# On Multiplicative Linear Logic, Modality and Quantum Circuits

Ugo Dal Lago
Università di Bologna & INRIA
dallago@cs.unibo.it

Claudia Faggian
CNRS & Université Denis-Diderot Paris 7
faggian@pps.jussieu.fr

A logical system derived from linear logic and called QMLL is introduced and shown able to capture all unitary quantum circuits. Conversely, any proof is shown to compute, through a concrete GoI interpretation, some quantum circuits. The system QMLL, which enjoys cut-elimination, is obtained by endowing multiplicative linear logic with a quantum modality.

## 1 Introduction

It's more and more clear that strong relationships exist between linear logic [5] and quantum computation. This seems to go well beyond the easy observation that the intrinsic resource-consciousness of linear logic copes well with the impossibility of cloning and erasing qubits. There are several different research directions in which this interaction has recently started to manifest itself. We like to mention the following:

- First of all, various lambda calculi for quantum computation have been introduced in the last ten years [14, 12, 13, 2]. The common denominator between the different proposals is precisely the use of linearity to control duplication and erasing: it is enforced either by typing or by structural constraints on the shape of lambda terms.
- Coherence spaces (the semantics from which linear logic originated) have been revisited by Girard [8], in an attempt to improve the understanding of the relations between quantum and logic, and to relate coherence spaces and quantum actions.
- Blute and Panangaden have recently shown how a simple calculus of Feynman's diagrams can give semantics to linear logic proof-nets [1].

Even with all these recent advances, we still lack a truly convincing correspondence between linear logic as a proof theory and quantum computation as a computational model. In particular, a quantum analogue of the Curry-Howard correspondence has not been defined yet, and the known attempts (e.g. [4]) have not any direct relationship with linearity in the sense of linear logic.

At a deeper level, a fundamental aspect of linear logic, which has not been exploited in a quantum setting yet, is its rooting into a mathematical model based on operator algebras, through the so-called geometry of interaction [6, 7, 3] (GoI in the following). The GoI program is that of a dynamic interpretation of computation as a flow of information circulating around a net; this is at the heart of linear logic from its beginnings. This flow of information can be formulated both as a classical, token-based interactive machine [10] or as an algebra of bounded operators on the infinite dimension Hilbert space [7], which is the canonical state space for quantum computation models like quantum Turing machines. We believe that this aspect is highly relevant to the logical approach to quantum computing, and has the potential for turning it into a powerful tool. Recently, GoI has been shown to be able to give semantics to Selinger and Valiron's quantum lambda calculus [11].

Bart Jacobs, Peter Selinger, and Bas Spitters (Eds.):
8th International Workshop on Quantum Physics and Logic (QPL 2011)
EPTCS 95, 2012, pp. 55–66, doi:10.4204/EPTCS.95.6

In this paper, we describe ongoing work about the relationships between quantum computation and linear logic and a first investigation on the underlying GoI. Some motivations and goals underlie and guide our investigation:

- we would like to get a model which is concrete, together with an efficient encoding; in our view, GoI should be able to give a concrete syntax (as is the case of linear logic), and should eventually be able to talk about the computational complexity of the calculus.
- we aim to have a proof-theoretical account of both quantum information and computation (i.e. quantum data and algorithms).

Specifically, in this paper we introduce a logical system, called QMLL, which is obtained by endowing multiplicative linear logic with quantum modalities; we then investigate in detail the relations between QMLL and quantum circuits. A key ingredient in the proof of this correspondence is an interactive abstract machine (in the sense of [3]) for the system, which is proved both to be a model of QMLL cut-elimination and to give a computational meaning to proofs. This concrete approach, and the close connection between circuits, logic and semantic models are an important difference with the current efforts in this direction. The results we have obtained are encouraging.

## 2 Proof-Nets, GoI, and Superposition

The geometry of interaction of a proof, as initially conceived by Girard [6, 7], is an operator on a Hilbert space $\ell^2$. As a matter of fact, however, the interpretation of linear logic proofs only makes use of a small fragment of the setting laid out in [7]. Fundamentally, the interpretation of a proof (at least in the multiplicative fragment) is just a permutation on a finite set. Our aim here is to enrich linear logic in such a way that a larger portion of the GoI semantic universe is actually exploited, this way going towards a calculus with quantum features. The design of QMLL has been guided by intuitions on what an hypothetical "quantum GoI" interpretation would look like.

In this section, we discuss some of the ideas which underlie GoI. The presentation is going to be very simplified; our purpose is to give an intuition rather than the formal details. For a more thorough presentation of GoI, we refer to [6], or to Girard's introductory notes [9]. We here focus our attention on multiplicative linear logic (MLL in the following), and moreover only to *cut-free* proofs.

**What is a MLL proof of $A$?** Let us consider the (cut-free) proof-nets of MLL, and make the assumption that all axioms are atomic. A cut-free proof of a formula $A$ with $n$ occurrences of atoms will be interpreted as an $n \times n$ matrix (since the dimension is finite, we identify operators and matrices). But how does a cut-free proof of a formula $A$ look like? Until we reach the axiom links, we have no freedom: in a proof-net, each formula is conclusion of a well-defined link, corresponding to the principal connective of the formula. In other words, a proof-net with conclusion $A$ is necessarily the disjoint union of two graphs:

- the formula tree $\mathsf{T}(A)$ of $A$ (whose leaves are the occurrences of atoms);
- axiom links connecting pairs of dual atoms.

All cut-free proofs of the same formula $A$ have the same formula tree. What characterizes each of them is the linking among the occurrences of atoms. *The atom links are hence enough to fully describe a cut-free MLL proof of $A$.*

As an example, let us consider the two cut-free proofs of the formula $B = (\alpha^\perp \parr \alpha^\perp) \parr (\alpha \otimes \alpha)$. By indexing different occurrences of the same atom or co-atom, we obtain $B = (\alpha_1^\perp \parr \alpha_2^\perp) \parr (\alpha_1 \otimes \alpha_2)$. The two proofs (let us call them $\pi$ and $\rho$) are in Figure 1 below. Both $\pi$ and $\rho$ have the same formula tree

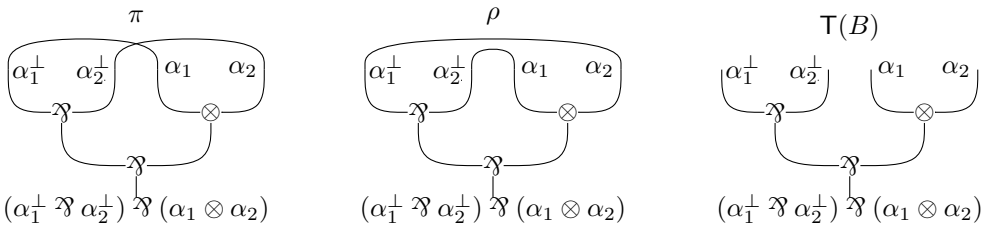



Figure 1: Two proofs of $B$ and its syntax three $\mathsf{T}(B)$

$\mathsf{T}(B)$. In the case of $\pi$, the axiom links are $\{\alpha_1^\perp, \alpha_1\}$ and $\{\alpha_2^\perp, \alpha_2\}$. In the case of $\rho$, the axioms links are $\{\alpha_1^\perp, \alpha_2\}$ and $\{\alpha_2^\perp, \alpha_1\}$.

A convenient way to describe the links among $n$ (occurrences of) atoms is by means of a $n \times n$ matrix, which can be seen as the adjacency matrix of the graph describing the axiom links, as the two graphs describing $\pi$ and $\rho$ in Figure 2. Since the axiom links describe the proof, this matrix itself is a faithful representation of the proof. Going back to our example, $\pi$ and $\rho$ can be easily seen to be described by

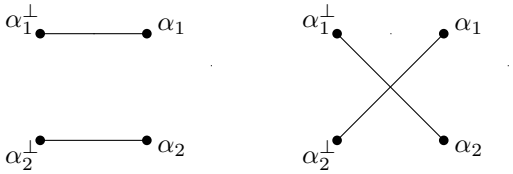



Figure 2: Axiom graphs for $\pi$ and $\rho$.

the following two matrices (once a suitable total order on atom and co-atom occurrences has been fixed):

$$M = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \qquad N = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

As a matter of fact, in this (simple, because the proofs are cut-free) case, $M$ is actually the GoI interpretation of $\pi$, while $N$ is the interpretation of $\rho$.

In general, the interpretation of a proof is defined by induction, starting from the interpretation of the axioms. For example, if $A$ is a formula with $n$ atoms, then the axiom $\vdash A, A^\perp$ is associated to the $2n \times 2n$ matrix

$$\begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}$$

where $I_n$ is the identity $n \times n$ matrix. We do not want to give more details here: the reader can find them clearly explained in [9], Section 19.3.

**Towards a quantum calculus.** A matrix which interprets a MLL proof is hermitian, because the links are undirected. It also has the following features: on the one hand it has exactly one non-null element per row and column, and on the other hand such an element is 1. In other words, the matrix is a permutation matrix. What if we relax these constraints? Let us work again with an example. Let us consider the

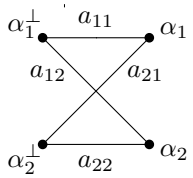
following $4 \times 4$ hermitian complex matrix $M$:

$$\begin{pmatrix} 0 & U \\ U^* & 0 \end{pmatrix}$$

where U is the following $2 \times 2$ *unitary* matrix.

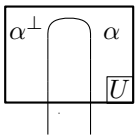
$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

If we have two copies $\alpha_1^\perp, \alpha_2^\perp$ of $\alpha^\perp$ and two copies $\alpha_1, \alpha_2$ of $\alpha$, we can see each non-zero coefficient $a_{ij}$ of $U$ as describing the existence of a link between the co-atom occurrence $\alpha_i^\perp$ and the atom occurrence $\alpha_j$; the link is weighted by the coefficient $a_{ij}$. Hence we read the matrix $M$ above as the interpretation of the following "weighted" set of axiom links:




We think of this set of links as being in "quantum superposition": we have the link $\{\alpha_1^\perp, \alpha_1\}$ with amplitude $a_{11}$, and the link $\{\alpha_1^\perp, \alpha_2\}$ with amplitude $a_{12}$.

Such a "generalized axiom" can be described in a compact way by providing a pair: an atomic axiom link and the unitary matrix $U$. The graph above, in other words, becomes the following proof




namely something like a "box", labeled with the unitary matrix $U$ and containing an axiom link. This is actually the idea beyond the $\mathsf{QR}_n$-rule, which characterizes our calculus QMLL with respect to ordinary, classical, MLL (see next section). More generally, an atomic axiom link and a unitary matrix $V = (a_{ij})$ on $\mathbb{C}^{2^n}$, describe a generalized axiom link, which consists in:

- $2^n$ occurrences of $\alpha^\perp$ and $2^n$ occurrences of $\alpha$;
- $2^{2n}$ links; the complex number $a_{ij}$ from $V$ describes the presence of a link with amplitude $a_{ij}$ from the occurrence $\alpha_i^\perp$ to the occurrence $\alpha_j$.

Logically, the intuition is that the rule $\mathsf{QR}_n$ produces $2^{2n}$ copies of the axiom link, which are in "quantum superposition". Actually, rule $\mathsf{QR}_n$ acts not only on axiom links, but on arbitrary proofs.

The operator-theoretic GoI interpretation of QMLL, as well as a formal development of a system of proof-nets for it, is not the object of this preliminary report; we postpone them to a follow-up paper. We briefly explained it here because these are the main inspiring ideas behind QMLL.

## 3 The Syntax of QMLL

Formulas of QMLL are generated by the following grammar:

$$A ::= \alpha \mid \alpha^\perp \mid A \parr A \mid A \otimes A \mid \boxdot A \mid \diamond A$$

In other words, QMLL's formulas are obtained by enriching the language of MLL with two unary modal connectives, namely $\boxdot$ and $\diamondsuit$, which are dual of each other. Linear negation can then be defined in the usual way, by setting $(\boxdot A)^\perp = \diamondsuit A^\perp$ and $(\diamondsuit A)^\perp = \boxdot A^\perp$. As an example, $(\boxdot(A \parr B))^\perp = \diamondsuit(A^\perp \otimes B^\perp)$. $\boxdot^n A$ is syntactic sugar for

$$\underbrace{\boxdot(\boxdot(\ldots\boxdot}_{n \text{ times}}(A)\ldots)).$$

Similarly for $\diamondsuit^n A$.

A *modal formula* is a formula in the form $\boxdot A$ or $\diamondsuit A$. We reserve the metavariables $Q, R$ to indicate modal formulas, and the metavariables $F, G$ to indicate formulas whose most-external connective is not a modality ($\boxdot$ or $\diamondsuit$).

QMLL will be given as a sequent calculus. *Sequents* have the form $\vdash \Gamma$, where $\Gamma, \Delta$ are finite multisets of formulas. $\mathbb{U}_n$ is the class of unitary operators from $\mathbb{C}^{2^n}$ to itself. We denote by $I_n$ the identity operator on $\mathbb{U}_n$. The following are the rules of QMLL.

$$\frac{}{\vdash A^\perp, A}\ \mathsf{A} \qquad \frac{\vdash \Gamma, A \quad \vdash \Delta, A^\perp}{\vdash \Gamma, \Delta}\ \mathsf{C} \qquad \frac{\vdash \Gamma, A, B}{\vdash \Gamma, A \parr B}\ \parr$$

$$\frac{\vdash \Gamma, A \quad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \otimes B}\ \otimes \qquad \frac{\vdash Q, R \quad U \in \mathbb{U}_n}{\vdash \diamondsuit^n Q, \boxdot^n R}\ \mathsf{MR}_n \qquad \frac{\vdash F, G \quad U \in \mathbb{U}_n}{\vdash \diamondsuit^n F, \boxdot^n G}\ \mathsf{RR}_n$$

The rules $\mathsf{MR}_n$ and $\mathsf{RR}_n$ are said to be *quantum rules*. Observe how the two quantum rules act exactly the same way on their premise, adding $n$ instances of the modalities $\boxdot$ and $\diamondsuit$ to each of the two formulas in it. The only difference is in the nature of those formulas, which are required to be modal formulas in $\mathsf{MR}_n$ and not modal formulas in $\mathsf{RR}_n$. In the following, $\mathsf{QR}_n$ stands for either $\mathsf{MR}_n$ or $\mathsf{RR}_n$.

A *proof* $\pi$ is, as usual, a tree built according to the rules above. Occurrences of quantum rules can be seen as *boxes*, similarly to what happens with exponential modalities, e.g., in MELL.

The *principal formulas* of an instance of a rule are the occurrences of formulas which are introduced (or cut) by the rule. Observe how any instance of $\mathsf{QR}_n$ has two principal formulas (and no other formula).

## 4 Cut Elimination

In this section, QMLL will be proved to enjoy cut-elimination. This will be carried out by giving an effective binary relation on proofs which allows to remove all instances of rule C from proofs.

Formally, the relation $\Longrightarrow$ on the space of QMLL proofs is defined by some *reduction rules*, which can be applied in any context:

- **Axiom Reduction.** Every time one of the premises of a cut-rule is an axiom, the cut is eliminated in the usual way, by means of the following reduction:

$$\dfrac{\Gamma, A \quad \dfrac{}{\vdash A^\perp, A}\ \mathsf{A}}{\vdash \Gamma, A}\ \mathsf{C} \Longrightarrow \vdash \Gamma, A$$

- **Multiplicative Principal Reduction.** The dual multiplicative connectives $\otimes$ and $\parr$ annihilate each other, as usual:

$$\dfrac{\dfrac{\vdash \Gamma, A \quad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \otimes B}\ \otimes \quad \dfrac{\vdash \Theta, A^\perp, B^\perp}{\vdash \Theta, A^\perp \parr B^\perp}\ \parr}{\vdash \Gamma, \Delta, \Theta}\ \mathsf{C} \Longrightarrow \dfrac{\vdash \Gamma, A \quad \dfrac{\vdash \Delta, B \quad \vdash \Theta, A^\perp, B^\perp}{\vdash \Delta, \Theta, A^\perp}\ \mathsf{C}}{\vdash \Gamma, \Delta, \Theta}\ \mathsf{C}$$

- **Quantum Principal Reduction.** This reduction can be performed when both cut-formulas are introduced by the rule $\mathsf{QR}_m$ (the arity $m$ being the same in both sides):

$$\dfrac{\dfrac{\vdash A,B \quad U\in\mathbb{U}_m}{\vdash \diamondsuit^m A,\boxdot^m B}\,\mathsf{QR}_m \quad \dfrac{\vdash B^\perp,C \quad V\in\mathbb{U}_m}{\vdash \diamondsuit^m B^\perp,\boxdot^m C}\,\mathsf{QR}_m}{\vdash \diamondsuit^m A,\boxdot^m C}\,\mathsf{C} \quad\Longrightarrow\quad \dfrac{\dfrac{\vdash A,B \quad \vdash B^\perp,C}{\vdash A,C}\,\mathsf{C} \quad U\cdot V\in\mathbb{U}_m}{\vdash \diamondsuit^m A,\boxdot^m C}\,\mathsf{QR}_m$$

- **Quantum $\eta$-Expansion.** Axioms introducing modal formulas can be $\eta$-expanded as follows:

$$\dfrac{}{\diamondsuit^n A^\perp,\boxdot^n A}\,\mathsf{A} \Longrightarrow \dfrac{\dfrac{}{\vdash A^\perp,A}\,\mathsf{A} \quad I_n\in\mathbb{U}_n}{\vdash \diamondsuit^n A^\perp,\boxdot^n A}\,\mathsf{QR}_n$$

- **Quantum Contraction.** Two successive applications of a quantum rule can be contracted:

$$\dfrac{\dfrac{\vdash A,B \quad U\in\mathbb{U}_k}{\diamondsuit^k A,\boxdot^k B}\,\mathsf{QR}_k \quad V\in\mathbb{U}_n}{\vdash \diamondsuit^{k+n} A,\boxdot^{k+n} B}\,\mathsf{QR}_n \Longrightarrow \dfrac{\vdash A,B \quad U\otimes V\in\mathbb{U}_{k+n}}{\vdash \diamondsuit^{k+n} A,\boxdot^{k+n} B}\,\mathsf{QR}_{k+n}$$

- **Commuting Reduction.** These three reduction rules allow us to lift up a cut whose principal formula is not introduced immediately over it:

$$\dfrac{\vdash \Gamma,A \quad \dfrac{\vdash \Delta,A^\perp,B,C}{\vdash \Delta,A^\perp,B\parr C}\,\parr}{\vdash \Gamma,\Delta,B\parr C}\,\mathsf{C} \Longrightarrow \dfrac{\dfrac{\vdash \Gamma,A \quad \vdash \Delta,A^\perp,B,C}{\vdash \Gamma,\Delta,B,C}\,\mathsf{C}}{\vdash \Gamma,\Delta,B\parr C}\,\parr$$

$$\dfrac{\vdash \Gamma,A \quad \dfrac{\vdash \Delta,A^\perp,B \quad \vdash \Theta,C}{\vdash \Delta,\Theta,A^\perp,B\otimes C}\,\otimes}{\vdash \Gamma,\Delta,\Theta,B\otimes C}\,\mathsf{C} \Longrightarrow \dfrac{\dfrac{\vdash \Gamma,A \quad \vdash \Delta,A^\perp,B}{\vdash \Gamma,\Delta,B}\,\mathsf{C} \quad \vdash \Theta,C}{\vdash \Gamma,\Delta,\Theta,B\otimes C}\,\otimes$$

$$\dfrac{\vdash \Gamma,A \quad \dfrac{\vdash \Delta,B \quad \vdash \Theta,A^\perp,C}{\vdash \Delta,\Theta,A^\perp,B\otimes C}\,\otimes}{\vdash \Gamma,\Delta,\Theta,B\otimes C}\,\mathsf{C} \Longrightarrow \dfrac{\dfrac{\vdash \Gamma,A \quad \vdash \Theta,A^\perp,C}{\vdash \Gamma,\Theta,C}\,\mathsf{C} \quad \vdash \Delta,B}{\vdash \Gamma,\Delta,\Theta,B\otimes C}\,\otimes$$

Let $\Longrightarrow^*$ be the reflexive and transitive closure of $\Longrightarrow$. A proof $\pi$ is *normal* if there is not any $\rho$ such that $\pi\Longrightarrow\rho$.

**Proposition 4.1** *Every normal proof is cut-free.*

**Proof.** We can prove that any proof $\pi$ containing a cut is not normal by induction on the structure of $\pi$. The only interesting case is the one when the last rule of $\pi$ is a cut and the two immediate sub-proofs are cut-free. All the other cases can be easily handled by way of the induction hypothesis. In other words, $\pi$ is

$$\dfrac{\rho:\vdash \Gamma,A \quad \sigma:\vdash \Delta,A^\perp}{\vdash \Gamma,\Delta}\,\mathsf{C}$$

where $\rho$ an $\sigma$ are cut-free. Now:

- If either $\rho$ or $\sigma$ is introduced by an axiom, $\pi$ is not normal, since an axiom reduction can be applied to it;
- If the last rule in $\rho$ is multiplicative, then:
  - If the principal formula of that rule is not $A$, then a commuting reduction can be applied to $\pi$.

- If the principal formula of that rule is precisely $A$, then consider the last rule of $\sigma$. If it is multiplicative and has principal formula $A^\perp$, then $\pi$ is not normal, because a multiplicative principal reduction can be applied to it. If it is multiplicative and has a principal formula in $\Delta$, then again $\pi$ is not normal, because a commuting reduction can be applied to it.
- If the last rule in $\sigma$ is multiplicative, then we can proceed as in the previous case;
- We can then assume that $\pi$ has the following form:

$$\dfrac{\dfrac{\xi : \vdash A, B}{\vdash \diamondsuit^m A, \boxdot^m B}\ \mathsf{QR}_m \qquad \dfrac{\mu : \vdash C, D}{\vdash \diamondsuit^n C, \boxdot^n D}\ \mathsf{QR}_n}{\vdash \diamondsuit^m A, \boxdot^n D}\ \mathsf{C}$$

  If $n = m$, then we perform a quantum principal reduction. Otherwise, let assume $m > n$. In this case, both $C$ and $D$ must be modal formulas, because $\diamondsuit^n C = (\boxdot^m B)^\perp$ and, as a consequence, the last rule in $\mu$ must be itself a quantum rule, or an axiom. Hence we can perform either a quantum contraction, or (in case of axiom) a quantum expansion.

This concludes the proof. □

**Proposition 4.2** *The binary relation $\Longrightarrow$ is confluent and strongly normalizing.*

**Proof.** Actually, $\Longrightarrow$ is *strongly* confluent, as can be proved by analyzing the different cases. The fact $\Longrightarrow$ is strongly normalizing can be proved by attributing a weight to any rule and by showing that the total weight of a proof $\pi$ (i.e. the sum of the weight of all rule instances in $\pi$) strictly decreases along $\Longrightarrow$. □

## 5 Encoding of Quantum Circuits

*Quantum circuits* are an efficient model of quantum computation. A quantum circuit is an acyclic network of quantum gates connected by wires, where each gate represents an operation on the qubits on which the gate acts. In this paper, we are interested in *unitary quantum circuits*, i.e. circuits in which all the gates correspond to unitary operations. It is a standard result that a general quantum circuit can be simulated by a unitary quantum circuit (its *unitary purification*) plus some ancillary qubits, to be measured or ignored at the end of the computation.

In this section, we give some intuitions about the quantum modality, by illustrating the fact that all unitary quantum circuits are captured by QMLL proofs. Let us consider proofs in QMLL which do not make use of multiplicative connectives. We can see a proof of conclusion $\vdash \diamondsuit^n \alpha^\perp, \boxdot^n \alpha$ as a circuit on $n$ qubits. The number of occurrences of modalities in which $\alpha^\perp$ (resp. $\alpha$) is nested in the conclusion, corresponds to the number of qubits on which the circuit acts. More precisely, at depth 1 we have the first qubit, at depth 2 the second, and so on. We can then act on the qubits from $j+1$ to $j+k$, by applying a quantum rule $\mathsf{QR}_k$ to $\vdash \diamondsuit^j \alpha^\perp, \boxdot^j \alpha$. This is best illustrated by some examples. Let us start with a simple circuit on 3 qubits (and no operation on them), and its encoding:

$$\begin{array}{c}\\ \\ \\ \hline\hline\hline\end{array} \qquad \dfrac{\vdash \alpha^\perp, \alpha \quad I \otimes I \otimes I \in \mathbb{U}_3}{\vdash \diamondsuit^3 \alpha^\perp, \boxdot^3 \alpha}$$

The application of the Hadamard gate on the second qubit can be represented as follows:

$$\begin{array}{c}\hline\\ \hline -\boxed{H}- \\ \hline\end{array} \qquad \dfrac{\dfrac{\dfrac{\vdash \alpha^\perp, \alpha \quad I \in \mathbb{U}_1}{\vdash \diamondsuit^1 \alpha^\perp, \boxdot^1 \alpha} \quad H \in \mathbb{U}_1}{\vdash \diamondsuit^2 \alpha^\perp, \boxdot^2 \alpha} \quad I \in \mathbb{U}_1}{\vdash \diamondsuit^3 \alpha^\perp, \boxdot^3 \alpha}$$

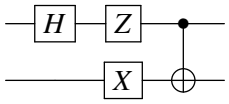
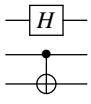



Figure 3: An Example Quantum Circuit

Let us now represent a circuit which applies Hadamard to the first qubit, and the CNOT gate to the second and third qubits:




$$\dfrac{\dfrac{\vdash \alpha^{\perp}, \alpha \quad H \in \mathbb{U}_1}{\vdash \diamondsuit^1\alpha^{\perp}, \boxdot^1\alpha} \qquad CNOT \in \mathbb{U}_2}{\vdash \diamondsuit^3\alpha^{\perp}, \boxdot^3\alpha}$$

Applying a gate after the other to the same qubit(s) corresponds to composing the unitary operators, which is naturally performed by the cut-rule. As an example, the quantum circuit $\mathbf{Q}$ graphically represented in Figure 3 can be encoded as follows:

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdash \alpha^{\perp}, \alpha \quad H \in \mathbb{U}_1}{\vdash \diamondsuit^1\alpha^{\perp}, \boxdot^1\alpha}\,\mathsf{QR}_1 \qquad I \in \mathbb{U}_1}{\vdash \diamondsuit^2\alpha^{\perp}, \boxdot^2\alpha}\,\mathsf{QR}_1 \qquad \dfrac{\dfrac{\vdash \alpha^{\perp}, \alpha \quad Z \in \mathbb{U}_1}{\vdash \diamondsuit^1\alpha^{\perp}, \boxdot^1\alpha}\,\mathsf{QR}_1 \qquad X \in \mathbb{U}_1}{\vdash \diamondsuit^2\alpha^{\perp}, \boxdot^2\alpha}\,\mathsf{QR}_1}{\vdash \diamondsuit^2\alpha^{\perp}, \boxdot^2\alpha} \qquad \dfrac{\vdash \alpha^{\perp}, \alpha \quad CNOT \in \mathbb{U}_2}{\vdash \diamondsuit^2\alpha^{\perp}, \boxdot^2\alpha}\,\mathsf{QR}_2}{\vdash \diamondsuit^2\alpha^{\perp}, \boxdot^2\alpha}$$

With this, it is easy to see that we can faithfully capture any unitary quantum circuit $\mathbf{Q}$ acting on $m$ qubits by a QMLL proof $\pi_{\mathbf{Q}}$ with conclusion $\vdash \diamondsuit^m\alpha^{\perp}, \boxdot^m\alpha$. Conversely, given a generic QMLL proof, we can retrieve a set of quantum circuits. The next section is devoted to formalizing and proving this claim. This is done by introducing an abstract machine, which given a quantum register and a QMLL derivation, applies to the register the operations coded in the proof.

# 6 The Quantum Interaction Abstract Machine

It is natural to wonder if there is any computational interpretation of the cut elimination procedure we introduced in Section 4. The classical, multiplicative, portion of QMLL behaves as usual: $\parr$ and $\otimes$ are dual connectives which interact in a purely classical fashion by annihilating each other. This corresponds to (linear) beta reduction in the lambda calculus. But what about the new modalities $\boxdot$ and $\diamondsuit$? The reduction rules involving them, namely quantum principal reduction, quantum $\eta$-expansion and quantum contraction correspond to various ways of creating and aggregating unitary transformations (i.e. quantum gates). However, what we would like to have in order to talk of quantum computation, is the ability to act on a quantum register.

In this section, we describe an interpretation of QMLL proofs in terms of an automata-based view of the Geometry of Interaction due to Danos and Regnier [3], called the Quantum Interaction Abstract Machine (QIAM in the following). This, in particular, will constitute a concrete computational interpretation of QMLL cut elimination, being a model of it.

In order to give the machine, we need to introduce some technical definitions. A *context* is simply a formula with an "hole" $[\cdot]$ in it:

$$C ::= [\cdot] \mid C \parr A \mid A \parr C \mid C \otimes A \mid A \otimes C \mid \boxdot C \mid \diamondsuit C.$$

The formula obtained by substituting $A$ for $[\cdot]$ in a context $C$ is indicated as $C[A]$. If $A = C[\alpha]$ (respectively, if $A = C[\alpha^\perp]$), then $C$ is said to be a *positive* (respectively, a *negative*) *context for* $A$. If $C$ is either positive or negative for $A$, then we simply say that $C$ is a *context for* $A$. To emphasize that a context $C$ is positive (negative, respectively) for a formula $A$, we indicate it with the metavariable $P$ (respectively, $N$). Given a context $C$, its dual $C^\perp$ can be easily defined, e.g. $(A \otimes C)^\perp = A^\perp \parr C^\perp$.

The *nesting depth* of $C$, denoted $\partial(C)$, is the number of occurrences of modal operators in which $[\cdot]$ is embedded. A *stack* is an element of $\{\boxdot, \diamondsuit\}^*$, i.e., a finite sequence of elements of $\{\boxdot, \diamondsuit\}$, each seen as an atomic symbol.

The *quantum interactive abstract machine* $M_\pi$ associated to any proof $\pi$ consists in:

1. The set of *states* $Q_\pi$, which contains all the quadruples in the form $(A, C, s, Q)$, where $A$ is an occurrence of a formula in $\pi$, $C$ is a context for $A$, $s$ is a stack, and $Q$ is a *quantum register* of $\partial(C) + |s|$ qubits.
2. A *transition relation* $\longrightarrow_\pi \subseteq Q_\pi \times Q_\pi$.

The transition relation $\longrightarrow_\pi \subseteq Q_\pi \times Q_\pi$ is defined by way of a set of rules which we will introduce shortly. Before doing that, let us remark that:

- We can see the transition rules as providing instructions for a token to travel around the proof. With the transition $(A, C, s, Q) \longrightarrow_\pi (B, D, r, R)$, the token moves from the (occurrence of) formula $A$ to the (occurrence of) formula $B$. In general, $A$ and $B$ appear in sequents which are one on top of the other (i.e., premise and conclusion of the same rule); the only exception is when $A$ is the principal formula of a cut or an axiom: in such a case $B$ will be the principal formula $A^\perp$. In the case when $A$ and $B$ appear in sequents which are one on top of the other, if $C$ is positive (negative, respectively) for $A$, then the token goes *down* (*up*, respectively). When on axioms and on principal formulas of the cut rule, the token *inverts its direction*.
- The size $\partial(C) + |s|$ of the quantum register is constant. We operate on the the quantum register $Q$ only when exiting from a quantum box. At that moment, the unitary transformation associated to the box (or its inverse) is applied to $Q$.
- The rôle of the context $C$ is similar to the one of the multiplicative stack in ordinary IAM, while the rôle of $s$ consists in keeping track of which of the two ports of boxes have been traversed to reach the current position. In other words, the length of the stack is exactly the "box-nesting depth" of $A$ in $\pi$.

The rules defining $\longrightarrow_\pi$ are indeed independent on the specific structure of $\pi$ and, instead, only depend on the six proof rules of QMLL. They are in Figure 4 and are given in an informal but hopefully intuitive way. As it can be easily seen, the relation $\longrightarrow_\pi$ is a partial function: for every state $S$ there is *at most* one state $T$ such that $S \longrightarrow_\pi T$. Moreover, it is an injection: no two states $S, T$ can lead to the same $R$ via $\longrightarrow_\pi$.

Now, let us turn our attention to the way the quantum register $Q$ is manipulated during computation. As previously observed, the only way to alter the value of the quantum register consists in exiting from a box. Moreover, the way any state $(A, N, s, Q)$ evolves does *not* depend on $Q$: the operations applied to the underlying quantum register along $\longrightarrow_\pi$ only depend on the first three components of the state. The current value of the quantum register has no effect on the value of the first three components after any transition. This is captured by the following:

**Lemma 6.1 (Uniformity)** *For every proof $\pi$ and for every $A, C, s$, there are $B, D, r$ and a unitary operator $U$ on $\mathbb{C}^{2^{\partial(C)+|r|}}$ such that for every $Q$, if $(A, C, s, Q) \longrightarrow_\pi (C, E, q, R)$ then $C = B$, $E = D$, $q = r$ and $R = U(Q)$.*

Rule A

$$\begin{array}{rcl}(A,N,s,Q) & \longrightarrow_\pi & (A^\perp,N^\perp,s,Q)\\ (A^\perp,N,s,Q) & \longrightarrow_\pi & (A,N^\perp,s,Q)\end{array} \qquad \frac{}{\vdash A^\perp,A}$$

Rule C

$$\begin{array}{rcl}(A,P,s,Q) & \longrightarrow_\pi & (A^\perp,P^\perp,s,Q)\\ (A^\perp,P,s,Q) & \longrightarrow_\pi & (A,P^\perp,s,Q)\\ (\Gamma_1,N,s,Q) & \longrightarrow_\pi & (\Gamma_2,N,s,Q)\\ (\Delta_1,N,s,Q) & \longrightarrow_\pi & (\Delta_2,N,s,Q)\\ (\Gamma_2,P,s,Q) & \longrightarrow_\pi & (\Gamma_1,P,s,Q)\\ (\Delta_2,P,s,Q) & \longrightarrow_\pi & (\Delta_1,P,s,Q)\end{array} \qquad \frac{\vdash \Gamma_2,A \quad \vdash \Delta_2,A^\perp}{\vdash \Gamma_1,\Delta_1}$$

Rule $\parr$

$$\begin{array}{rcl}(A\parr B,N\parr B,s,Q) & \longrightarrow_\pi & (A,N,s,Q)\\ (A\parr B,A\parr N,s,Q) & \longrightarrow_\pi & (B,N,s,Q)\\ (A,P,s,Q) & \longrightarrow_\pi & (A\parr B,P\parr B,s,Q)\\ (B,P,s,Q) & \longrightarrow_\pi & (A\parr B,A\parr P,s,Q)\\ (\Gamma_1,N,s,Q) & \longrightarrow_\pi & (\Gamma_2,N,s,Q)\\ (\Gamma_2,P,s,Q) & \longrightarrow_\pi & (\Gamma_1,P,s,Q)\end{array} \qquad \frac{\vdash \Gamma_2,A,B}{\vdash \Gamma_1,A\parr B}$$

Rule $\otimes$

$$\begin{array}{rcl}(A\otimes B,N\otimes B,s,Q) & \longrightarrow_\pi & (A,N,s,Q)\\ (A\otimes B,A\otimes N,s,Q) & \longrightarrow_\pi & (B,N,s,Q)\\ (A,P,s,Q) & \longrightarrow_\pi & (A\otimes B,P\otimes B,s,Q)\\ (B,P,s,Q) & \longrightarrow_\pi & (A\otimes B,A\otimes P,s,Q)\\ (\Gamma_1,N,s,Q) & \longrightarrow_\pi & (\Gamma_2,N,s,Q)\\ (\Delta_1,N,s,Q) & \longrightarrow_\pi & (\Delta_2,N,s,Q)\\ (\Gamma_2,P,s,Q) & \longrightarrow_\pi & (\Gamma_1,P,s,Q)\\ (\Delta_2,P,s,Q) & \longrightarrow_\pi & (\Delta_1,P,s,Q)\end{array} \qquad \frac{\vdash \Gamma_2,A \quad \vdash \Delta_2,B}{\vdash \Gamma_1,\Delta_1,A\otimes B}$$

Rule $\mathsf{QR}_n$

$$\begin{array}{rcl}(\diamond^n A,\diamond^n N,s,Q) & \longrightarrow_\pi & (A,N,s\cdot\diamond^n,Q)\\ (\boxdot^n B,\boxdot^n N,s,Q) & \longrightarrow_\pi & (A,N,s\cdot\boxdot^n,Q)\\ (A,P,s\cdot\diamond^n,Q) & \longrightarrow_\pi & (\diamond^n A,\diamond^n P,s,Q)\\ (A,P,s\cdot\boxdot^n,Q) & \longrightarrow_\pi & (\diamond^n A,\diamond^n P,s,(I_{\partial(P)}\otimes U^*\otimes I_{|s|})(Q))\\ (B,P,s\cdot\boxdot^n,Q) & \longrightarrow_\pi & (\boxdot^n B,\boxdot^n P,s,Q)\\ (B,P,s\cdot\diamond^n,Q) & \longrightarrow_\pi & (\boxdot^n B,\boxdot^n P,s,(I_{\partial(P)}\otimes U\otimes I_{|s|})(Q))\end{array} \qquad \frac{\vdash A,B \quad U\in\mathbb{U}_n}{\vdash \diamond^n A,\boxdot^n B}\ \mathsf{QR}_n$$

Figure 4: Defining Rules for $\longrightarrow_\pi$

But what are the reasons why $\longrightarrow_\pi$ can be partial? Clearly, it is not defined on any state $S = (A, P, s, Q)$ where $A$ occurs in the conclusion of $\pi$: $P$ tells us that the next state should be "below $S$", but there's nothing below the conclusion of $\pi$. For the same reasons, no state are mapped to a quadruple in the form $(A, N, s, Q)$. This motivates the following definition: the set $IQ_\pi$ of *initial states* for a proof $\pi$ consists of the states in $Q_\pi$ in the form $(A, N, \varepsilon, Q)$, where $A$ is the conclusion of $\pi$. Analogously, *final states* are those in the form $(A, P, \varepsilon, Q)$ and are the elements of $FQ_\pi$. The *semantics* of $\pi$ is the partial function

$$[\![\pi]\!] : IQ_\pi \rightharpoonup FQ_\pi$$

defined by stipulating that $[\![\pi]\!](S) = T$ iff $S \longrightarrow_\pi^* T$. One can prove that if we start from an initial state, we are guaranteed to reach a final state:

**Proposition 6.2** *For every $\pi$, $[\![\pi]\!]$ is total.*

**Proof.** A state is said to be have a *legal stack* if its third component is coherent with the box-depth of its first component in the proof $\pi$. On the one hand, any state $S$ reachable from an initial state has the property of having a legal stack, as can be easily proved by induction on the length of any chain of transitions leading any initial state to $S$. On the other hand, any state with a legal stack is *deadlock-free*, i.e. it is either final or such that $S \longrightarrow_\pi T$ for some $T$. This means that starting from any initial state we can either reach a final state or go on forever. But the latter is not possible, since $\longrightarrow_\pi$ is injective even when restricted to the first three components of states, and moreover the set of states having a legal stack (again, if we discard the quantum register) is finite. □

**Proposition 6.3** *If $\pi \Longrightarrow \rho$, then $[\![\pi]\!] = [\![\rho]\!]$.*

**Proof.** It is an easy task to prove that each cut-elimination step can possibly alter the underlying QIAM, but in a way which cannot be observed from the environment, i.e., by querying the machine from an initial state. □

Lemma 6.1 justifies the following definition: given a proof $\pi$ with conclusion $A$ and a negative context $N$ for its $A$, *the semantics* of $\pi$ relative to $N$ is the function

$$[\![\pi]\!]_N : \mathbb{C}^{2^{\partial(N)}} \longrightarrow \mathbb{C}^{2^{\partial(N)}}$$

defined by stipulating that $[\![\pi]\!]_N(Q) = R$ iff $(A, N, \varepsilon, Q) \longrightarrow_\pi^* (A, P, \varepsilon, R)$. Noticeably:

**Theorem 6.4** *For every $\pi$ and for every negative context $N$ for the conclusion of $\pi$, $[\![\pi]\!]_N$ is unitary. Moreover, a quantum circuit computing it can be effectively extracted from $N$.*

**Proof.** An easy corollary of Lemma 6.1, Proposition 6.2 and the fact $M_\pi$ is and effective and executable description of $\pi$. □

# 7 Conclusions

Theorem 6.4 establishes a sort of *soundness* result: any QMLL proof can be interpreted as a set of independent unitary quantum circuits by way of a concrete GoI interpretation. We already know (Section 5) that any unitary quantum circuit $\mathbf{Q}$ acting on $m$ qubits is captured by a QMLL proof $\pi_{\mathbf{Q}}$ with conclusion $\vdash \diamond^m \alpha^\perp, \boxdot^m \alpha$. Hence, QMLL is somehow a *complete* system for unitary quantum circuits. Some observations are now in order:

- The encoding is correct: the (unique!) circuit obtained from $[\![\pi_{\mathbf{Q}}]\!]$ by way of Theorem 6.4 is $\mathbf{Q}$.

- The unitary operators in $\pi_{\mathbf{Q}}$ are exactly the quantum gates in the circuit $\mathbf{Q}$. If we apply cut-elimination to $\pi_{\mathbf{Q}}$, however, some of those unitary operators are composed or tensorized. From a purely syntactical point of view this can be seen as a way to alter the quantum circuit underlying a proof, preserving equivalence.

We also observe that the encoding does not make use of the multiplicative connectives at all. So, in a sense the modal fragment of QMLL is itself complete for quantum circuits. A further clarification of the rôle of multiplicatives in QMLL is a fascinating subject which we leave for future work.

## References


[1] Richard Blute & Prakash Panangaden: *Proof Nets as Formal Feynman Diagrams*. Submitted.

[2] Ugo Dal Lago, Andrea Masini & Margherita Zorzi (2009): *On a measurement-free quantum lambda calculus with classical control*. *Mathematical Structures in Computer Science* 19(2), pp. 297–335, doi:10.1017/S096012950800741X.

[3] Vincent Danos & Laurent Regnier (1995): *Proof nets and the Hilbert space*. In J.-Y. Girard, Y. Lafont & L. Regnier, editors: *Advances in Linear Logic*, Cambridge University Press, pp. 307–328.

[4] Ross Duncan (2009): *Generalised Proof-Nets for Compact Categories with Biproducts*. In S. Gay & I. Mackie, editors: *Semantics of Quantum Computation*, Cambridge University Press, pp. 70–134.

[5] Jean-Yves Girard (1987): *Linear Logic*. *Theoretical Computer Science* 50(1), pp. 1–102, doi:10.1016/0304-3975(87)90045-4.

[6] Jean-Yves Girard (1987): *Multiplicatives*. In: *Rendiconti del Seminario Matematico dell'Università e Policlinico di Torino. Special issue on Logic and Computer Science*, pp. 11–33.

[7] Jean-Yves Girard (1989): *Geometry of Interaction I: Interpretation of System F*. In: *Proceedings of the Logic Colloquium '88*, North Holland, pp. 221–260.

[8] Jean-Yves Girard (2004): *Between logic and quantic: a tract*. In P. Ruet T. Ehrhard, J.-Y. Girard & P. Scott, editors: *Linear Logic in Computer Science*, Cambridge University Press, pp. 346–281.

[9] Jean-Yves Girard (2011): *The Blind Spot: Lectures on Logic*. European Mathematical Society.

[10] Georges Gonthier, Martín Abadi & Jean-Jacques Lévy (1992): *The Geometry of Optimal Lambda Reduction*. In: *19th Symposium on Principles of Programming Languages (POPL), Proceedings.*, ACM Press, pp. 15–26, doi:10.1145/143165.143172.

[11] Ichiro Hasuo & Naohiko Hoshino (2011): *Semantics of Higher-Order Quantum Computation via Geometry of Interaction*. In: *26th Symposium on Logic in Computer Science (LICS), Proceedings*, IEEE, pp. 237–246, doi:10.1109/LICS.2011.26.

[12] Peter Selinger & Benoît Valiron (2006): *A lambda calculus for quantum computation with classical control*. *Mathematical Structures in Computer Science* 16(3), pp. 527–552, doi:10.1017/S0960129506005238.

[13] Peter Selinger & Benoît Valiron (2008): *On a Fully Abstract Model for a Quantum Linear Functional Language: (Extended Abstract)*. *Electronic Notes in Theoretical Computer Science* 210, pp. 123–137, doi:10.1016/j.entcs.2008.04.022.

[14] André van Tonder (2004): *A Lambda Calculus for Quantum Computation*. *SIAM J. Comput.* 33(5), pp. 1109–1135, doi:10.1137/S0097539703432165.