

Computing with Proof-Nets

(a subject by Olivier Laurent, ENS Lyon)

Questions marked with (*) might be a bit more involved.

We only use the terminology *proof-net* for a proof-structure which satisfies the Danos-Regnier correctness criterion (acyclicity and connectedness in the multiplicative case, and acyclicity only in the multiplicative exponential case).

Multiplicative Booleans

In this part we work with proof-nets for multiplicative linear logic without units, thus built upon the following formulas:

$$A ::= X \mid X^\perp \mid A \otimes A \mid A \wp A$$

X ranges over the elements of a given set of variables. X and $X^\perp$ are called *atomic formulas*. A proof-net is *atomic* if the conclusions of all its axiom nodes are labelled with atomic formulas.

Question 1. Prove it is possible to transform any proof-net into an atomic one without changing the labels of its conclusions.

We consider the formula $\mathbf{B} = (X^\perp \wp X^\perp) \wp (X \otimes X)$.

Question 2. Give all the cut-free proof-nets with a unique conclusion labelled $\mathbf{B}$.

Among the two atomic proof-nets of Question 2, only one can be obtained through the transformation of Question 1. We call it **TRUE**. The other atomic one is called **FALSE**. The set of Booleans is $\mathbb{B} = \{\mathbf{true}, \mathbf{false}\}$ and we define $\mathbf{true} = \mathbf{TRUE}$ and $\mathbf{false} = \mathbf{FALSE}$.

A **function** f from $\mathbb{B}$ to $\mathbb{B}$ is said to be **represented by the proof-net $\mathcal{R}$** with two conclusions $\mathbf{B}^\perp$ and $\mathbf{B}$ if the normal form of the proof-net $\mathcal{R}_b$ (obtained by putting a cut node between the conclusion $\mathbf{B}$ of b and the conclusion $\mathbf{B}^\perp$ of $\mathcal{R}$) is $f(b)$, for any $b \in \mathbb{B}$.

Question 3. Give a proof-net representing the negation function $\mathbb{B} \rightarrow \mathbb{B}$:

$$\begin{aligned} \mathbf{true} &\mapsto \mathbf{false} \\ \mathbf{false} &\mapsto \mathbf{true} \end{aligned}$$

Question 4. Give all the cut-free proof-nets with two conclusions: $\mathbf{B}^\perp$ and $\mathbf{B}$.

Question 5. Give a function from $\mathbb{B}$ to $\mathbb{B}$ which cannot be represented by a proof-net.

Let G be a formula, a **function** f from $\mathbb{B}^n$ ($n \geq 0$) to $\mathbb{B}$ is said to be **G -represented by the proof-net $\mathcal{R}$** with n conclusions $\mathbf{B}^\perp$ and a conclusion $\mathbf{B} \otimes G$ if the normal form of the proof-net $\mathcal{R}_{\vec{b}}$ (obtained by putting n cut nodes between the conclusion $\mathbf{B}$ of each b_i ($b_i \in \vec{b}$) and the i th conclusion $\mathbf{B}^\perp$ of $\mathcal{R}$) has a $\otimes$ node above its unique conclusion with $f(\vec{b})$ above its left premise, for any $\vec{b} \in \mathbb{B}^n$.

Question 6. Prove any function from $\mathbb{B}$ to $\mathbb{B}$ can be **B**-represented by some proof-net.

If A is a formula, we define $\mathbf{B}[A] = \mathbf{B}[A/X] = (A^\perp \wp A^\perp) \wp (A \otimes A)$ (in particular $\mathbf{B}[X] = \mathbf{B}$).

Question 7. If $\mathcal{R}$ is a proof-net with conclusions $C_1, \dots, C_n$ and A is a formula, define a proof-net $\mathcal{R}[A/X]$ with conclusions $C_1[A/X], \dots, C_n[A/X]$.

We define $\text{TRUE}[A] = \text{TRUE}[A/X]$ and $\text{FALSE}[A] = \text{FALSE}[A/X]$ with conclusion $\mathbf{B}[A]$.

Let G and $A_1, \dots, A_n$ be formulas, a function f from $\mathbb{B}^n$ ($n \geq 0$) to $\mathbb{B}$ is said to be *G-represented up to $(A_1, \dots, A_n)$* by the proof-net $\mathcal{R}$ with conclusions $\mathbf{B}[A_1]^\perp, \dots, \mathbf{B}[A_n]^\perp$ and $\mathbf{B} \otimes G$ if the normal form of the proof-net $\mathcal{R}_{\vec{b}}$ (obtained by putting n cut nodes between the conclusion $\mathbf{B}[A_i]$ of each $\vec{b}_i[A_i]$ and the conclusion $\mathbf{B}[A_i]^\perp$ of $\mathcal{R}$, with $b_i \in \vec{b}$) has a $\otimes$ node above its unique conclusion with $f(\vec{b})$ above its left premise, for any $\vec{b} \in \mathbb{B}^n$.

Question 8. Give a proof-net **B**-representing up to $(\mathbf{B}, X, X)$ the **if** function $\mathbb{B}^3 \rightarrow \mathbb{B}$:

$$\text{true}, b_1, b_2 \mapsto b_1$$

$$\text{false}, b_1, b_2 \mapsto b_2$$

Question 9. If $f : \mathbb{B}^{n+1} \rightarrow \mathbb{B}$ is *G*-represented up to $(A_0, \dots, A_n)$ by $\mathcal{R}$ and $g : \mathbb{B}^m \rightarrow \mathbb{B}$ is *H*-represented up to $(C_1, \dots, C_m)$ by $\mathcal{S}$, explain how to represent the composition:

$$b_1, \dots, b_m, b_{m+1}, \dots, b_{m+n} \mapsto f(g(b_1, \dots, b_m), b_{m+1}, \dots, b_{m+n})$$

Question 10. (*) Prove any function from $\mathbb{B}^2$ to $\mathbb{B}$ can be $(\mathbf{B} \otimes \mathbf{B} \otimes \mathbf{B} \otimes \mathbf{B}[\mathbf{B}] \otimes \mathbf{B}[\mathbf{B}])$ -represented up to $(\mathbf{B}[\mathbf{B}] \otimes \mathbf{B}[\mathbf{B}], \mathbf{B})$ by some proof-net.

Exponential Booleans

We now move to proof-nets for multiplicative exponential linear logic without units, thus built upon the following formulas:

$$A ::= X \mid X^\perp \mid A \otimes A \mid A \wp A \mid !A \mid ?A$$

We consider the formula $\mathbf{C} = !(?X^\perp \wp (?X^\perp \wp X))$.

Question 11. Show that there exist exactly two cut-free proof-nets with unique conclusion $\mathbf{C}$.

As in the previous part, we obtain a representation of Booleans by defining $\widetilde{\text{true}}$ and $\widetilde{\text{false}}$ to be these two proof-nets.

Question 12. Give a proof-net with two conclusions: $?(\mathbf{B}[!X]^\perp)$ and $\mathbf{C}$.

Question 13. Give a proof-net with two conclusions: $\mathbf{C}^\perp$ and $!\mathbf{B}[!X]$.

Question 14. Compute the normal form of the proof-net with conclusions $?(\mathbf{B}[!X]^\perp)$ and $!\mathbf{B}[!X]$ obtained by adding a cut node between the conclusions $\mathbf{C}$ and $\mathbf{C}^\perp$ of the proof-nets of the previous two questions. *Give some comments.*

A function f from $\mathbb{B}^n$ ($n \geq 0$) to $\mathbb{B}$ is said to be *e-represented* by the proof-net $\mathcal{R}$ with n conclusions $\mathbf{C}^\perp$ and a conclusion $\mathbf{C}$ if the normal form of the proof-net $\mathcal{R}_{\vec{b}}$ (obtained by putting n cut nodes between the conclusion $\mathbf{C}$ of each $\vec{b}_i$ and the i th conclusion $\mathbf{C}^\perp$ of $\mathcal{R}$, with $b_i \in \vec{b}$) is $\widetilde{f(\vec{b})}$ (up to the R  tor   equivalence), for any $\vec{b} \in \mathbb{B}^n$.

Question 15. (*) Prove any function from $\mathbb{B}^n$ ($n \geq 0$) to $\mathbb{B}$ can be e-represented by some proof-net.