

# Sublogarithmic uniform Boolean proof nets

Clément Aubert\*

LIPN – UMR7030, CNRS – Université Paris 13,  
99 av. J.-B. Clément, 93430 Villetaneuse, France

**Abstract** Using a proofs-as-programs correspondence, Terui was able to compare two models of parallel computation: Boolean circuits and proof nets for multiplicative linear logic. Mogbil *et. al.* gave a logspace translation allowing us to compare their computational power as uniform complexity classes. This paper presents a novel translation in  $AC^0$  and focuses on a simpler restricted notion of uniform Boolean proof nets. We can then encode constant-depth circuits and compare complexity classes below logspace, which were out of reach with the previous translations.

## Introduction

Boolean proof nets were introduced by Terui in [8] to study the implicit complexity of *proofs nets for Multiplicative Linear Logic* [4] comparatively to Boolean circuits. Those two models of parallel computation were successfully linked using a *proofs-as-programs* framework, which matches up *cut-elimination* in proof nets with *evaluation* in circuits. Surprisingly [8] does not take into account uniformity, which guarantees that the resources needed to build a Boolean circuit is inferior to the computational power it will deliver. [7] and [6] studied the Boolean proof nets in a uniform way and introduced some non-determinism in it. As their translation from Boolean circuit families to Boolean proof net families is in logspace ( $L$ ), it remained unknown if the results were still valid when applied to sublogarithmic classes of complexity, that is to say  $AC^0$  and  $NC^1$ . By restricting the Boolean proof nets we use, this paper offers a new proof of the correspondence between circuits and proof nets and extends it to constant-depth circuits.

Boolean circuits ([9], section 1) and proof nets ([3], section 3) are canonical models of parallel computation, but the latter was mostly seen from the viewpoint of *sequential* implicit complexity. To *evaluate* a proof net is to eliminate its cuts, but to do so with suitable bounds we need to define a parallel elimination. Trying to apply the two usual rules of rewriting ( $\rightarrow_m$  and  $\rightarrow_a$ ) in parallel leads to critical pairs, so we are forced to define a new kind of cut (*tightening-cut*) and a new rewriting rule ( $\rightarrow_t$ ). The simulation of this reduction rule by Boolean circuits needs  $UstConn_2$  gates to be made with efficiency.

The proof nets we study are for Multiplicative Linear Logic with unbounded arity (**MLLu**, section 2) and because of the linearity of this logic, we are forced to keep track of the partial results generated by the evaluation that are unused in the result. Boolean proof nets (section 4) – as introduced by Terui – have an expensive way of manipulating this *garbage*. In this paper we introduce *proof circuits* (section 5) as a refinement of the Boolean proof nets that are simpler to manipulate. They are made of *pieces* which translate *gates* and compose easily, so that we reduce the size of the proof net translating the Boolean circuits. In section 6 we conclude our paper with our main result (theorem 2): there exists a constant-depth reduction from Boolean circuit families to proof circuit families. So our new framework offers a variant of the proofs for complexity results and extends them to small classes of complexity, in a uniform way.

---

\*Work partially supported by the French project Complice (ANR-08-BLANC-0211-01).

## 1 Boolean circuits

Boolean circuits (definition 2) are of great interest in the study of complexity, for instance because of the efficiency of their parallel evaluation. One of their features is that they work only on inputs of fixed length, and that forces us to deal with *families* of Boolean circuits – and there arises the question of *uniformity* (definition 4).

**Definition 1** (Boolean function). A  $n$ -ary Boolean function  $f^n$  is a map from  $\{0, 1\}^n$  to  $\{0, 1\}$ . A Boolean function family is a sequence  $f = (f^n)_{n \in \mathbb{N}}$  and a basis is a set of Boolean functions and Boolean function families. We set :

$$\mathfrak{B}_0 = \{\neg, \vee^2, \wedge^2\} \text{ and } \mathfrak{B}_1 = \{\neg, (\vee^n)_{n \geq 2}, (\wedge^n)_{n \geq 2}\}$$

The Boolean function  $UstConn_2$ , given in input the coding of an undirected graph  $G$  of degree at most 2 and two names of gates  $s$  and  $t$ , outputs 1 iff there is a path between  $s$  and  $t$  in  $G$ .

**Definition 2** (Boolean circuits). Given a basis  $\mathfrak{B}$ , a Boolean circuit over  $\mathfrak{B}$  with  $n$  inputs  $C$  is a directed acyclic finite and labeled graph. The nodes of fan-in 0 are called *input nodes* and are labeled with  $x_1, \dots, x_n, 0, 1$ . Non-input nodes are called *gates* and each one of them is labeled with a Boolean function from  $\mathfrak{B}$  whose arity coincides with the fan-in of the gate. There is a unique node of fan-out 0 which is the *output gate*. We indicate with a subscript the number of inputs: a Boolean circuit  $C$  with  $n$  inputs will be named  $C_n$ .

The *depth* of a Boolean circuit  $C_n$   $d(C_n)$  is the length of the longest path between an input node and the output gate. Its *size*  $|C_n|$  is its number of nodes. We will only consider Boolean circuits of size  $n^{O(1)}$ , that is to say polynomial in the size of their input.

$C_n$  *accepts a word*  $w \equiv w_1 \dots w_n \in \{0, 1\}^n$  if  $C_n$  evaluates to 1 when  $w_1, \dots, w_n$  are respectively assigned to  $x_1, \dots, x_n$ . A *family of Boolean circuits* is an infinite sequence  $C = (C_n)_{n \in \mathbb{N}}$  of Boolean circuits,  $C$  *accepts a language*  $X \subseteq \{0, 1\}^*$  iff for all  $w \in X$ ,  $C_{|w|}$  accepts  $w$ .

We now recall the definition of the *Direct Connection Language* of a family of Boolean circuits, an infinite sequence of tuples that describes it totally.

**Definition 3** (Direct Connection Language [9]). Given  $\overline{(\cdot)}$  a suitable coding of integers and  $C = (C_n)_{n \in \mathbb{N}}$  a family of Boolean circuits over a basis  $\mathfrak{B}$ , its *Direct Connection Language* – written  $L_{DC}(C)$  – is the set of tuples  $\langle y, \overline{g}, \overline{p}, \overline{b} \rangle$ , such that for  $|y| = n$ , we have:  $g$  is a gate in  $C_n$ , labeled with  $b \in \mathfrak{B}$  if  $p = \epsilon$ , else  $b$  is its  $p^{th}$  predecessor.

**Definition 4** (Uniformity [1]). A family  $C$  is said to be *DLOGTIME*-uniform if there exists a deterministic Turing Machine with random access to the input tape that given  $L_{DC}(C)$ ,  $n$  and  $\overline{g}$  outputs in time  $O(\log(|C_n|))$  any information (position, label or predecessors) about the gate  $g$  in  $C_n$ .

Despite the fact that a *DLOGTIME* Turing Machine has more computational power than a constant-depth circuit, “*a consensus has developed among researchers in circuit complexity that this DLOGTIME uniformity is the ‘right’ uniformity condition*” for small complexity classes [5]. Any further reference to uniformity is to be read as *DLOGTIME* uniformity.

**Definition 5** ( $AC^i$ ,  $NC^i$ ). For all  $i \in \mathbb{N}$ , given  $\mathfrak{B}$  a basis, a language  $X \subseteq \{0, 1\}^*$  belongs to the class  $AC^i(\mathfrak{B})$  (resp.  $NC^i(\mathfrak{B})$ ) if  $X$  is accepted by a uniform family of polynomial-size,  $\log^i$ -depth Boolean circuits over  $\mathfrak{B}_1 \cup \mathfrak{B}$  (resp.  $\mathfrak{B}_0 \cup \mathfrak{B}$ ). We set  $AC^i(\emptyset) = AC^i$  and  $NC^i(\emptyset) = NC^i$ .

## 2 MLLu

Rather than using Multiplicative Linear Logic (**MLL**) – which would force us to compose binary connectives to obtain  $n$ -ary connectives – we work with **MLLu** which differs only on the arities of the connectives but better relates to circuits. We write  $\vec{A}$  (resp.  $\overleftarrow{A}$ ) for an ordered sequence of formulae  $A_1, \dots, A_n$ , (resp.  $A_n, \dots, A_1$ ).

**Definition 6** (Formulae of **MLLu**). Given  $\alpha$  a literal and  $n \geq 2$ , formulae of **MLLu** are:

$$A ::= \alpha \mid \alpha^\perp \mid \otimes^n(\vec{A}) \mid \wp^n(\overleftarrow{A})$$

Duality is defined with respect to De Morgan's law :

$$\begin{aligned} (A^\perp)^\perp &\equiv A \\ (\otimes^n(\vec{A}))^\perp &\equiv \wp^n(A^\perp) \\ (\wp^n(\overleftarrow{A}))^\perp &\equiv \otimes^n(\overrightarrow{A^\perp}) \end{aligned}$$

As for the rest of this article, consider that  $A$ ,  $B$  and  $D$  will refer to **MLLu** formulae.  $A[B/D]$  denotes  $A$  where every occurrence of  $B$  is replaced by an occurrence of  $D$ . We write  $A[D]$  if  $B = \alpha$ .

**Definition 7** (Sequent calculus for **MLLu**). A *sequent* of **MLLu** is of the form  $\vdash \Gamma$ , where  $\Gamma$  is a multiset of formulae. The *inference rules* of **MLLu** are as follow :

$$\begin{array}{c} \frac{}{\vdash A, A^\perp} \text{ax.} \qquad \frac{\vdash \Gamma_1, A_1 \quad \dots \quad \vdash \Gamma_n, A_n}{\vdash \Gamma_1, \dots, \Gamma_n, \otimes^n(\vec{A})} \otimes^n \\ \\ \frac{\vdash \Gamma, A \quad \vdash \Delta, A^\perp}{\vdash \Gamma, \Delta} \text{cut} \qquad \frac{\vdash \Gamma, \overleftarrow{A}}{\vdash \Gamma, \wp^n(\overleftarrow{A})} \wp^n \end{array}$$

*Derivations of MLLu* are built with respect to those rules. **MLLu** has neither weakening nor contraction, but admits implicit exchange and eliminates cuts. The formulae  $A$  and  $A^\perp$  in the rule *cut* are called the *cut formulae*.

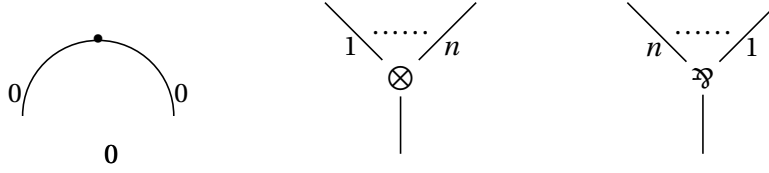
## 3 Proof nets

Proof nets are a parallel syntax for **MLLu** that abstract away everything irrelevant and only keep the structure of the proofs. We introduce measures (definition 10) on them in order to study their structure and complexity, and a parallel elimination of their cuts (definition 11).

**Definition 8** (Links). We introduce in figure 1 three sorts of *links* –  $\bullet$ ,  $\otimes^n$  and  $\wp^n$  – which correspond to **MLLu** rules.

Every link may have two kinds of *ports*: *principal* ones, indexed by 0 and written below, and *auxiliary* ones, indexed by  $1, \dots, n$  and written above. The auxiliary ports are ordered, but as we always represent the links as in figure 1, we may safely omit the numbering. Axiom links have two principal ports, both indexed with 0, but we can always differentiate them (for instance by naming them  $0_r$  and  $0_l$ ) if we need to.

*Remark 1.* There is no sort cut: a cut is represented with an edge between two principal ports.

Figure 1:  $ax$ -link,  $\otimes^n$ -link and  $\wp^n$ -link

**Definition 9** (Decorated derivations and proof net). Given a derivation of **MLLu**, we decorate it in the following way:

- an index is associated to every formula. The formulae introduced by an axiom have the same proper index, and the formulae introduced by a logical rules ( $\otimes^n$  and  $\wp^n$ ) have a *fresh* index,
- a *description* is associated to every sequent.

The rules given in figure 2 indicate how a proof is decorated and how to build a *proof net* from a description.

The *type* of a proof net  $P$  is  $\Gamma$  if there exists a decorated derivation of  $\vdash \Gamma \triangleright \mathcal{D}(P)$ : a proof net always has several types, but up to  $\alpha$ -equivalence (renaming of the literals) we may always assume it has a unique *principal type*. If a proof net may be typed with  $\Gamma$ , then for every  $A$  it may be typed with  $\Gamma[A]$ . By extension we will use the notion of type of an edge.

The structures obtained by following those rules respect criterion of correctness. For instance two ports of a same link may not be connected, a port may be connected only once and every auxiliary port is connected. We do not have to take into account *pseudo nets*.

*Remark 2.* The same proof net – as it abstracts derivations – may be induced by several descriptions. Conversely, several graphs – as representations of proof nets – may correspond to the same proof net: we get round of this difficulty by associating to every proof net a single drawing among the drawings with the minimal number of crossings between edges, for the sake of simplicity. Two graphs representing proof nets that can be obtained from the same description are taken to be equal.

**Definition 10** (Size and depth of a proof net). The size  $|P|$  of a proof net  $P$  is the number of its links.

The depth of a proof net is defined with respect to its type:

- The depth of a formula is defined by recurrence:

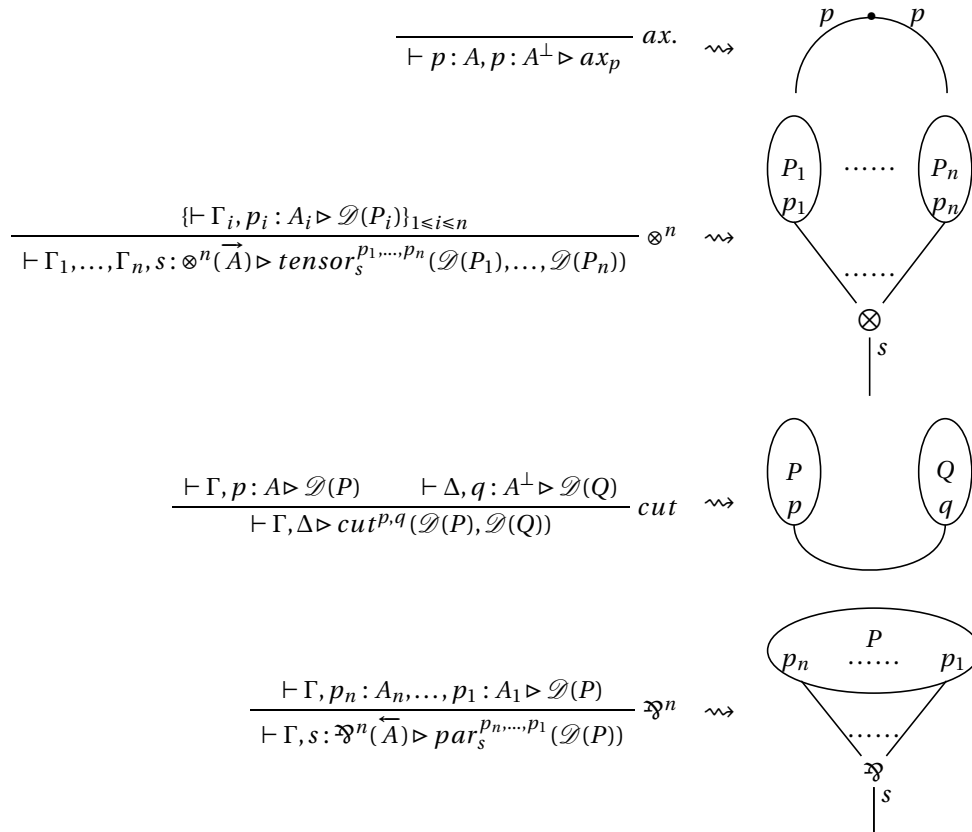
$$\begin{aligned} d(\alpha) &= d(\alpha^\perp) = 1 \\ d(\otimes^n(\vec{A})) &= d(\wp^n(\vec{A})) = 1 + \max(d(A_1), \dots, d(A_n)) \end{aligned}$$

- The depth  $d(\pi)$  of a derivation  $\pi$  is the maximum depth of cut formulae in it.
- The depth  $d(P)$  of a proof net  $P$  is

$$\min\{d(\pi) \mid \pi \text{ can be decorated as } \vdash \Gamma \triangleright \mathcal{D}(P) \text{ for some } \Gamma\}$$

The depth  $d(P)$  of a proof net depends on its type, but it is minimal when we consider the principal type of the proof net.

To make the most of the computational power of proof nets, we need to achieve a speed-up in the number of steps needed to normalize them. If we try roughly to reduce in parallel a cut between two  $ax$ -links, we are faced with a critical pair. [8] avoids this situation by using a *tightening reduction* which eliminates in one step all the cuts between axioms. We can then safely reduce all the other cuts in parallel.



Edges representing  $\Gamma$  or  $\Delta$  are not drawn,  $\mathcal{D}(P)$  is one of the description of the proof net  $P$ .

Figure 2: From decorated derivations to proof nets

**Definition 11** (Cuts and parallel cut-elimination). A cut is an edge between the principal ports of two links. If one of these links is an  $ax$ -link, two cases occurs:

if the other link is an  $ax$ -link, we take the maximal chain of  $ax$ -links connected by their principal ports and defines this set of cuts as a  $t$ -cut,

otherwise the cut is an  $a$ -cut.

Otherwise it is a  $m$ -cut and we know that for  $n \geq 2$ , one link is a  $\otimes^n$ -link and the other is a  $\wp^n$ -link.

We define on figure 3 three rewriting rules on the proof nets. For  $r \in \{t, a, m\}$ , if  $Q$  may be obtained from  $P$  by erasing all the  $r$ -cuts of  $P$  in parallel, we write  $P \Rightarrow_r Q$ . If  $P \Rightarrow_t Q$ ,  $P \Rightarrow_a Q$  or  $P \Rightarrow_m Q$ , we write  $P \Rightarrow Q$ . To *normalize a proof net*  $P$  is to apply  $\Rightarrow$  until we reach a cut-free proof net.  $\Rightarrow^*$  is defined as the transitive reflexive closure of  $\Rightarrow$ .

**Theorem 1** (Parallel cut-elimination [8]). *Every proof net  $P$  normalizes in at most  $O(d(P))$  applications of  $\Rightarrow$ .*

So the time needed to evaluate a proof net is relative to its depth, and can be in the worst case linear in its size – as for the Boolean circuits.

For all  $\circ \in \{(\wp^n)_{n \geq 2}, (\otimes^n)_{n \geq 2}\}$ ,  $\circ$  may be  $\bullet$  in  $\rightarrow_m$ .

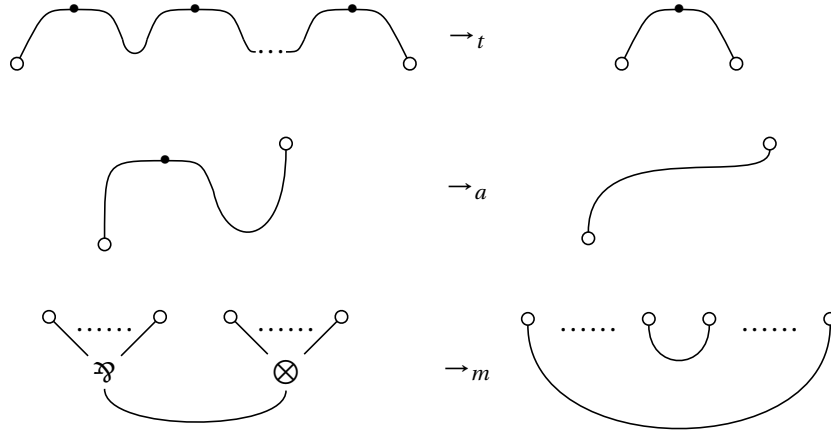


Figure 3:  $t$ -,  $a$ - and  $m$ -reductions

## 4 Boolean proof nets

In order to compare the complexities of proof nets and of Boolean circuits, we need to define how proof nets represent Boolean values (definition 12) and Boolean functions (definition 13). To study them in a uniform framework we define their Direct Connection Language (definition 14).

**Definition 12** (Boolean type, 0 and 1 [8]). Let  $b_0$  and  $b_1$  be the two proof nets of type

$$\mathbf{B} = \wp^3(\alpha^\perp, \alpha^\perp, \alpha \otimes \alpha)$$

respectively used to represent false and true:

$$\begin{aligned} \mathcal{D}(b_0) &= \text{par}_s^{q,p,r}(\text{tensor}_r^{p,q}(ax_p, ax_q)) & b_0 &\equiv \text{Diagram 1} \\ \mathcal{D}(b_1) &= \text{par}_s^{p,q,r}(\text{tensor}_r^{p,q}(ax_p, ax_q)) & b_1 &\equiv \text{Diagram 2} \end{aligned}$$

We write  $\vec{b}$  for  $b_{i_1}, \dots, b_{i_n}$  for  $i \in \{0, 1\}$ .

As we can see,  $b_0$  and  $b_1$  differ on their planarity: descriptions and proof nets exhibit the exchanges that were kept implicit in derivations.

**Definition 13** (Boolean proof nets [8]). A *Boolean proof net with  $n$  inputs* is a proof net  $P(\vec{p})$  of type

$$\vdash p_1 : \mathbf{B}^\perp[A_1], \dots, p_n : \mathbf{B}^\perp[A_n], s : \otimes^{1+m}(\mathbf{B}[A], D_1, \dots, D_m)$$

Given  $\vec{b}$  of length  $n$ ,  $P(\vec{b})$  is obtained by connecting with cuts  $p_j$  to  $b_{i_j}$  for all  $1 \leq j \leq n$ .

$P(\vec{b}) \Rightarrow^* Q$  where  $Q$  is unique, cut-free and for some descriptions  $Q_1, \dots, Q_n$  described by

$$tensor(\mathcal{D}(b_i), Q_1, \dots, Q_m) \text{ for } i \in \{0, 1\}.$$

We write  $P(\vec{b}) \rightarrow_{ev.} b_i$ .

$P(\vec{p})$  represents a Boolean function  $f^n$  if for all  $w \equiv i_1 \dots i_n \in \{0, 1\}^n$ ,  $P(b_{i_1}, \dots, b_{i_n}) \rightarrow_{ev.} b_{f(w)}$ .

We may easily define families of Boolean proof nets and language accepted by a family of Boolean proof nets.


The tensor indexed with  $s$  in the type is the *result tensor*: it collects the result of the computation on its first auxiliary port and the *garbage* – here named  $D_1, \dots, D_m$  – on its other auxiliary ports.

**Definition 14** (Direct Connection Language for proof nets [7]). Given  $P = (P_n)_{n \in \mathbb{N}}$  a family of Boolean proof nets, its *Direct Connection Language* – written  $L_{DC}(P)$  – is the set of tuples  $\langle y, \bar{g}, \bar{p}, \bar{b} \rangle$  where for  $|y| = n$ :  $g$  is a link in  $P_n$ , of sort  $b$  if  $p = e$  else the  $p^{th}$  premise of  $g$  is the link  $b$ .

If  $\langle y, \bar{p}, 0, \bar{b} \rangle$  or  $\langle y, \bar{b}, 0, \bar{p} \rangle$  belong to  $L_{DC}(P)$ , there is a cut between  $b$  and  $p$  in  $C_{|y|}$ .

## 5 Proof circuits

A proof circuit is a Boolean proof net (fact 1) made out of pieces (definition 15) which represents Boolean functions, constants or duplicates values. Garbage is manipulated in an innovative way, examples 1 should help to understand the mechanism of computation.

From now on every edge represented by  is connected on its right to an auxiliary port numbered with an integer other than 1 of the result tensor: it carries a piece of garbage.

**Definition 15** (Pieces). We present in the table 1 the set of *pieces* at our disposal. Entries are labeled with  $e$ , exits with  $s$  and garbage with  $g$ . Edges labeled  $b_k$  – for  $k \in \{0, 1\}$  – are connected to the edge labeled  $s$  of the piece  $b_k$ .

Table 1: Pieces

We set  $2 \leq j \leq i$ .

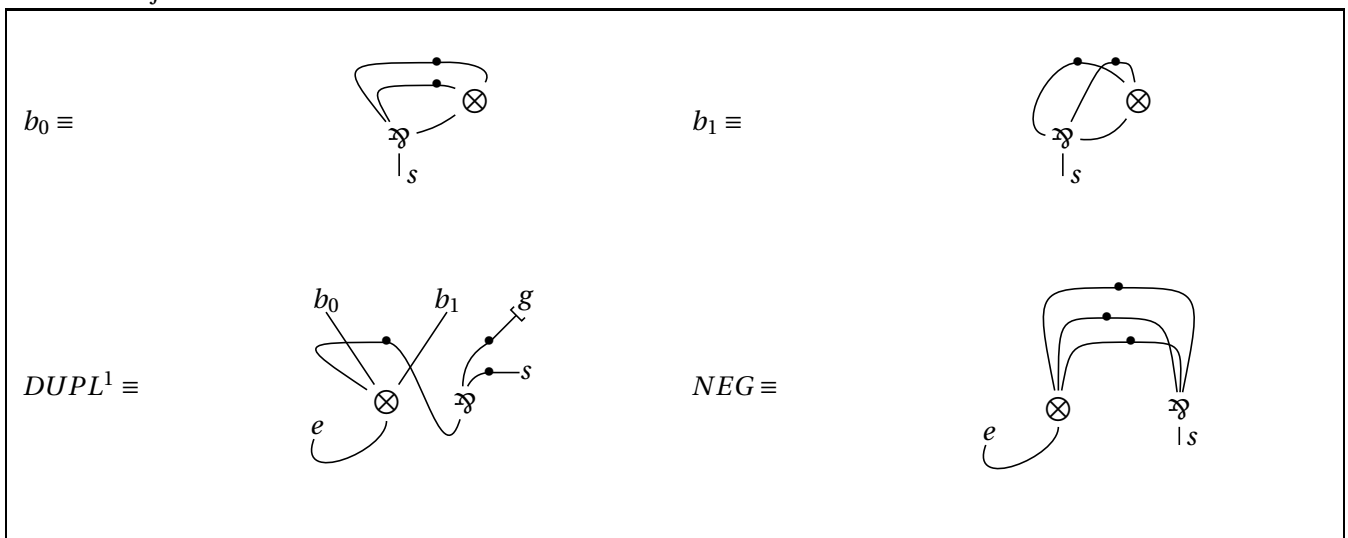
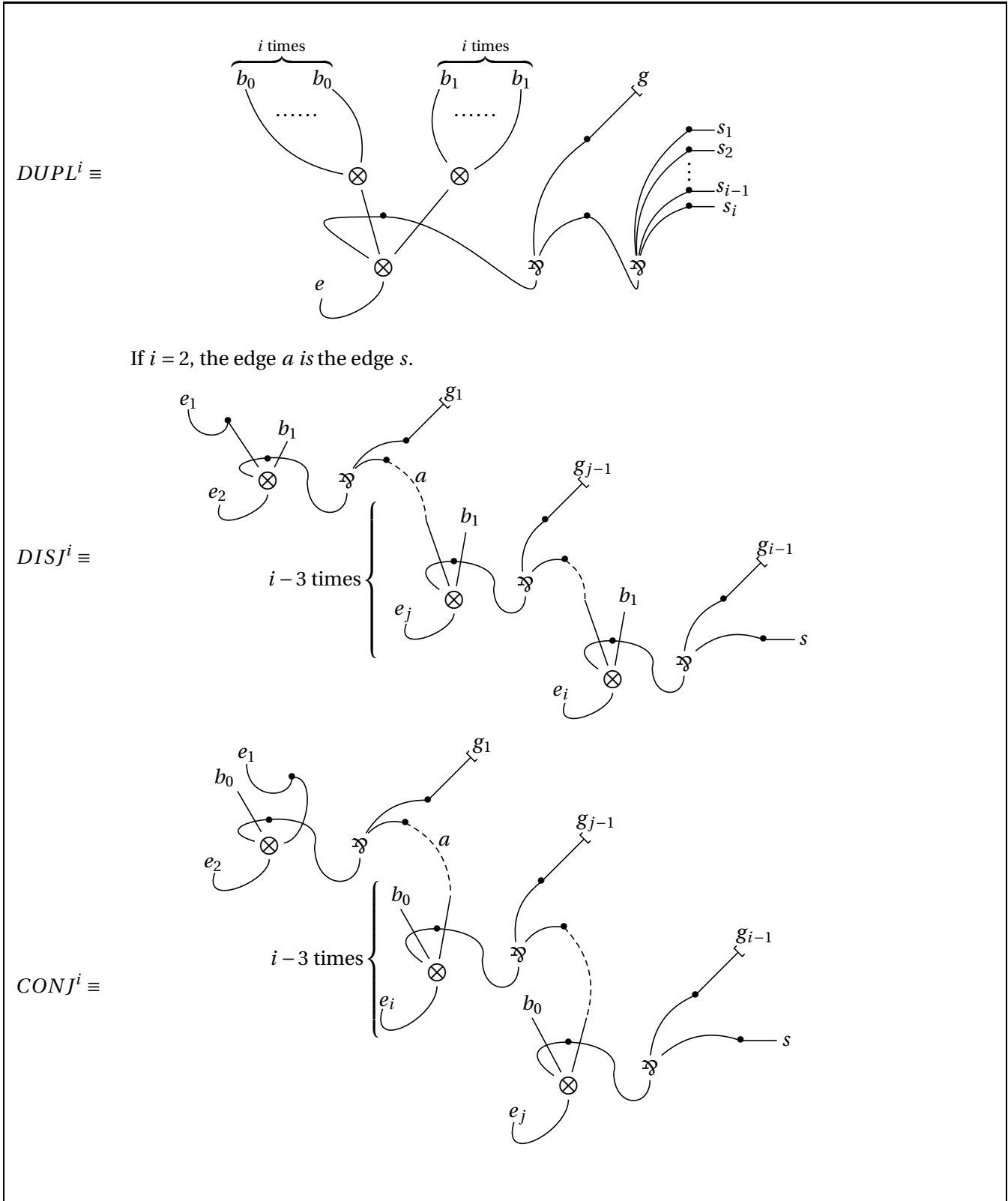


Table 1: Pieces – continued from previous page





A piece  $\mathcal{P}$  with  $i \geq 0$  entries,  $j \geq 1$  exits and  $k \geq 0$  garbage is one of the piece in the table 1, where  $i$  edges are labeled with  $e_1, \dots, e_i$ ,  $j$  edges are labeled with  $s_1, \dots, s_j$  and  $k$  edges go to the result tensor.

We have  $\mathcal{P} \in \{b_0, b_1, NEG, \{DUPL^i\}_{i \geq 1}, \{DISJ^i\}_{i \geq 2}, \{CONJ^i\}_{i \geq 2}\}$ .

To compose two pieces  $\mathcal{P}_1$  and  $\mathcal{P}_2$  we connect an exit of  $\mathcal{P}_1$  to an entry of  $\mathcal{P}_2$ . It is not allowed to loop: we can not connect an entry and an exit belonging to the same piece.

An entry (resp. an exit) that is not connected to an exit (resp. an entry) of another piece is said to be *unconnected*.

**Definition 16** (Proof circuits). A proof circuit  $\mathcal{C}_n(\vec{p})$  with  $n$  inputs and one output is obtained by composing pieces such that  $n$  entries and one exit are unconnected. If no garbage is created we add a  $DUPL^1$ -piece connected to the unconnected exit to produce some artificially. Then we add a result tensor whose first edge is connected to the exit – which is also the output of the proof circuit – and the others to the garbage. We then label every unconnected entries with  $p_1, \dots, p_n$ : those are the inputs of the proof circuit.

Given  $\vec{b}$  of length  $n$ ,  $\mathcal{C}_n(\vec{b})$  is obtained by connecting with cuts  $p_j$  to  $b_{i_j}$  for all  $1 \leq j \leq n$ .

**Fact 1.** Every proof circuit is a Boolean proof net.

**Proof.** We prove this fact with a contractibility criterion [2], by induction on the height of the pieces of the proof circuit (counted as the number of pieces from the considered piece to the result tensor). As a proof circuit can always be typed with

$$\vdash \mathbf{B}^\perp[A_1], \dots, \mathbf{B}^\perp[A_n], \otimes^{1+m}(\mathbf{B}[A], D_1, \dots, D_m)$$

it is a Boolean proof net.

This fact establishes that proof circuits normalize and output a value, and that it is possible to represent Boolean functions with them.

Families of proof circuits and *acceptation of a language by a family of proof circuits* are defined as usual.

*Examples 1.* We present briefly two examples of computation: the normalization of a piece  $b_0$  connected to a  $NEG$ -piece (figure 4, page 24) and how the conditional works (figure 5, page 25). Conditional is the core of the computation, we find this pattern in every piece except  $NEG$  and the constants.

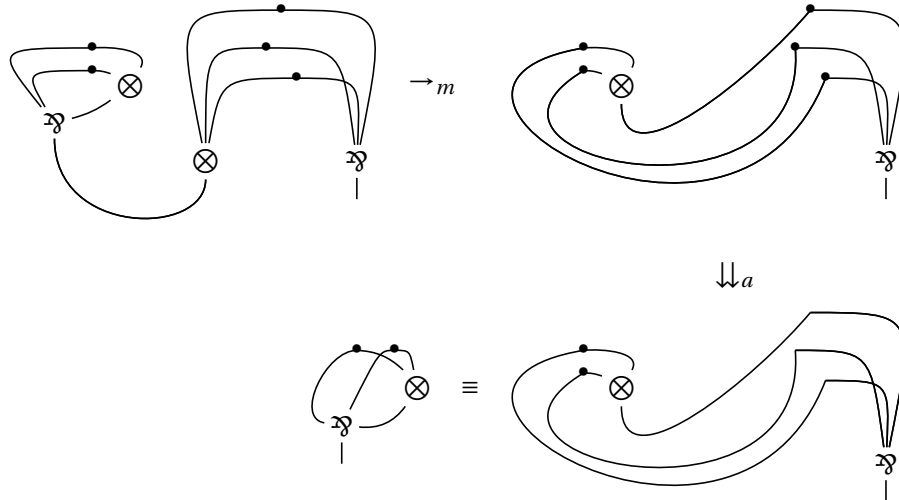
*Remark 3.* To compose two proof circuits  $\mathcal{C}_1$  and  $\mathcal{C}_2$ , we remove the result tensor of  $\mathcal{C}_1$ , identify the unconnected exit of  $\mathcal{C}_1$  with the selected input of  $\mathcal{C}_2$ , and recollect all the garbage with the result tensor of  $\mathcal{C}_2$ . We then label the unconnected entries anew and obtain a proof circuit.

**Definition 17** ( $PCC^i$  (resp.  $mBN^i$ , [7])). A language  $X \subseteq \{0, 1\}^*$  belongs to the class  $PCC^i$  (resp.  $mBN^i$ ) if  $X$  is accepted by a polynomial-size,  $\log^i$ -depth uniform family of proof circuits (resp. of Boolean proof nets).

If we add "*UstConn<sub>2</sub>-pieces*" to the set of pieces, we may easily define  $PCC^i(UstConn_2)$  and remark that for all  $i \in \mathbb{N}$ ,  $PCC^i \subseteq PCC^i(UstConn_2)$ . [8] proves that there exists Boolean proof nets of constant-depth and polynomial size that represent  $UstConn_2$ , so we do not define  $mBN^i(UstConn_2)$  because it would be easy to prove that this class is equal to  $mBN^i$  for all  $i \in \mathbb{N}$ .

*Remark 4.* By fact 1 we have trivially that for all  $i \in \mathbb{N}$ ,  $PCC^i \subseteq mBN^i$ .

**Lemma 1.** For all proof circuit  $\mathcal{C}_n(\vec{p})$  and all  $\vec{b}$ , the cuts at maximum depth in  $\mathcal{C}_n(\vec{b})$  are between the entry of a piece and a value (a constant  $b_0$  or  $b_1$ , or an input  $b_{i_j}$  for some  $1 \leq j \leq n$ ).

Figure 4:  $b_0$  connected to  $NEG$  normalizes to  $b_1$ 

**Proof.** For every piece  $\mathcal{P}$  of  $\mathcal{C}_n(\vec{b})$  any cut connecting an entry is always of depth superior or equal to the maximal depth of the cuts connecting the exits. The cuts of  $\mathcal{P}$  that do not connect an entry or an exit of a piece are always of depth inferior or equal to cuts connecting the entries.

The depths of the cut formulae slowly increase from the exit to the entry, and as the entries that are not connected to other pieces are connected to values, this lemma is proved.

## 6 Results

By using our proof circuits we prove anew the inclusions between  $AC^i$  and logical classes of complexity and extend this inclusion to sublogarithmic classes of complexity.

**Definition 18** (Problem: Translation from  $AC^i$  to  $PCC^i$ ).

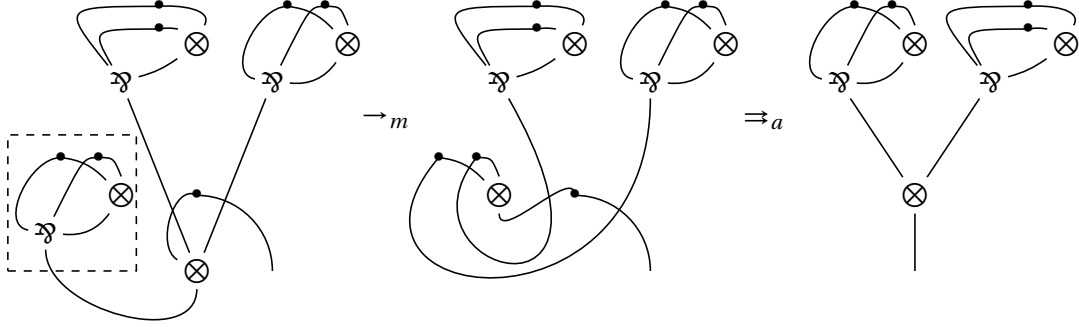
Input:  $L_{DC}(C)$  for  $C$  a family of Boolean circuits in  $AC^i$ .

Output:  $L_{DC}(\mathcal{C})$  for  $\mathcal{C}$  a family of proof circuits in  $PCC^i$ , such that for all  $n \in \mathbb{N}$ , for all  $\vec{b} \equiv b_{i_1}, \dots, b_{i_n}$ ,  $\mathcal{C}_n(\vec{b}) \rightarrow_{ev} b_j$  iff  $C_n(i_1, \dots, i_n)$  evaluates to  $j$ .

**Theorem 2.** For all  $i \in \mathbb{N}$ , translation from  $AC^i$  to  $PCC^i$  belongs to  $AC^0$ .

**Proof.** The translation from  $C$  to  $\mathcal{C}$  is obvious, it relies on coding: for every  $n$ , a first constant-depth circuit associate to every gate of  $C_n$  the corresponding piece simulating its Boolean function. If the fan-out of this gate is  $k > 1$ , a  $DUPL^k$ -piece is associated to the exit of the piece, and the pieces are connected as the gates. The input nodes are associated to the inputs of  $\mathcal{C}_n$ . A second constant-depth circuit recollects the only free exit and the garbage of the pieces and connects them to the result tensor. The composition of these two Boolean circuits produces a constant-depth Boolean circuit that builds proof circuits.

It is easy to check that  $CONJ^k$ ,  $DISJ^k$  and  $NEG$  represent  $\wedge^k$ ,  $\vee^k$  and  $\neg$  respectively.  $DUPL^k$  duplicates a value  $k$  times,  $b_0$  and  $b_1$  represent 0 and 1 by convention. The composition of these pieces does not raise any trouble:  $\mathcal{C}_n$  effectively simulates  $C_n$  on every input of size  $n$ .



The input (here in a dashed rectangle) is proof net of type **B**, and it “selects” – according to its planarity or non-planarity – during the normalization which one of  $b_0$  or  $b_1$  is connected to the first auxiliary port of the tensor and so is considered as the result – the other being treated as garbage.

Figure 5: The conditional, the core of the computation

Concerning the bounds: the longest path between an entry or a constant and the result tensor goes through at most  $2 \times d(C_n)$  pieces and we know by lemma 1 that the increase of the depth is linear in the number of pieces crossed. We conclude that  $d(\mathcal{C}_n) \leq 2 \times 3 \times d(C_n)$  and that  $\mathcal{C}_n$  normalizes in  $O(d(C_n))$  parallel steps.

Concerning the size, by counting we know that a gate of fan-in  $n$  and fan-out  $m$  is simulated by a piece made of  $O(m + n)$  links. As the number of edges in  $C_n$  is bounded by  $|C_n|^2$ , the size of  $\mathcal{C}_n$  is at most  $O(|C_n|^2)$ .

A Boolean circuit with unbounded (resp. bounded) arity of size  $s$  is translated by a Proof circuit of size quadratic (resp. linear) in  $s$ , whereas [8] considers only unbounded Boolean circuits and translate them with Boolean proof nets of size  $O(s^5)$ . Our translation – thanks mostly to the easier garbage collection – needs less computational power, is more clear and besides lower the size of the Boolean proof nets obtained.

Of course, we could naturally extend this translation to a translation from  $AC^i(UstConn_2)$  to  $PCC^i(UstConn_2)$  and still remain in  $AC^0$ . But it is of little interest to look for a sublogarithmic translation toward a class of complexity which is probably not strictly included in  $L$ .

**Fact 2.** *As the reduction from  $C$  to  $\mathcal{C}$  is in  $AC^0$ , we know that this reduction is correct for Boolean circuit families in  $AC^0$  and that every  $\mathcal{C}$  obtained by this translation is uniform.*

This result brings a novelty in the study of the proof nets as a class of complexity, making them able to simulate very small classes of complexity born from the Boolean circuits.

**Theorem 3** (Simulation). *For all  $i \in \mathbb{N}$ , for all Boolean proof net family  $P = (P_n)_{n \in \mathbb{N}}$  in  $mBN^i$ , there exists a family of Boolean circuits  $C = (C_n)_{n \in \mathbb{N}}$  in  $AC^i(UstConn_2)$  and a constant-depth circuit in  $AC^0$  that given  $L_{DC}(P)$  outputs  $L_{DC}(C)$  such that for all  $\vec{b} \equiv b_{i_1} \dots b_{i_n}$ ,  $P_n(\vec{b}) \rightarrow_{ev.} b_j$  iff  $C_n(i_1, \dots, i_n)$  evaluates to  $j$ .*

**Proof.** We know thanks to [8] that for  $r \in \{a, m, t\}$  an unbounded fan-in constant-depth circuit with  $O(|P_n|^3)$  gates – with  $UstConn_2$  gates to identify chains of axioms if  $r = t$  – is able to reduce all the  $r$ -cuts of  $P_n$  in parallel.

A first constant-depth circuit establishes the configuration – which describes  $P_n$  – from  $L_{DC}(P)$  and constant-depth circuits update this configuration after steps of normalization. Once the configuration of the normal form of  $P_n$  is obtained, a last constant-depth circuit identifies the first proof

net connected to the result tensor and establishes if it is  $b_0$  or  $b_1$  – that is to say if the result of the evaluation is *false* or *true*.

As all the circuits are of constant depth, the depth of  $C_n$  is linear in  $d(P_n)$ . The size of  $C_n$  is  $O(|P_n|^4)$ : every circuit simulating a parallel reduction needs  $O(|P_n|^3)$  gates and in the worst case – if  $d(P_n)$  is linear in the size of the proof circuit –  $O(|P_n|)$  steps are needed to normalize the proof net.

The remark 4 helps us to conclude that  $PCC^i \subseteq mBN^i \subseteq AC^i(UstConn_2)$

The simulation is slightly different from the translation: the Boolean circuit does not have to identify the pieces or any mechanism of computation of  $P_n$ , but simply to apply  $\Rightarrow_t, \Rightarrow_a, \Rightarrow_m$  to it until it reaches a normal form and then look at the value obtained. This simulation can be applied to any Boolean proof net, but in order to have results concerning complexity we preferred to stay in this uniform framework.

**Theorem 4.** *For all  $i \in \mathbb{N}$ ,  $AC^i \subseteq PCC^i \subseteq AC^i(UstConn_2)$ .*

**Proof.** By theorem 2 and theorem 3. The key point is to notice – as the reductions are in  $AC^0$  – that  $AC^0 \subseteq PCC^0 \subseteq AC^0(UstConn_2)$ .

*Remark 5.* We focused on sublogarithmic classes of complexity, but we can draw more general conclusions by re-introducing  $UstConn_2$ . From what precedes and from the fact that  $UstConn_2$  may be represented by Boolean proof nets of constant-depth and polynomial size, it is easy to conclude that for all  $i \in \mathbb{N}$ ,  $PCC^i(UstConn_2) = AC^i(UstConn_2) = mBN^i$ .

## Conclusion

By restricting ourselves to the uniform complexity classes and by lightening the simulation of the Boolean functions by proof nets, we established the validity of results given by [8] and [6] when extended to constant-depth Boolean circuits. Those complexity classes are of great interest as they are below  $L$  and mostly used in reductions. This paper proves that proof nets for Multiplicative Linear Logic are a pertinent tool to study complexity classes, including very small ones, even if we do not use exponentials.

The simulation of the parallel elimination of  $t$ -cuts by Boolean circuits needs  $UstConn_2$  gates. But as  $UstConn_2 \in L$ , there is for the time being no clue if a sublogarithmic Boolean circuit can simulate Boolean proof nets:  $AC^0(UstConn_2) \subseteq AC^1 \supseteq L$ .

Our future work will aim to prove that proof nets are a model of computation as relevant as Alternating Turing Machines but easier to manipulate: as we are in an implicit complexity framework, the size of our object suffices to know in which class of complexity it rests, whereas the only way of knowing where is an ATM is to run it on inputs. We already have gateways – by using correspondences with Boolean circuits – between Boolean proof nets and ATM, but our objective is to establish direct proofs.

## References

- [1] David A. Barrington, Neil Immerman & Howard Straubing (1990): *On uniformity within NCI*. *Journal of Computer and System Sciences* 41(3), pp. 274–306, doi:10.1109/SCT.1988.5262.
- [2] Vincent Danos (1990): *La Logique Linéaire appliquée à l'étude de divers processus de normalisation (principalement du  $\lambda$ -calcul)*. These de doctorat, Université Paris VII.
- [3] Vincent Danos & Laurent Regnier (1989): *The structure of multiplicatives*. *Archive for Mathematical logic* 28(3), pp. 181–203, doi:10.1007/BF01622878.
- [4] Jean-Yves Girard (1996): *Proof-nets: The parallel syntax for proof-theory*. *Logic and Algebra* 180, pp. 97–124.
- [5] William Hesse, Eric Allender & David A. Barrington (2002): *Uniform constant-depth threshold circuits for division and iterated multiplication*. *Journal of Computer and System Sciences* 65(4), pp. 695–716, doi:10.1016/S0022-0000(02)00025-9. Available at <http://ftp.cs.rutgers.edu/pub/allender/division.pdf>.
- [6] Virgile Mogbil (2009): *Non-deterministic Boolean Proof Nets*. In: *Proceedings of FOPARA'09, Lecture Notes in Computer Science* 6324, Springer, pp. 131–145, doi:10.1007/978-3-642-15331-0\_9. Available at [http://hal.archives-ouvertes.fr/docs/00/44/39/25/PDF/nBPN\\_preprintLIPN09.pdf](http://hal.archives-ouvertes.fr/docs/00/44/39/25/PDF/nBPN_preprintLIPN09.pdf).
- [7] Virgile Mogbil & Vincent Rahli (2007): *Uniform circuits, & Boolean proof nets*. In: *Proceedings of LFCS'07, Lecture Notes in Computer Science* 4514, Springer, pp. 401–421, doi:10.1007/978-3-540-72734-7\_28. Available at [http://hal.archives-ouvertes.fr/docs/00/14/39/28/PDF/mwBN\\_preprintLIPN07.pdf](http://hal.archives-ouvertes.fr/docs/00/14/39/28/PDF/mwBN_preprintLIPN07.pdf).
- [8] Kazushige Terui (2004): *Proof Nets and Boolean Circuits*. In: *Proceedings of LICS'04*, pp. 182–191, doi:10.1109/LICS.2004.1319612. Available at <http://www.kurims.kyoto-u.ac.jp/~terui/pn.pdf>.
- [9] Heribert Vollmer (1999): *Introduction to Circuit Complexity: A Uniform Approach*. Springer Verlag.