The Separation Theorem for Differential Interaction Nets

Damiano Mazza[1,⋆] and Michele Pagani[2,⋆⋆]

[1] Laboratoire d'Informatique de Paris Nord
damiano.mazza@lipn.univ-paris13.fr
http://www-lipn.univ-paris13.fr/~mazza
[2] Dipartimento di Filosofia – Università degli Studi Roma Tre
pagani@uniroma3.it
http://logica.uniroma3.it/~pagani

Abstract. Differential interaction nets (DIN) have been introduced by Thomas Ehrhard and Laurent Regnier as an extension of linear logic proof-nets. We prove that DIN enjoy an internal separation property: given two different normal nets, there exists a dual net separating them, in analogy with Böhm's theorem for the λ-calculus. Our result implies in particular the faithfulness of every non-trivial denotational model of DIN (such as Ehrhard's finiteness spaces). We also observe that internal separation does not hold for linear logic proof-nets: our work points out that this failure is due to the fundamental asymmetry of linear logic exponential modalities, which are instead completely symmetric in DIN.

Keywords: Differential interaction nets, faithfulness, linear logic, observational equivalence, proof-nets.

1 Introduction

The question of separation is an important one in computer science and, more recently, also in proof theory. The best known example of separation result is Böhm's theorem for the pure λ-calculus [1]: if t, t' are two distinct closed $\beta\eta$-normal terms, then there exist terms $u_1, \dots, u_n$, such that $tu_1 \dots u_n \to_\beta^* \mathbf{0}$ and $t'u_1 \dots u_n \to_\beta^* \mathbf{1}$.[3] This result has consequences both at the semantical level as well as at the syntactical one: on the one hand it entails that a model of the λ-calculus cannot identify two different $\beta\eta$-normal forms without being trivial (in this case we say that the model is *faithful*, or *injective*); on the other hand it establishes a balance between syntactical constructs and β-reduction: any difference in the structure of a $\beta\eta$-normal form implies a difference in the value of that normal form on suitable arguments.

After Böhm, this kind of question was studied by Friedman and Statman in the simply typed framework [2, 3], leading to what is often called "typed Böhm's

[⋆] Supported by a post-doc fellowship of French ANR project "NOCoST".

[⋆⋆] Post-doc fellow, research project: "Ricerche sulla geometria della logica".

[3] As it is usual in the λ-calculus, $\mathbf{1} = \lambda xy.x$ and $\mathbf{0} = \lambda xy.y$.

theorem".[4] In this case the two distinct $\beta\eta$-normal terms have the same type $A_1, \ldots, A_n \to X$, and they are not separated directly on that type, but on an instance of it: that is, there is a type B and, for each $1 \leq i \leq n$, an argument u_i of type $A_i[B/X]$ such that $tu_1 \ldots u_n \to_\beta^* \mathbf{0}$ and $t'u_1 \ldots u_n \to_\beta^* \mathbf{1}$.[5]

After the introduction of linear logic [5], the question of separation has been addressed also in proof theoretical frameworks. The first work on the subject is [6], where the authors deal with "pure proof-nets", a linear logical system corresponding to the pure λ-calculus. But it is only with Girard's work on ludics [7] that separation became a key property of proof theory, which may now be seen as a fundamental step in analyzing the structure of our representation of proofs.

There is a good reason why syntactical, interactive separation in the style of Böhm's theorem has taken so many years to shift from computer science to proof theory: the lack of results was essentially due to the absence of interesting logical systems where proofs could be represented in a "nice" canonical way. The only existing exception was natural deduction for minimal logic which, being isomorphic to the simply typed λ-calculus, had already been fully covered by Friedman and Statman's results.

In linear logic, canonical representations of proofs do exist, under the form of directed graphs called *proof-nets* [5]. A key ingredient of proof-nets is to forget the context of logical rules (except for the so-called promotion rule), so as to allow a higher degree of parallelism in the representation of proofs, which becomes thus more canonical. The typical (and most fundamental) form of parallelism we refer to here is the one needed to obtain the associativity of deduction: from three lemmas proving that A implies B, B implies C, and C implies D, we should only obtain one proof that A implies D, even if there are two ways of composing the lemmas. This is true in proof-nets (as it is true in natural deduction), but is strikingly false in sequent calculus.

In recent years, Tortora de Falco studied the canonicity of linear logic proof-nets by addressing the question of faithfulness (injectivity) in coherent spaces (which is, as cited above, strictly related to syntactical separation). With the exception of certain subsystems of linear logic, this study yielded a series of negative results: coherent spaces are not in general a faithful model of proof-nets, and separation fails [8]. The problem lies in the exponential modalities of linear logic, and more precisely in their *uniform* behavior: during cut-elimination, if at some point there is the need for two proofs of the same exponential formula to be provided, the procedure always answers this need with two copies of *the same* proof. In an interactive setting, this corresponds to the environment giving the same answer to a program querying multiple times for the value of an argument.

[4] Actually Friedman and Statman proved the faithfulness of standard models of the simply typed λ-calculus; from those semantic results however one can easily infer the syntactical separation (see for example [4]).

[5] Here we are supposing that X is the only variable occurring in the type of t, t'. To consider a term of type A also as a term of type $A[B/X]$, for any formula B, is sometimes called "Statman's typical ambiguity".

A new, potentially very powerful tool for the analysis of linear logic proofs came from the work of Ehrhard and Regnier, which led to the introduction of *differential interaction nets* (DIN, [9]). Based on Lafont's interaction nets [10], DIN are a syntax corresponding to the semantical constructions defined by Ehrhard in his *finiteness spaces* [11]. This semantical interpretation models linear proofs with linear functions on certain topological vector spaces, on which one can define an operation of derivative. Non-linear proofs (i.e., proofs using exponential modalities) become analytic functions, in the sense that they can be arbitrarily approximated by the equivalent of a Taylor expansion, which becomes available thanks to the presence of a derivative operator.

In syntactical terms, these constructions take a very interesting form: they correspond to "symmetrizing" the exponential modalities, i.e., in the logical system arising from finiteness spaces the rules handling the two dual exponential modalities *of course*/*why not* are perfectly symmetrical (although the logic is not self-dual). What is equally interesting is that the "old" rules of linear logic exponentials are not lost: proof-nets can be encoded in DIN.

This paper considers the question of separation for DIN, giving a positive answer in Theorem 1: given two different normal nets, we find another (dual) net separating them, up to Statman's typical ambiguity. This separation is as meaningful as that of Böhm's theorem, as it implies the faithfulness of every denotational semantics of DIN (Corollary 1), so in particular of finiteness spaces themselves.

We then apply Theorem 1 to the framework of proof-nets, and show with a few examples that pairs of proof-nets which cannot be interactively distinguished can on the contrary be easily separated once encoded in DIN, by heavily exploiting the symmetry of DIN exponentials. This shows concretely one of the main insight provided by our work: separation in proof-nets fails because of the asymmetry of linear logic exponentials.

2 Differential Interaction Nets

Preliminaries. In what follows, the set of all permutations over n elements is denoted by $\mathfrak{S}_n$.

The formulas of propositional multiplicative exponential linear logic (**MELL**) are generated by the following grammar, where $X, X^\perp$ range over a denumerable set of propositional variables:

$$A, B ::= X \mid X^\perp \mid 1 \mid A \otimes B \mid \perp \mid A \parr B \mid !A \mid ?A.$$

Linear negation is defined through De Morgan laws:

$$\begin{array}{rcl} (X)^\perp = X^\perp & \qquad & (X^\perp)^\perp = X \\ (1)^\perp = \perp & & (\perp)^\perp = 1 \\ (A \otimes B)^\perp = A^\perp \parr B^\perp & & (A \parr B)^\perp = A^\perp \otimes B^\perp \\ (!A)^\perp = ?A^\perp & & (?A)^\perp = !A^\perp \end{array}$$

Lists of occurrences of formulas will be ranged over by Γ, Δ, Σ. If $\Gamma = A_1, \ldots, A_n$, we shall denote by $\Gamma^\perp$ the list $A_1^\perp, \ldots, A_n^\perp$.

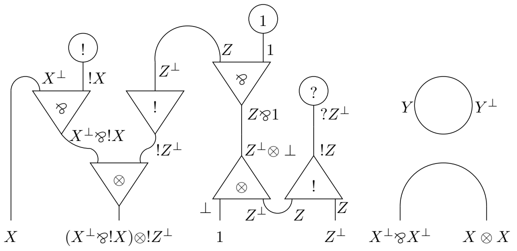


Fig. 1. A simple net.

Differential Interaction Nets. Differential interaction nets are defined on top of simple nets, which are particular interaction nets [10]. Here we give an informal definition; for a more detailed one, see [12].

A *simple net* is a set of *cells* and *wires*, graphically represented as in Fig. 1. Each cell has a *type*, which is a **MELL** connective, i.e., a symbol belonging to the set $\{1, \otimes, \perp, \parr, !, ?\}$, and a number of *ports*, exactly one of which is called *principal*, while the others (if any) are called *auxiliary*. The arity of a cell is equal to the number of its auxiliary ports; cells of type 1 and $\perp$ are required to be nullary, and those of type $\otimes$ and $\parr$ must be binary. Graphically, the principal port of a non-nullary cell is seen as one of the "tips" of the triangle representing it, while a nullary cell is represented by a circle.

A wire is represented as. . . a wire; the extremities of wires not connected to anything are called *free ports* of the net. For example, the net in Fig. 1 has six free ports. In the case of cyclic wires like the one at the top-right of Fig. 1, which are called *deadlocks*, we stipulate that there are two wires connecting the same two *internal ports*. Hence, there are four kinds of ports: principal, auxiliary, free, and internal. A wire connecting two non-principal ports is said to be an *axiom*; a wire connecting two principal or internal ports is said to be a *cut*. Note that a wire may be an axiom and a cut at the same time; this is the case of deadlocks. Those wires that are neither axioms nor cuts are called *simple*.

Each port i has a *type* $T(i)$, which is a **MELL** formula. These types must satisfy the following:

- if i, j are connected by an axiom or a cut, then $T(i) = T(j)^\perp$;
- if i, j are connected by a simple wire, then $T(i) = T(j)$;
- if i_0 is the principal port of a cell of type 1, then $T(i_0) = 1$;
- if i_0 is the principal port of a cell of type $\otimes$, whose two auxiliary ports are i_1, i_2, then $T(i_0) = T(i_1) \otimes T(i_2)$;
- if i_0 is the principal port of a cell of type $\perp$, then $T(i_0) =\perp$;
- if i_0 is the principal port of a cell of type $\parr$, whose two auxiliary ports are i_1, i_2, then $T(i_0) = T(i_1) \parr T(i_2)$;
- if i_0 is the principal port of a cell of type !, whose auxiliary ports are $i_1, \ldots, i_n$, then $T(i_1) = \cdots = T(i_n) = A$, and $T(i_0) = !A$;

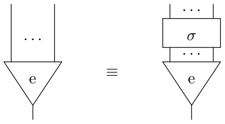
- if i_0 is the principal port of a cell of type ?, whose auxiliary ports are $i_1, \ldots, i_n$, then $T(i_1) = \cdots = T(i_n) = A$, and $T(i_0) = ?A$;

If a simple net α has n free ports, we assume that they are numbered by the integers $1, \ldots, n$, so that p_k is the kth free port. Then, we refer to the list of occurrences of formulas $T(p_1), \ldots, T(p_n)$ as the *conclusions* of α.

The empty simple net will be denoted by $\mathbf{1}$.

We now introduce a fundamental equivalence on simple nets, accounting for the fact that the auxiliary ports of exponential cells are unordered:

Definition 1 (σ-equivalence). *We define σ-equivalence, denoted by $\equiv$, as the contextual, reflexive-transitive closure of the following unoriented equation:*



where σ is a generic permutation, and the symbol e *stands for either* ! *or* ?.

Unless otherwise stated, simple nets will be considered modulo $\equiv$, i.e., whenever we refer to "the simple net α", we actually mean "the σ-equivalence class containing α".

Definition 2 (Differential interaction net). *A* differential interaction net*, or, more simply, a* net*, is a denumerable set of σ-equivalence classes of simple nets with the same conclusions Γ, which are also said to be the conclusions of the net. Nets will be ranged over by μ, ν. The empty net $\emptyset$, which can be considered to have any conclusions (including none), will be denoted by* $\mathbf{0}$.

Definition 3 (Composition). *Let α and β be two simple nets with resp. conclusions Δ, Γ and $\Gamma^\perp, \Sigma$. We denote by $\langle \alpha \,|\, \beta \rangle$ the simple net with conclusions Δ, Σ obtained by plugging each conclusion in Γ of α to the dual conclusion in $\Gamma^\perp$ of β. Similarly, if μ and ν are two nets with resp. conclusions Δ, Γ and $\Gamma^\perp, \Sigma$, we pose $\langle \mu \,|\, \nu \rangle = \{\langle \alpha \,|\, \beta \rangle \mid \alpha \in \mu, \beta \in \nu\}$, which is a net of conclusions Δ, Σ.*

In the sequel, we shall confuse a simple net α with the net $\{\alpha\}$ whenever this is not source of ambiguity. In particular, the net with no conclusions containing only the empty simple net, i.e. $\{\mathbf{1}\}$, will simply be denoted by $\mathbf{1}$.

Nets are provided with two rewriting relations, corresponding to **MELL** cut-elimination (β-reduction) and non-atomic axiom-elimination (η-expansion). On simple nets, these are the contextual closures of the rules resp. given in Fig. 2 and Fig. 3, and are resp. denoted by $\succ_\beta$ and $\succ_\eta$.

The two topmost rules of Fig. 2 are called *multiplicative*; the bottom rule is called *exponential.* In all rules, a simple net reduces to a net; in the multiplicative cases, the right member must be seen as a singleton. In the exponential case, if the arities of the two interacting cells do not match, the rule yields the empty

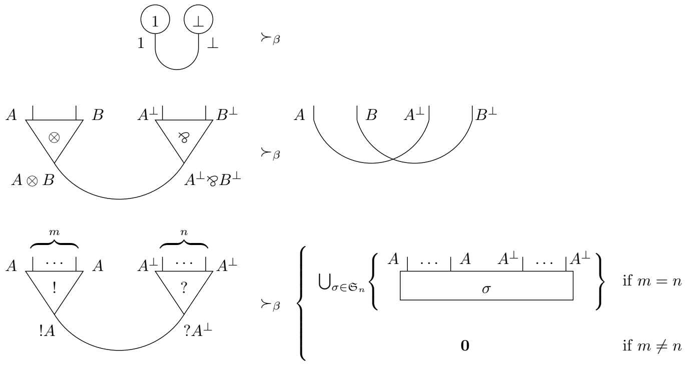


Fig. 2. Cut-elimination rules (β-reduction).

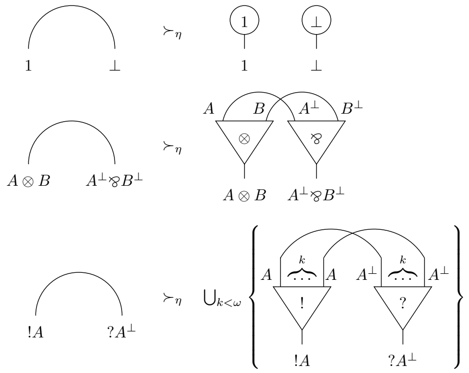


Fig. 3. Non-atomic axiom-elimination rules (η-expansion).

net; in case the arities match, the rule yields a net containing all simple nets obtained by connecting in all possible ways the auxiliary ports of the two cells.

Similarly, the topmost two rules of Fig. 3 are called multiplicative, and the bottom rule exponential. These rules also yield a net out of a simple net, with the right member of the multiplicative rules equal to a singleton. In the exponential rule, an axiom is replaced by its expansions using all possible arities for exponential cells.

Definition 4 (β-reduction and η-expansion). *We define the relation $\to_\beta$ on nets as follows: $\mu \to_\beta \mu'$ iff*

$$\mu' = \bigcup_{\alpha \in \mu} \nu_\alpha,$$

where $\alpha \succ_\beta \nu_\alpha$ or $\nu_\alpha = \{\alpha\}$, and $\alpha \succ_\beta \nu_\alpha$ for at least one $\alpha \in \mu$. The relation $\to_\eta$ is defined similarly, with $\succ_\eta$ instead of $\succ_\beta$. We pose $\to \; = \; \to_\beta \cup \to_\eta$, and we say that a net μ is normal *iff it contains no deadlock and there is no μ' such* *that $\mu \to \mu'$. A net μ is* normalizable *iff there exists a normal net ν such that $\mu \to^* \nu$.*

Proposition 1 (Confluence). *The relation $\to^*$ is confluent. Hence, a normalizable net has a unique normal form.*

Proof. Actually $\to^*$ is strongly confluent: if $\mu \to \mu', \mu''$ with $\mu' \neq \mu''$, then there exists ν s.t. $\mu', \mu'' \to^* \nu$ in at most one step. □

Observe that, if μ is finite, then every μ' such that $\mu \to_\beta \mu'$ is also finite. The finiteness of μ implies that there exists a non-negative integer $\sharp\mu$ which is the maximum number of cells contained in the simple nets of μ admitting a β-reduction. By simply inspecting Fig. 2, we see that $\sharp\mu' < \sharp\mu$, so every finite net is strongly β-normalizing.

However, strong normalization fails in general, even if we ignore deadlocks (which of course are not normalizable).[6] In fact, for each non-negative integer k, it is easy to find a simple net α_k such that $\{\alpha_k\}$ reduces to a normal net in at least k steps. Then, the net $\bigcup_{k<\omega}\{\alpha_k\}$ obviously has no normal form.

Differences with respect to Ehrhard-Regnier's presentation. There are two notable differences with respect to the definition of DIN given in [9].
(i) We consider generalized exponential cells, corresponding in [9] to trees of binary (co)contraction cells with (co)dereliction and (co)weakening cells on the leaves, modulo associativity, commutativity, and neutrality of (co)weakening. This is so-called *nouvelle syntaxe* [13], and provides more canonical nets. In fact, only commutativity needs to be explicitly treated in our framework (through σ-equivalence); associativity and neutrality are built-in.
(ii) In [9] nets are defined as *finite* sets of simple nets. The need to consider infinite nets is a consequence of (i), which forbids a conclusion of an axiom to be (co)contracted. In our syntax, such configurations are represented unsing η-expansion, which yields infinite nets in the exponential case. Additionally, infinite nets are required if one wants to consider the Taylor-Ehrhard expansion of proof-nets, as we do in Sect. 4.

3 The Separation Theorem

In this section, we fix a single propositional variable X, and consider only formulas built on the dual pair $X, X^\perp$. Everything we say can of course be generalized to types containing arbitrary atoms.

Let μ be a net with conclusions Γ and let A be a formula. We denote by $\mu[A/X]$ the net with conclusions $\Gamma[A/X]$ obtained from μ by substituting each occurrence of X with A.

Our main result is the following one:

[6] By the way, there are geometrical conditions, known as *correctness criteria* [9], which prevent a net satisfying them from producing deadlocks.

Theorem 1 (Separation). *For each pair of different normal nets μ, μ' with same conclusions Γ, there is a simple net ν with conclusions $\Gamma[?1/X]^{\perp}$ s.t. $\langle \nu \mid \mu[?1/X] \rangle \rightarrow_{\beta}^{*} \mathbf{1}$ and $\langle \nu \mid \mu'[?1/X] \rangle \rightarrow_{\beta}^{*} \mathbf{0}$, or vice versa.*

We remark that the use of multiplicative units is only a convenience: Theorem 1 also holds in their absence, using a formula of the form $?!A$ instead of $?1$, where A is arbitrary (for example X itself).

We now proceed with the proof of Theorem 1. First of all, in case Γ is empty (i.e., μ, μ' have no conclusion), then by definition of normal net, either $\mu = \mu'$ or $\mu = \mathbf{1}$ and $\mu' = \mathbf{0}$. Otherwise, observe that if two normal nets μ, μ' are different, then there is a simple net α in one of them which is different from every simple net in the other one; to separate μ and μ' we shall define a (simple) net ν which has the property of reducing to $\mathbf{1}$ when applied to α, and to $\mathbf{0}$ in all other cases (see Definition 6 and Lemma 1). To do this properly, we need to be careful because nets are defined as sets of σ-equivalence classes, which unfortunately do not have canonical representatives. Therefore, in the rest of the section, α will denote an actual simple net, and we may have $\alpha \neq \alpha'$ without having $\alpha \not\equiv \alpha'$.

We define a *wiring* to be a simple net containing no cells and no deadlock. Wirings will be ranged over by ω, and are said to be *atomic* if their conclusions are all atomic. If A is a formula, a *tree* of root A is a simple net defined by induction on A:

- if A is atomic, then the only tree of root A is a wire of conclusions $A^{\perp}, A$;
- if $A = 1$ (resp. $A = \perp$), then the only tree of root A consists of a single cell of type 1 (resp. $\perp$);
- if $A = A_1 \otimes A_2$ (resp. $A = A_1 \invamp A_2$), and τ_1, τ_2 are two trees of resp. roots A_1 and A_2, then the net obtained by plugging the roots of τ_1 and τ_2 to the auxiliary ports of a cell of type $\otimes$ (resp. $\invamp$) is a tree of root A;
- if $A = !B$ (resp. $A = ?B$), and $\tau_1, \ldots, \tau_n$ are trees of root B ($n \in \mathbb{N}$), then the net obtained by plugging the roots of each τ_i to the auxiliary ports of a cell of type $!$ (resp. $?$) is a tree of root A.

The perfect symmetry of DIN cells allows the following definition, which is a crucial point in the proof of Theorem 1:

Definition 5 (Mirror tree). *Let τ be a tree of root A. The* mirror tree *of τ, denoted by $\tau^{\perp}$, is the tree of root $A^{\perp}$ obtained from $\tau[X^{\perp}/X]$ by substituting each cell with one of dual type (i.e. $1 \leftrightarrow \perp$, $\otimes \leftrightarrow \invamp$, $! \leftrightarrow ?$).*

Definition 6 (Antagonist). *Let α be a normal simple net of conclusions $C_1, \ldots, C_n$. It is not hard to see that α can be decomposed in terms of an atomic wiring ω and n trees $\tau_1, \ldots, \tau_n$ as in Fig. 4a. Then, we say that a normal simple net $\alpha^{\dagger}$ of conclusions $C_1[?1/X]^{\perp}, \ldots, C_n[?1/X]^{\perp}$ is an* antagonist *of α iff $\alpha^{\dagger}$ is built as follows. First of all, fix two enumerations $0, \ldots, k$ of the conclusions of ω of type X and of the conclusions of type $X^{\perp}$. We write $\omega(i) = j$ iff the ith occurrence of X is connected to the jth occurrence of $X^{\perp}$ in ω. These enumerations induce two enumerations of the leaves of the forest $\varphi = \tau_1^{\perp}, \ldots, \tau_n^{\perp}$ (the*

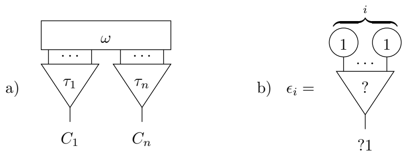


Fig. 4. a) Decomposition of a normal simple net. b) Definition of the net ϵ_i, $i \in \mathbb{N}$.

comma here denotes the juxtaposition of two simple nets). Then, $\alpha^\dagger$ is equal to $\varphi[?1/X]$ in which, for all $i \in \{0, \ldots, k\}$, the net ϵ_i is plugged to the leaf i, and the net $\epsilon_i^\perp$ is plugged to the leaf $\omega(i)$, where ϵ_i is defined in Fig. 4b.

Observe that, in the decomposition of Fig. 4a, ω may as well be empty; in that case, α is a forest $\tau_1, \ldots, \tau_n$, and its only antagonist is $\tau_1^\perp, \ldots, \tau_n^\perp$.

Lemma 1. *Let α be a normal simple net of conclusions $C_1, \ldots, C_n$, let $\alpha^\dagger$ be a simple net σ-equivalent to an antagonist of α, and let α' be a normal simple net with the same conclusions as α. Then:*

1. *$\alpha \equiv \alpha'$ implies $\langle \alpha^\dagger \,|\, \alpha'[?1/X] \rangle \to_\beta^* \mathbf{1}$;*
2. *$\alpha \not\equiv \alpha'$ implies $\langle \alpha^\dagger \,|\, \alpha'[?1/X] \rangle \to_\beta^* \mathbf{0}$.*

Proof. By induction on the number of cells in α. If α is a wiring, then it must be atomic, so α' is also an atomic wiring. In that case, $\alpha^\dagger$ is an antagonist of α, $\alpha \equiv \alpha'$ iff $\alpha = \alpha'$, and it is then easy to prove points 1 and 2 of the lemma. If α has a cell, then one of its conclusions must be connected to the principal port of a cell c, because α is normal. We can suppose w.l.o.g. this conclusion to be C_1. The proof splits into six cases, depending on the type of c. We consider only the case in which c is of type !, the ? case being perfectly symmetrical and the other cases being easier.

So we have $C_1 = !A$. This also means that the corresponding conclusion of α' is connected to the principal port of a cell c' of type ! (recall that α' is η-normal). If the arity of c' is different than that of c, then $\alpha' \not\equiv \alpha$ and we immediately have $\langle \alpha^\dagger \,|\, \alpha' \rangle \to_\beta^* \mathbf{0}$. So suppose that c and c' have same arity k. Let α_0 (resp. α_0') be the simple net obtained from α (resp. α') by removing c (resp. c'). Observe that the conclusions of α_0 (as those of α_0') are $A^1, \ldots, A^k, C_2, \ldots, C_n$, where $A^1, \ldots, A^k$ are occurrences of the same formula A and correspond to the type of the auxiliary ports of c and c'. In $\langle \alpha^\dagger \,|\, \alpha' \rangle$ we have a cut between c' and a cell $c^\dagger$ of type ?, which is also of arity k. By reducing this cut, we obtain

$$\langle \alpha^\dagger \,|\, \alpha' \rangle \to_\beta \{\langle \delta \,|\, \gamma \rangle \ ; \ \gamma \in P\},$$

where δ is obtained from $\alpha^\dagger$ by removing the cell $c^\dagger$, and P is the set of all simple nets obtained from α_0' by permuting the conclusions $A^1, \ldots, A^k$. Each $\gamma \in P$ has the same conclusions as α_0, so P can be partitioned into $P_{\mathbf{0}} = \{\gamma \in P \ ; \ \gamma \not\equiv \alpha_0\}$ and $P_{\mathbf{1}} = \{\gamma \in P \ ; \ \gamma \equiv \alpha_0\}$. Now, it is possible that δ is not σ-equivalent to an antagonist of α_0: this may be because $\alpha^\dagger$ is σ-equivalent to an antagonist of α thanks to a permutation $\sigma \in \mathfrak{S}_k$ on the auxiliary ports of $c^\dagger$. But in that case one can always include this permutation in the ones generated by the β-reduction ($\mathfrak{S}_k$ is a group, so $\sigma\mathfrak{S}_k = \mathfrak{S}_k$), so that actually δ can always be considered to be σ-equivalent to an antagonist of α_0. This latter contains strictly fewer cells than α, so by induction hypothesis $\langle \delta \,|\, \gamma \rangle \to_\beta^* \mu$ iff $\gamma \in P_\mu$, where $\mu \in \{\mathbf{0}, \mathbf{1}\}$. But $\alpha \equiv \alpha'$ iff $P_{\mathbf{1}} \neq \emptyset$, hence the lemma holds. □

We can now conclude the proof of Theorem 1. Take two different normal nets μ, μ'. As remarked above, we can assume w.l.o.g. that μ contains a σ-equivalence class not contained in μ'. Take any representative α of this equivalence class, and define ν to be the net containing only the equivalence class of an antagonist of α. By Lemma 1, we have $\langle \nu \,|\, \mu[?1/X] \rangle \to_\beta^* \mathbf{1}$, while $\langle \nu \,|\, \mu'[?1/X] \rangle \to_\beta^* \mathbf{0}$.

3.1 An Application: Faithfulness

A denotational semantics $\mathfrak{M}$ of DIN is a $*$-autonomous category with some additional structure (refer to [14] for the details) interpreting **MELL** formulas as objects and nets as morphisms. More precisely, having associated with the variable X an object $\mathcal{X}$, then $\mathfrak{M}$ associates with each **MELL** formula A an object $[\![A]\!]_\mathcal{X}$ and with each net μ of conclusions $C_1, \ldots, C_n$ (for $n \geq 0$) a morphism $[\![\mu]\!]_\mathcal{X}$ from $[\![1]\!]_\mathcal{X} = I$ (the identity object of the monoidal structure) to $[\![C_1 ⅋ \ldots ⅋ C_n]\!]_\mathcal{X}$, in such a way that:

composition: $[\![\langle \mu \,|\, \nu \rangle]\!]_\mathcal{X} = [\![\mu]\!]_\mathcal{X} \circ [\![\nu]\!]_\mathcal{X}$.[7]
invariance: if $\mu \to \mu'$ then $[\![\mu]\!]_\mathcal{X} = [\![\mu']\!]_\mathcal{X}$.

A semantics is faithful (or injective, see [8]) if for any two distinct normal nets μ, μ', there is an object $\mathcal{X}$, s.t. $[\![\mu]\!]_\mathcal{X} \neq [\![\mu']\!]_\mathcal{X}$. A notable corollary of Theorem 1 is the faithfulness of every non-trivial denotational semantics (for example Ehrhard's *finiteness spaces*, introduced in [11]).

Corollary 1 (Faithfulness). *Let $\mathfrak{M}$ be a denotational semantics for DIN. If there exist two distinct normal nets μ, μ' s.t. for every object $\mathcal{X}$, $[\![\mu]\!]_\mathcal{X} = [\![\mu']\!]_\mathcal{X}$, then the semantics is trivial, i.e., for every object $\mathcal{X}$, for every net ν, $[\![\nu]\!]_\mathcal{X} = [\![\mathbf{0}]\!]_\mathcal{X}$.*

Proof. Suppose that for every object $\mathcal{X}$, $[\![\mu]\!]_\mathcal{X} = [\![\mu']\!]_\mathcal{X}$. By Theorem 1, there is a simple net α such that $\langle \{\alpha\} \,|\, \mu[?1/X] \rangle \to_\beta^* \mathbf{1}$ and $\langle \{\alpha\} \,|\, \mu'[?1/X] \rangle \to_\beta^* \mathbf{0}$. Now let ν be a net and consider the net $\nu\alpha$ obtained by juxtaposing α to each simple net of ν. Remark that $\langle \nu\alpha \,|\, \mu[?1/X] \rangle \to_\beta \nu$ and $\langle \nu\alpha \,|\, \mu'[?1/X] \rangle \to_\beta \mathbf{0}$. By hypothesis we have that, for every object $\mathcal{X}$, $[\![\mu[?1/X]]\!]_\mathcal{X} = [\![\mu'[?1/X]]\!]_\mathcal{X}$, hence by composition $[\![\langle \mu[?1/X] \,|\, \nu\alpha \rangle]\!]_\mathcal{X} = [\![\langle \mu'[?1/X] \,|\, \nu\alpha \rangle]\!]_\mathcal{X}$, and finally by invariance $[\![\nu]\!]_\mathcal{X} = [\![\mathbf{0}]\!]_\mathcal{X}$. □

[7] Here we are implicitly exploiting the $*$-autonomous structure of the category: a morphism of type $I \to [\![\Delta]\!] ⅋ [\![\Gamma]\!]$ and a morphism of type $I \to [\![\Gamma^\perp]\!] ⅋ [\![\Sigma]\!]$ can be seen resp. as morphisms of type $[\![\Delta^\perp]\!] \to [\![\Gamma]\!]$ and $[\![\Gamma]\!] \to [\![\Sigma]\!]$, so it makes sense to compose them.

4 Proof-nets in DIN

We shall now apply Theorem 1 to the framework of proof-nets, and show a few examples of interactively indistinguishable proof-nets which can be easily separated once encoded in DIN.

Our definition of **MELL** proof-nets follows closely that of Danos and Regnier [15]:

Definition 7 (Proof-net). *A* proof-net *is a simple net containing only multiplicative cells, arbitrary* ? *cells, and unary* ! *cells (which are called* promotion cells *in the context of proof-nets), and satisfying the following conditions:*

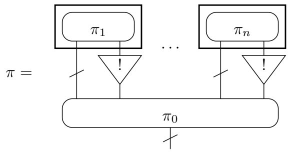
boxing condition: *each promotion cell c has an associated subnet $\mathcal{B}$, called a* !-box*, such that one conclusion of $\mathcal{B}$, called* principal door*, is connected to the auxiliary port of c, and all the other conclusions, called* auxiliary doors*, are connected to auxiliary ports of* ? *cells. Moreover, two* !*-boxes must either be disjoint, or included one in the other. In graphical representations,* !*-boxes will be drawn as rectangular frames.*

sequentialization condition: *the net must be defined inductively as follows: the empty net is a proof-net; a wire, a $\perp$ or* 1 *cell are proof-nets; the graph obtained from a proof-net π by adding a $\parr$ or* ? *cell with auxiliary ports conclusions of π is a proof-net; the graph obtained from two proof-nets π_1, π_2 by juxtaposing them, or by linking a conclusion of π_1 and one of π_2 by a wire or by a $\otimes$ cell, is a proof-net; if a proof-net π has conclusions $A, ?C_1, \ldots, ?C_n$, then the graph obtained from π by adding a* ! *cell with auxiliary port the conclusion A, and whose associated* !*-box is the (maximal) subnet of π not containing the* ? *cells with conclusions $?C_1, \ldots, ?C_n$, is a proof-net.*

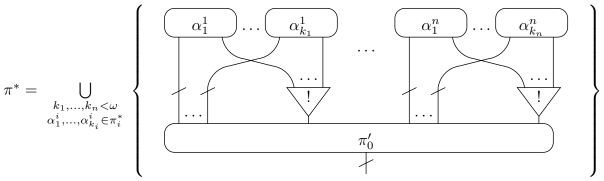
If π is a proof-net, the depth *of a cell of π is the number of nested* !*-boxes in which it is contained. The depth of π, denoted by $\partial(\pi)$, is the maximum depth of its cells.*

A proof-net is not a simple net because it contains additional information, namely that carried by !-boxes. However, this additional information can be accommodated in DIN thanks to the Taylor-Ehrhard formula, which is the reformulation in terms of nets of the usual Taylor expansion of analytic functions around the origin [11].

Definition 8 (Taylor-Ehrhard expansion). *Let π be a proof-net of conclusions Γ. Its* Taylor-Ehrhard expansion *π^* is a net of conclusions Γ defined by induction on the depth of π: if $\partial(\pi) = 0$, then $\pi^* = \{\pi\}$; if $\partial(\pi) > 0$, then we have*



where π_0 contains no !-boxes. In the above picture, a wire with a diagonal stroke drawn across it represents an arbitrary number of wires (possibly zero). Then, we set


$\pi^* = \bigcup_{\substack{k_1,\dots,k_n<\omega \\ \alpha_1^i,\dots,\alpha_{k_i}^i \in \pi_i^*}}$
α_1^1
$\alpha_{k_1}^1$
α_1^n
$\alpha_{k_n}^n$
!
!
π_0'

where π_0' is obtained as follows: by the boxing condition (Definition 7), each conclusion of π_i which is not connected to the auxiliary port of a promotion cell must be connected to an auxiliary port of a ? cell c in π_0. Then, π_0' is obtained from π_0 by changing the arity of such cells c as follows: if the arity of c is $k+1$ in π_0, then it becomes $k+k_i$ in π_0'.

Cut-elimination is defined exactly as in Fig. 2, except for exponential cuts. In these cuts !-boxes play a crucial role, since they delimit subnets to be erased or duplicated as a whole in one step. Fig. 5 defines exponential cut-elimination for proof-nets: what happens is that the !-box dispatches n copies of π_1 ($n \geq 0$ being the arity of ? cell shown) inside the !-boxes (if any) crossed by the auxiliary doors of the ? cell.

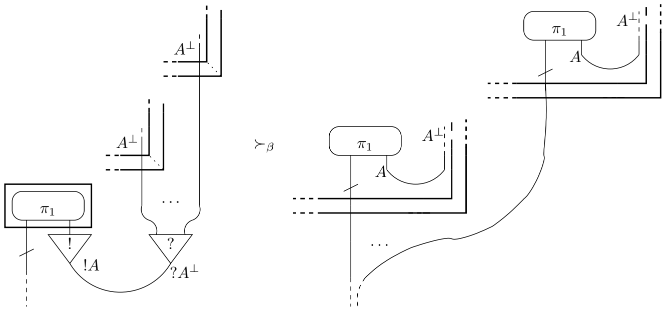


Fig. 5. Cut-elimination rule for promotion.

The Taylor-Ehrhard expansion preserves **MELL** reductions on proof-nets, in the sense given by the following proposition:

Proposition 2 (Simulation). *Let π_1 (resp. π_2) be a normal proof-net of conclusions A, Γ (resp. $A^\perp, \Delta$). If $\langle \pi_1 \mid \pi_2 \rangle \to_\beta^* \pi_3$, then $\langle \pi_1^* \mid \pi_2^* \rangle \to_\beta^* \pi_3^*$.*

Proof. It is enough to prove that, given a generic proof-net π, if $\pi \to_\beta \pi'$ by reducing a cut at depth 0, then $\pi^* \to_\beta \pi'^*$. We omit the details. □

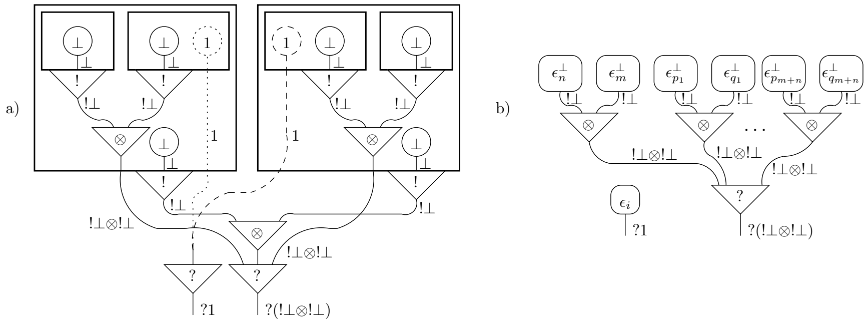


Fig. 6. a) Example 1 of non-separable proof-nets: π_1 is defined by considering the dotted wire and cell, instead π_2 by considering the dashed ones. b) Definition of $\alpha\langle i, n, m, p_1, q_1, \ldots, p_{n+m}, q_{n+m}\rangle$, where ϵ_i is the simple net of Fig. 4b.

Coherent spaces provide the most classical denotational semantics for proof-nets (see [5]). Lorenzo Tortora de Falco proves in [8] that this semantics fails to be faithful: there are distinct normal proof-nets which are associated with the same morphism, for any interpretation of the variables. We reproduce in Fig. 6a and in Fig. 7a two examples of pairs of non-separable proof-nets. This means that **MELL** proof-nets cannot verify the separation property, at least in the strong form of Theorem 1, as this would contradict Corollary 1 (which would hold also for **MELL** in that case).

The example of Fig. 6a morally[8] corresponds to the following PCF terms:

$$\lambda x.\texttt{if}\,x\,\texttt{then}\,(\texttt{if}\,x\,\texttt{then}\,\texttt{false}\,\texttt{else}\,\frac{\texttt{true}}{\texttt{false}})\,\texttt{else}\,(\texttt{if}\,x\,\texttt{then}\,\frac{\texttt{false}}{\texttt{true}}\,\texttt{else}\,\texttt{false})$$

where the term corresponding to π_1 is obtained by choosing `true` from $\frac{\texttt{true}}{\texttt{false}}$ and `false` from $\frac{\texttt{false}}{\texttt{true}}$, while π_2 by making the opposite choices. It is well-known that this two terms are indistinguishable also in PCF, since the nested `if then else` have all the same argument x (corresponding to the ? cell of conclusion ?(!⊥⊗!⊥) in Fig. 6a).

The example of Fig. 7a is reported[9] in [8]. Notice that this example does not use promotion: the proof-nets of Fig. 7a are already simple nets, i.e. $\pi_i^* = \pi_i$. The problem of proof-net separation therefore lies in the contraction rule, and not in the exponential box.

Although the examples of Fig. 6a and Fig. 7a are not separable in **MELL** proof-nets, they become easily separable when translated in DIN. Let us start with the proof-nets π_1, π_2 defined in Fig. 6a. Their Taylor-Ehrhard expansions

[8] We cheated a bit in order to have simpler proof-nets. The exact proof-nets should use additives and have conclusions $?(\perp \& \perp), 1 \oplus 1$.

[9] To be pedantic, the example we show here is a slight simplification of that defined in [8], since we are using units and mix.

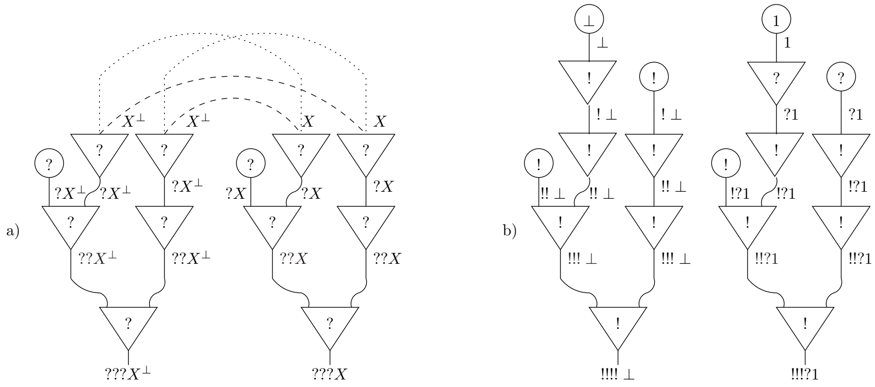


Fig. 7. a) Example 2 of non-separable proof-nets: π_1 is defined by considering the dashed wires, instead π_2 by considering the dotted ones. b) Simple net separating π_1^*, π_2^* of a)

in DIN are:

$$\pi_1^* = \left\{ \alpha \langle i, n, m, p_1, q_1, \ldots, p_{n+m}, q_{n+m} \rangle \mid i = \textstyle\sum_{j=1}^{n} q_j \right\}$$

$$\pi_2^* = \left\{ \alpha \langle i, n, m, p_1, q_1, \ldots, p_{n+m}, q_{n+m} \rangle \mid i = \textstyle\sum_{j=n+1}^{n+m} p_j \right\}$$

where $\alpha \langle i, n, m, p_1, q_1, \ldots, p_{n+m}, q_{n+m} \rangle$ is the simple net defined in Fig. 6b, and n, m, p_j, q_j range over all non-negative integers.

An example of separating simple net is $\alpha^\perp \langle 2, 1, 0, 0, 2 \rangle$. In fact, we have $\langle \pi_1^* \mid \alpha^\perp \langle 2, 1, 0, 0, 2 \rangle \rangle \rightarrow_\beta^* \mathbf{1}$ and $\langle \pi_2^* \mid \alpha^\perp \langle 2, 1, 0, 0, 2 \rangle \rangle \rightarrow_\beta^* \mathbf{0}$.

Let us turn to π_1, π_2 as defined in Fig. 7a. Let α be the simple net of Fig. 7b; we have $\langle \pi_1[?1/X] \mid \alpha \rangle \rightarrow_\beta^* \mathbf{1}$ and $\langle \pi_2[?1/X] \mid \alpha \rangle \rightarrow_\beta^* \mathbf{0}$.

Observe that both examples are separable by means of simple nets which make a crucial use of ! cells of arity different (in particular, higher) than 1, which are exactly the cells not allowed in **MELL** proof-nets.

5 Concluding Remarks

Faithfulness of relational semantics. It is known that in general a denotational semantics for **MELL** does not provide a semantics for DIN: for example, coherent semantics does not interpret cocontraction (i.e., ! cells of arity higher than 1).

On the other hand, any denotational semantics of DIN provides a semantics for **MELL** through the Taylor-Ehrhard expansion: given a proof-net π, one can define $[\![\pi]\!]$ as $[\![\pi^*]\!]$.[10]

[10] This is possible only if one considers DIN modulo commutativity of exponential cells, as we do with our σ-equivalence. For a more detailed discussion of the link between DIN and linear logic denotational semantics see [14].

An immediate consequence of our result is that any semantics of DIN separates any two proof-nets with different Taylor-Ehrhard expansions. This sheds more light upon the faithfulness of relational semantics: a few years ago Tortora de Falco conjectured in [8] that such semantics is faithful for **MELL** proof-nets, a question which still waits to be settled. Since relational semantics is a semantics for DIN, we can reduce Tortora's conjecture to the question of whether different normal proof-nets have different Taylor-Ehrhard expansions.

$\lambda\mu$-calculus. The question of separation for the $\lambda\mu$-calculus has been addressed by David and Py in [16]. In that paper the authors produce two $\lambda\mu$-terms which are indistinguishable: the two terms are a variant of the nested `if then else` analyzed in the example of Fig. 6a. Very recently Lionel Vaux has introduced in [17] a differential extension of the $\lambda\mu$-calculus: in such extension, it is not hard to find a term separating David and Py's terms in exactly the same way as we did for separating the two proof-nets of Fig. 6a. It is then likely that a separation result similar to Theorem 1 holds for Vaux's extension of the $\lambda\mu$-calculus.

References

1. Böhm, C.: Alcune proprietà delle forme $\beta\eta$-normali nel λ-K-calcolo. Pubblicazioni dell'IAC **696** (1968) 1–19
2. Friedman, H.: Equality between functionals. In: Proceedings of LC 72-73. Volume 453 of Lecture Notes in Math. (1975) 22–37
3. Statman, R.: Completeness, invariance and λ-definability. J. Symbolic Logic (1983) 17–26
4. Joly, T.: Codages, séparabilité et représentation de fonctions en λ-calcul simplement typé et dans d'autres systèmes de types. Ph.D. Thesis, Université de Paris 7 (2000)
5. Girard, J.Y.: Linear logic. Theoret. Comput. Sci. **50** (1987) 1–102
6. Mascari, G., Pedicini, M.: Head linear reduction and pure proof net extraction. Theoret. Comput. Sci. **135** (1994) 111–137
7. Girard, J.Y.: Locus solum. Math. Struct. Comput. Sci. **11** (2001) 301–506
8. Tortora de Falco, L.: Obsessional experiments for linear logic proof-nets. Math. Struct. Comput. Sci. **13** (2003) 799–855
9. Ehrhard, T., Regnier, L.: Differential interaction nets. Theoret. Comput. Sci. **364** (2006) 166–195
10. Lafont, Y.: Interaction nets. In: POPL'90. (1990) 95–108
11. Ehrhard, T.: Finiteness spaces. Math. Struct. Comput. Sci. **15** (2005) 615–646
12. Mazza, D.: Interaction Nets: Semantics and Concurrent Extensions. Ph.D. Thesis, Universitée de la Méditerranée/Università degli Studi Roma Tre (2006)
13. Regnier, L.: Lambda-calcul et réseaux. Ph.D. Thesis, Université de Paris 7 (1992)
14. De Carvalho, D.: Sémantique de la logique linéaire et temps de calcul. Ph.D. Thesis, Université d'Aix-Marseille 2 (2007)
15. Danos, V., Regnier, L.: Proof nets and the Hilbert space. In: Advances in Linear Logic, Cambridge University Press (1995) 307–328
16. David, R., Py, W.: $\lambda\mu$-calculus and Böhm's theorem. J. Symbolic Logic **66** (2001) 407–413
17. Vaux, L.: The differential $\lambda\mu$-calculus. Theoret. Comput. Sci. **379** (2007) 166–209