *MSJ Memoirs*, pages 255–295. The Mathematical Society of Japan, Tokyo, Japan, 1998.

Term name	Term definition	Term value	Term type	Term evaluated type
$d_{A\vee B}$	$*$	$\dfrac{}{A\vee B\vdash A\vee B}\,ax$	$A\vee B\vdash A\vee B$	$A\vee B\vdash A\vee B$
$S_{A\vee B}$	$soundness(d_{A\vee B})$	$\lambda\ \Gamma\ H.H$	$[\![A\vee B]\!]\leq[\![A\vee B]\!]$	$\forall\Gamma,\Gamma\in[\![A\vee B]\!]\to\Gamma\in[\![A\vee B]\!]$
	$[\![A\vee B]\!]$	$\lambda\ \Gamma.\forall\omega\in\Omega,\lfloor A\rfloor\cup\lfloor B\rfloor\subseteq\omega\to\Gamma\in\omega$	$Type$	$Type$
	Weakening for $A\vee B$	$\lambda D\ d.d$	$[A\vee B]\in cl(A\vee B)$	$\forall D,A\vee B\vdash^{*}D\to A\vee B\vdash^{*}D$
Kcl_X	Key lemma for X atomic	$\lambda\Gamma\ H.H\ X\ \dfrac{\dfrac{}{X\vdash_{ne}X}\,ax}{X\vdash^{*}X}\,coerce$	$cl(X)\subseteq[\![X]\!]$	$\forall\Gamma,(\forall D,X\vdash^{*}D\to\Gamma\vdash^{*}D)\to\Gamma\vdash^{*}X$
$Kcl_{A\vee B}$	Key lemma for $A\vee B$	$\lambda\Gamma\ Hcl\ D\ Hsub.Hcl\ D\ (Hsub\ [A\vee B]\ *)$	$cl(A\vee B)\subseteq[\![A\vee B]\!]$	$\forall\Gamma,\Gamma\in cl(A\vee B)\to\forall D,[\![A]\!]\cup[\![B]\!]\subseteq\lfloor D\rfloor\to\Gamma\vdash^{*}D$