On a fully abstract model for a quantum linear functional language (extended abstract)

Peter Selinger\textsuperscript{1,2}

Dalhousie University, Halifax, Nova Scotia, Canada

Benoît Valiron\textsuperscript{3}

University of Ottawa, Ottawa, Ontario, Canada

\textbf{Abstract}

This paper studies the linear fragment of the programming language for quantum computation with classical control described in \cite{4}. We sketch the language, and discuss equivalence of terms. We also describe a fully abstract denotational semantics based on completely positive maps.

\textbf{Keywords:} Quantum computing, functional programming, linear lambda calculus, higher order, semantics.

\section{Introduction}

This work studies a linear functional programming language for quantum computation with classical control, derived from the language in \cite{4}.

The first denotational semantics of a quantum programming language was given by the first author in \cite{3}, for the quantum flowchart language QFC. The semantics given there was compositional and took place in a category of superoperators, which are special completely positive maps. However, the language lacked a crucial feature found in functional programming languages, namely, the notion of higher-order functions.

In \cite{4}, we sought to address this omission by introducing a typed lambda calculus for quantum computation. This language resembles QFC in that it combines quantum and classical data types with classical control features, but it also includes lambda abstractions and therefore function closures. The problem of deciding the
duplicability of data was solved syntactically, by giving a type system that distin-
guishes duplicable and non-duplicable types. The quantum lambda calculus pos-
sesses a reduction semantics, but no denotational semantics has been given for it so
far.

In this paper, we study the restriction of the quantum lambda calculus to the
purely linear case. This means we study the fragment of the language where each
element, classical and quantum, must be used exactly once. The linear quantum
lambda calculus differs from its nonlinear cousin in that it is less sensitive to the
evaluation order of terms. We give a denotational semantics for this language in
a category of completely positive maps, and we show that it is fully abstract with
respect to the operational semantics.

The question of finding a denotational semantics for the full quantum lambda
calculus is still open, but we hope that this work is a step in that direction.

The plan of the paper is as follows. First we brieﬂy describe the language and
the type system. Then we develop an operational semantics for it, and we deﬁne
a notion of equivalence of terms. Finally we build a denotational semantics for the
language, and we show the full abstraction result.

2 A linear lambda-calculus for quantum computation

In [4], we have deﬁned an operational semantics for a lambda calculus for quantum
computation with classical control. Here, we study the purely linear fragment of
this language. We begin by re-adapting the deﬁnitions and results from this earlier
paper for the linear setting.

2.1 Terms and Programs

Definition 2.1 The linear quantum lambda calculus has the following terms:

$$M, N, P ::= x | MN | \lambda x.M | \text{if } M \text{ then } N \text{ else } P | 0 | 1 | \text{meas} | \text{new} | U | * | \langle M, N \rangle | \text{let } \langle x, y \rangle = M \text{ in } N | \Omega.$$ 

We follow Barendregt’s convention for identifying terms up to α-equivalence [1].
The set of free variables of a term $M$ is written $\text{FV}(M)$. We also sometimes use
the shorthand notation $\langle M_1, \ldots, M_n \rangle = \langle M_1, \langle M_2, \ldots \rangle \rangle$. In the following, we often write $c$ for an arbitrary constant of the language, i.e., 0, 1, meas, new, $U$, or $*$. The set of types is deﬁned by

$$A, B ::= \text{bit} | \text{qbit} | A \rightarrow B | \top | A \otimes B.$$ 

Note that, unlike the language of [4], there is no type constructor $!A$. We use
the same shortcut for the product type as we did for the product term, to deﬁne
$A \otimes \ldots \otimes A$. To each constant term $c$, we associate a ﬁxed type $A_c$, namely meas : qbit $\rightarrow$ bit, 0, 1 : bit, new : bit $\rightarrow$ qbit, $*$ : $\top$ and $U : \text{qbit}^{\otimes n} \rightarrow \text{qbit}^{\otimes n}$. A typing judgement is a triple $\Delta \triangleright M : A$, where $\Delta$ is a list of distinct typed variables called a typing context, $M$ is a term, and $A$ is a type. We say that a typing judgement is valid if it follows from the typing rules given in Table 1.
3 Operational semantics

3.1 Small step semantics

Although this language is intended to manipulate quantum information, no constants of type qbit are provided in the definition of lambda-terms. Indeed, while it would be possible to allow constant qubit expressions such as $\alpha|0\rangle + \beta|1\rangle$, such a notation would not lend itself to expressing entangled states. Instead, we introduce the concept of a quantum array and a linking function to express terms with embedded quantum data.

**Definition 2.2** A quantum closure is a triple $[Q, L, M]$ where $Q$ is a normalized vector in $\otimes_{i=1}^{n} \mathbb{C}^2$, for some $n \geq 0$, $L$ is a bijective function from a set $|L|$ of term variables to $\{0, \ldots, n-1\}$, and $M$ is a term. $Q$ is called a quantum array, and $L$ is called a linking function. We write $|Q| = n$. If $L(x_i) = i$, we will sometimes write $L$ as the ordered list $[x_1 \cdots x_n]$. The idea is that the variable $x_i$ is bound in the term $M$ to qubit number $L(x_i)$ of the state $Q$. We also call the pair $(Q, L)$ a quantum context.

We extend the notion of $\alpha$-equivalence to quantum closures:

$$[Q, [x \cdots y \cdots z], M] =_\alpha [Q, [x \cdots y' \cdots z], M[y'/y]]$$

if $y \notin \text{FV}(M) \cup |L|$.

**Definition 2.3** A quantum closure $[Q, L, M]$ is well-typed (or valid) of type $A$ in the typing context $\Gamma$, written $\Gamma \vdash [Q, L, M] : A$, if $|L| \cap |\Gamma| = \emptyset$ and $\Gamma, x_1: \text{qbit}, \ldots, x_k: \text{qbit} \vdash M : A$ is a valid typing judgement, where $\{x_1 \ldots x_k\} = |L| \cap \text{FV}(M)$.

A well-typed quantum closure is closed if $|\Gamma| = \emptyset$, and a closed well-typed quantum closure is also called a program.

A well-typed quantum closure is called a computation if $|L| \subseteq \text{FV}(M)$, or equivalently, if $\text{FV}(M) = |L| \cup |\Gamma|$.

3 Operational semantics

3.1 Small step semantics

The language contains a probabilistic operation: the measurement. This probabilistic operation forces us to choose a reduction strategy.
rules for the reduction are an adaptation of the ones found in A value program to the quantum lambda calculus by structural induction. For this purpose we need the notion "quantum" rules. In the first two rules, let...

\[ Q;L,N \rightarrow^{\alpha}_{\rho} [Q',L',N'] \]
\[ Q;L,M \rightarrow^{\beta} [Q',L',M'] \]
\[ Q;L,MN \rightarrow^{\rho}_{\rho} [Q',L',MN'] \]
\[ Q;L,MV \rightarrow^{\rho}_{\rho} [Q',L',M'V] \]
\[ Q;L,M_1 \rightarrow^{\rho}_{\rho} [Q',L',M'_1] \]
\[ Q;L,M_2 \rightarrow^{\rho}_{\rho} [Q',L',M'_2] \]
\[ Q;L,\langle M_1,M_2 \rangle \rightarrow^{\rho}_{\rho} [Q',L',\langle M'_1,M_2 \rangle] \]
\[ Q;L,\langle V_1, M_2 \rangle \rightarrow^{\rho}_{\rho} [Q',L',\langle V_1, M'_2 \rangle] \]
\[ Q;L,P \rightarrow^{\rho}_{\rho} [Q',L',P'] \]
\[ Q;L,if \ P \ then \ M \ else \ N \rightarrow^{\rho}_{\rho} [Q',L',if \ P' \ then \ M \ else \ N] \]
\[ Q;L,M \rightarrow^{\rho}_{\rho} [Q',L',M'] \]
\[ Q;L,let \ \langle x_1,x_2 \rangle = M \ in \ N \rightarrow^{\rho}_{\rho} [Q',L',let \ \langle x_1,x_2 \rangle = M' \ in \ N] \]

Table 2
Reduction rules for the quantum lambda calculus

**Definition 3.1** We define the call-by-value reduction strategy for the linear quantum lambda calculus by structural induction. For this purpose we need the notion of a value. We define a value term to be of the form \( V,W \ ::= x \mid c \mid \lambda x.M \mid \langle V,W \rangle \).

A value program is a program of the form \([Q,L,V]\), where \( V \) is a value term. The rules for the reduction are an adaptation of the ones found in [4].

We set the rules to be the "classical" ones found in Table 2, plus the following "quantum" rules. In the first two rules, let \( Q = \sum_j Q_j^0 \otimes \alpha_j |0\rangle \otimes Q_j^0 + \sum_j Q_j^1 \otimes \beta_j |1\rangle \otimes Q_j^1 \), where \( Q_j^0 \in \mathbb{C}^{2^{n-1}} \) and \( Q_j^1 \in \mathbb{C}^{2^n-1} \).

\[ [Q,|x_1 \ldots x_n\rangle, \text{meas } x_i] \rightarrow^{m_i}_{|\alpha|^2} [\sum_j Q_j^0 \otimes Q_j^0, |x_1 \ldots x_{i-1}x_{i+1} \ldots x_n\rangle, 0], \]
\[ [Q,|x_1 \ldots x_n\rangle, \text{meas } x_i] \rightarrow^{m_i}_{|\alpha|^2} [\sum_j Q_j^1 \otimes Q_j^1, |x_1 \ldots x_{i-1}x_{i+1} \ldots x_n\rangle, 1]. \]

If \( w \) is a fresh term variable not yet in use:

\[ [Q,|x_1 \ldots x_n\rangle, \text{new } 0] \rightarrow^{n_o} [Q \otimes |0\rangle, |x_1 \ldots x_n w\rangle, w], \]
\[ [Q,|x_1 \ldots x_n\rangle, \text{new } 1] \rightarrow^{n_i} [Q \otimes |1\rangle, |x_1 \ldots x_n w\rangle, w]. \]

If \( Q' \) is the result of applying \( U \) to the quantum bits \( L(x_1), \ldots, L(x_n) \) in \( Q \):

\[ [Q,\langle x_1, \ldots, x_n \rangle] \rightarrow_{U}^{U} [Q',\langle x_1, \ldots, x_n \rangle]. \]

Note that since we want a linear language, we modified the measurement rule from [4] by deleting the quantum bit measured from the quantum array.

**Lemma 3.2 (Substitution)** If \( \Delta, x : A \triangleright M : B \) and if \( \Gamma \triangleright N : A \) then \( \Delta, \Gamma \triangleright M[N/x] : B \) is a valid typing judgement.
Note that, in the non-linear case, the Substitution Lemma only holds when \( N = V \) is a value. However, in the linear calculus considered here, it holds for general \( N \).

**Theorem 3.3 (Safety properties)** If \( P \) is a closed valid computation of type \( A \), either it is a value or \( P \rightarrow_p P' \), with \( P' \) a closed valid computation of type \( A \).

**Proof.** The proof is an adaptation of the proof of Theorems 1 and 2 in [4]. \( \square \)

The language being linear, the reduction has a strong relation on the length of the terms.

**Definition 3.4** Let \( l(M) \) be the length of a term \( M \), defined recursively as \( l(x) = l(c) = l(\Omega) = 1 \), \( l(\lambda x.M) = l(M) + 1 \), \( l(\text{let } (x, y) = M \text{ in } N) = l(M) + l(N) + 1 \), \( l(\text{if } P \text{ then } M \text{ else } N) = l(P) + \max(l(M), l(N)) \), \( l(MN) = l((M, N)) = l(M) + l(N) + 1 \).

**Lemma 3.5** If \( x \in FV(M) \), then \( l(M[N/x]) = l(M) + l(N) - 1 \).

**Lemma 3.6** If \( [Q, L, M] \rightarrow_p^x [Q', L', M'] \), then either \( x \neq \omega \) and \( l(M') < l(M) \) or \( x = \omega \) and \( l(M') = l(M) \). In the latter case, \( [Q, L, M] = [Q', L', M'] \).

**Definition 3.7** A program \( [Q, L, M] \) that reduces with a \( \omega \)-rule is called a fixed point.

**Theorem 3.8 (Strong Normalization)** If \( P = [Q, L, M] \) is a closed valid computation, \( P \) reduces to a value or to a fixed point in at most \( l(M) \) steps.

**Proof.** Follows from Lemma 3.6. \( \square \)

### 3.2 Quantum context and reduction

When describing the reduction rules, we carefully separated the quantum context from the lambda-term. In this subsection we show that the precise order of quantum bits in the quantum array does not matter.

**Definition 3.9** If \( \sigma \) is a permutation of \( \{1, \ldots, n\} \), we extend \( \sigma \) to \( \mathbb{N} \) with \( \sigma(j) = j \) for \( j > n \), and we define \( \bar{\sigma} \) to be the corresponding permutation of quantum bits \( \bar{\sigma}[x_1 \cdots x_n \cdots x_{n+k}] = [x_{\sigma(1)} \cdots x_{\sigma(n)} x_{n+1} \cdots x_{n+k}] \). We say that \( (Q_1, L_1) \) is \( \sigma \)-equivalent to \( (Q_2, L_2) \) if \( Q_1 \) and \( Q_2 \) have the same size, \( Q_2 = \bar{\sigma}(Q_1) \) and \( L_2 = \sigma^{-1} \circ L_1 \). We write \( (Q_1, L_1) =_\sigma (Q_2, L_2) \). We define an equivalence relation called alpha-equivalence on quantum contexts by \( (Q_1, L_1) =_\alpha (Q_2, L_2) \) if there exists a \( \sigma \) such that \( (Q_1, L_1) =_\alpha (Q_2, L_2) \).

The alpha-equivalence is sound with respect to the semantics.

**Lemma 3.10** If \( [Q, L, M] \rightarrow_p [Q', L', M'] \) then \( [\bar{\sigma}Q, \sigma L, M] \rightarrow_p [\bar{\sigma}Q', \sigma L', M'] \).

### 3.3 Reduction to values

In the reduction process, what we are really seeking is the final result of the computation. In this section we explicate the relation of programs to values.
Definition 3.11 We informally recall a notion defined in [4]: If $X$ is the set of closed valid programs and $U$ the set of values, let $\text{prob}_U : X \times U \to [0, 1]$ be the map $\text{prob}_U(P, V)$ that returns the total probability for a program $P$ to end up on the value $V$ in zero or more steps. This function is called the big-step reduction.

We also define the small-step reduction operation $\text{prob} : X \times X \to [0, 1]$: for closed programs $P, P'$, we define $\text{prob}(P, P') = p$ if there is a single-step probabilistic reduction $P \xrightarrow{\text{prob}} P'$, $\text{prob}(V, V) = 1$ if $V$ is a value program, and $\text{prob}(P, P') = 0$ in all other cases. Note that for all well-typed $P$, $\sum_{P' \in X} \text{prob}(P, P') = 1$.

Definition 3.12 If $P$ is a closed well-typed program of type $\text{bit}$, and $b \in \{0, 1\}$, we define $(P \Downarrow b) = \sum_{V \in U_b} \text{prob}(P, V)$, where $U_b$ is the set of valid programs with term the value $b$. We say that $P$ evaluates to $b$ with probability $P \Downarrow b$.

Definition 3.13 We define a formal probability distribution of quantum closures to be $\Gamma \vdash \sum_i \rho_i |Q_i, L_i, M_i| : A$, where each $\Gamma \vdash \sum_i |Q_i, L_i, M_i| : A$ is valid and $\sum \rho_i \leq 1$. The distribution is said to be closed if $|\Gamma| = \emptyset$.

Lemma 3.14 Given a set $Z$, let $\mathcal{C}Z$ be the set of probability distributions over it.

The small-step reduction $\text{prob} : X \times X \to [0, 1]$ can be curried to a map $\text{prob}' : \mathcal{C}X \to \mathcal{C}X$: $\text{prob}'(\sum_i \alpha_i P_i) = \sum_i \alpha_i \sum_{P' \in X} \text{prob}(P_i, P') P'$. Similarly, $\text{prob}_U : X \times U \to [0, 1]$ can be curried to a map $\text{prob}'_U : \mathcal{C}X \to \mathcal{C}U$: $\text{prob}'_U(\sum_i \alpha_i P_i) = \sum_i \alpha_i \text{prob}_U(P_i, V) V$. The definition of $P \Downarrow b$ can be extended in the same way to probability distributions of programs.

Lemma 3.15 If $\vdash P : A$ is valid, so is $\vdash \text{prob}' P : A$ and $\vdash \text{prob}'_U P : A$.

Due to the strong normalization theorem, applying the map $\text{prob}'_U$ is applying the map $\text{prob}'$ finitely many times.

Proposition 3.16 If $[Q, L, M]$ is a closed valid computation, then the reduction verifies

$$\text{prob}'^n(M)[Q, L, M] = \sum_{i=1}^n \rho_i [Q_i, L_i, V_i] + \sum_{j=1}^m \rho'_j P_j,$$

with $\text{prob}'_U[Q, L, M] = \sum_{i=1}^n \rho_i [Q_i, L_i, V_i]$, the $P_j$ being fixed points, $\sum \rho_i + \sum \rho'_j = 1$, and $n + m < 2^{|M|}$.

4 Denotational semantics

In [3] the notion of completely positive map is used to model the notion of quantum computation. We aim to show that the linear subset of the quantum lambda calculus has the category $\text{CPM}$ as a fully abstract model. Note that the interpretation will not be “onto” all completely positive maps, but will only be “onto up to scalar multiplies”. In this section we set the definition of the denotational semantics.

4.1 The category $\text{CPM}$

We recall the definition of the category $\text{V}$ [3].

- The objects are signatures $\sigma = n_1, \ldots, n_k$, i.e., finite tuples of positive integers,
\[ [x : A \triangleright x : A](v) = v \quad [\triangleright 0 : \text{bit}](x) = (x, 0) \]
\[ [\triangleright * : \top](x) = x \quad [\triangleright 1 : \text{bit}](x) = (0, x) \]
\[ [\Delta \triangleright \Omega : A] = 0 : [\Delta] \rightarrow [A] \]
\[ [\triangleright \text{new} : \text{bit} \rightarrow \text{qbit}] = \Phi(v) : 1 \rightarrow [\text{bit}] \otimes [\text{qbit}] \]
\[ [\triangleright \text{meas} : \text{qbit} \rightarrow \text{bit}] = \Phi(p) : 1 \rightarrow [\text{qbit}] \otimes [\text{bit}] \]
\[ [\triangleright U : \text{qbit}^\otimes n \rightarrow \text{qbit}^\otimes n] = \Phi(U) : 1 \rightarrow 2^n \]
\[ [\Delta, x : A \triangleright M : B] = f : [\Delta] \otimes [A] \rightarrow [B] \]
\[ [\Delta \triangleright \lambda x.M : A \rightarrow B] = \Phi(f) : [\Delta] \rightarrow [A] \otimes [B] \]
\[ [\Delta, \Gamma \triangleright MN : B] : x \otimes y \mapsto g(x \otimes (fy)) \otimes [\Delta] \otimes [\Gamma] \rightarrow [B] \]
\[ [\Delta \triangleright P : \text{bit}] : x \mapsto (px, qx) : [\Delta] \rightarrow [\text{bit}] \]
\[ [\Gamma \triangleright M : A] = f : [\Gamma] \rightarrow [A] \]
\[ [\Gamma \triangleright N : A] = g : [\Gamma] \rightarrow [A] \]
\[ [\Delta, \Gamma \triangleright \text{if } P \text{ then } M \text{ else } N : A] : x \otimes y \mapsto (px)(fy) + (qx)(gy) \]
\[ [\Delta \triangleright M : A] = f : [\Delta] \rightarrow [A] \]
\[ [\Gamma \triangleright N : B] = g : [\Gamma] \rightarrow [B] \]
\[ [\Delta, \Gamma \triangleright (M, N) : A \otimes B] : x \otimes y \mapsto f x \otimes gy : [\Delta] \otimes [\Gamma] \rightarrow [A] \otimes [B] \]

Table 3
Denotational semantics for typing judgments.

- the arrows \( \sigma \rightarrow \sigma' \) are linear maps \( V_\sigma \rightarrow V_{\sigma'} \), where \( V_{n_1, \ldots, n_k} = C^{n_1 \times n_1} \times \cdots \times C^{n_k \times n_k} \).

There is a tensor product \((n_1, \ldots, n_k) \otimes (m_1, \ldots, m_l) = n_1m_1, \ldots, n_1m_1, n_2 \ldots, n_km_l) \) and a canonical isomorphism \( V_{\sigma \otimes \tau} \simeq V_\sigma \otimes V_\tau \). Thus \( V \) has a structure of symmetric monoidal closed category. The unit element is the signature 1. From the vector spaces property, \( V(\sigma \otimes \tau, \sigma') =_\Phi V(\sigma, \tau \otimes \sigma') \): If \( B(\tau) \) is a basis for \( V_\tau \), then from \( f \in V(\sigma \otimes \tau, \sigma') \) we construct \( g = \Phi(f) \in V(\sigma, \tau \otimes \sigma') \) by \( g(s) = \sum_{b \in B(\tau)} b \otimes f(s \otimes b) \). Conversely, given such a \( g \), if \( g(s) = \sum_{u \in B(\sigma')} \alpha_{b, u} b \otimes u \), one constructs \( f = \Phi^{-1}(g) \) by \( f(s \otimes t) = \sum_{u \in B(\sigma')} \alpha_{t, u} u \). This makes \( V \) monoidal closed.

The category \( \text{CPM} \) has the same objects as \( V \) and as arrows completely positive maps (see [3]).

4.2 Modeling the quantum lambda-calculus
We set the denotation of types to be \([\text{bit}] = (1, 1), [A \otimes B] = [A] \otimes [B], [\text{qbit}] = 2, \) and \([A \rightarrow B] = [A] \otimes [B], \) and the denotation of contexts to be
\[ [x_1 : A_1, \ldots, x_n : A_n] = [A_1] \otimes \cdots \otimes [A_n], \quad [\emptyset] = 1. \]
The denotation for typing judgments of the form $\Delta \triangleright M : A$ is a linear map $[\Delta] \rightarrow [A]$, defined inductively as in Table 3. Here, $\Phi : \text{hom}(A \otimes B, C) \rightarrow \text{hom}(A, B \otimes C)$ is the bijection from the compact closed structure and $\iota$ and $p$ are respectively the quantum bits creation and the measurement operation:

$$\iota : 1,1 \rightarrow 2 \quad p : 2 \rightarrow 1,1$$

$$(a,b) \mapsto \left( \begin{array}{c} a \\ 0 \\ b \end{array} \right) \quad \left( \begin{array}{c} a \\ b \\ c \\ d \end{array} \right) \mapsto (a,d)$$

We also define the denotation for a computation. Consider the valid computation $\Delta \vdash [Q, L, M] : A$ where $L = |x_1 \cdots x_n|$ and $|Q| = n$. The quantum context $(Q, L)$ can be seen as a map $g : 1 \rightarrow 2^\otimes n$ such that $g(1) = Q$. Then if

$$[\Delta, x_1 : \text{qbit}, \ldots, x_n : \text{qbit} \triangleright M : A] = f : [\Delta] \otimes 2^\otimes n \rightarrow [A],$$

one defines $[\Delta \vdash [Q, L, M] : A]$ as the composition

$$[\Delta] \xrightarrow{id[\Delta] \otimes g} [\Delta] \otimes 2^\otimes n \xrightarrow{f} [A].$$

One extends this definition to probabilistic distributions of computations using linearity:

$$[\Delta \vdash \sum_i \rho_i P_i] = \sum_i \rho_i [\Delta \vdash P_i].$$

**Lemma 4.1** Denotations of terms and computations are completely positive maps.

**Lemma 4.2 (Substitution)** If $|\Gamma| \cap |\Delta| = \emptyset$ and $[\Delta, x : A \triangleright M : B] = G : [\Delta] \otimes [A] \rightarrow [B]$, $[\Gamma \triangleright N : A] = F : [\Gamma] \rightarrow [A]$, then $[\Delta, \Gamma \triangleright M[N/x] : B] = H : [\Delta] \otimes [\Gamma] \rightarrow [B]$, with $H(d \otimes g) = G(d \otimes (Fg))$.

**Lemma 4.3** Given a valid closed computation $P : A$ with prob$'P = \sum_i \rho_i P_i$, then $[P : A] = [\text{prob}' P : A] = [\text{prob}_U' P : A]$.

**4.3 Fullness of the semantics for the first order fragment**

**Proposition 4.4** For any types $A = U_1 \otimes \cdots \otimes U_n$ and $B = V_1 \otimes \cdots \otimes V_m$, where each $U_i$ and $V_j$ is either bit or qbit, if $F : [A] \rightarrow [B]$ is any superoperator, then there exists a valid typing judgement $x : A \triangleright M : B$ of denotation $F$.

**Corollary 4.5** For every type $A = U_1 \otimes \cdots \otimes U_n$, where each $U_i$ is either bit or qbit, and for every hermitian positive element $v \in V[A]$ of trace at most 1, $v = [M : A](1)$ for some closed valid term $M$.

**5 Equivalence classes of terms**

Being able to build terms, we need some tools to compare them. One can compare them through syntactic manipulations, or one can have a finer approach using the two semantics we have built: in the case of the operational semantics, the behavior of the terms is what defines the equivalence, and in the case of the denotational semantics, the equivalence is expressed by the denotation of the terms.
Selinger and Valiron

A first notion of equality of terms can be defined by a set of syntactic rules. This is known as the axiomatic equivalence.

**Definition 5.1** We define an equivalence relation $\approx_{ax}$ on typing judgement. We write the relation as $\Gamma \triangleright M \approx_{ax} N : A$, and we define it to be the smallest relation satisfying the rules in Table 4, the alpha-equivalence and one congruence rule $(\xi)$ per term constructor. This means for example:

$$
\frac{
\Gamma \triangleright M \approx_{ax} M' : A \rightarrow B \\
\Delta \triangleright N \approx_{ax} N' : A 
}{
\Gamma, \Delta \triangleright MN \approx_{ax} M'N' : B}
\tag{\xi_{app}}
$$

$$
\frac{
\Gamma, x : A \triangleright M \approx_{ax} M' : B 
}{
\Gamma \triangleright \lambda x.M \approx_{ax} \lambda x.M' : A \rightarrow B}
\tag{\xi_{\lambda}}
$$

We call it the axiomatic equivalence relation.

**Lemma 5.2** The order of the arguments in an application does not matter. Similarly, one can apply the arguments as a pairing or sequentially. More precisely:

$$
[Q, L, ((\lambda xy.M)N)P] \approx_{ax} [Q, L, ((\lambda yx.M)P)N]
$$

$$
[Q, L, let \langle x, y \rangle = \langle N, P \rangle in M] \approx_{ax} [Q, L, ((\lambda xy.M)N)P]
$$

**5.2 Operational context**

To say that two arbitrary terms have the same behavior, we need a way to observe them. The only observable types at our disposal are the types $\text{bit}$ and $\top$. So the fact that two terms $M$ and $M'$ have the same behavior can be understood as the fact that in whichever context $C[-]$ we “use” them, if $C[-] : \text{bit}$, then $C[M]$ reduces to 0, respectively, 1, with the same probability as $C[M']$. Such a term $C[-]$ is called an operational context.

**Definition 5.3** We define a formal operational context to be a formula defined by the following BNF:
\[ C[-] ::= [-] \mid (C[-]M) \mid (MC[-]) \mid \lambda x.C[-] \mid \langle C[-], M \rangle \mid \langle M, C[-] \rangle \]
\[
| \text{let } (x, y) = C[-] \text{ in } M | \text{let } (x, y) = M \text{ in } C[-] \\
| \text{if } C[-] \text{ then } M \text{ else } N | \text{if } M \text{ then } C[-] \text{ else } C'[\cdot].
\]

We call [-] the hole of the context.

The notions of well-typed contexts and free variables in contexts are defined the same ways as for terms. Note that there exists a new notion: the notion of captured variables, which are the variables whose scope includes the hole. We can make this more precise by speaking of typed contexts:

**Definition 5.4** A typed operational context is a typing tree with root \( \Gamma' \triangleright C[-] : B \), considering the additional axiom \( \Gamma \triangleright [-] : A \), i.e., a typing tree of the form
\[
\frac{\Gamma \triangleright [-] : A}{\Gamma' \triangleright C[-] : B}.
\]

We say that this context is of type \( B \), with free variables \( \Gamma' \), a hole of type \( A \), and captured variables \( \Gamma \). We also use the notation \( \Gamma' \triangleright C[\Gamma \triangleright - : A] : B \) for a typed operational context.

**Lemma 5.5** If
\[ \frac{\Gamma \triangleright [-] : A}{\Gamma' \triangleright C[-] : B}. \]
is a valid typing derivation, then so is
\[ \frac{\Delta, \Gamma \triangleright [-] : A}{\Delta, \Gamma' \triangleright C[-] : B}, \]
provided the variables that occur in \( \Delta \) are fresh.

### 5.3 Operational equivalence

We define a notion of operational equivalence, based on the reduction rules and observations of type \( \text{bit} \), as in [2]. (Equivalently, it would suffice to consider observations of type \( \top \)).

**Definition 5.6** Let \( \triangleright C[\Gamma \triangleright - : A] : \text{bit} \) be a closed typed operational context of type \( \text{bit} \), and let \( P = [Q, L, M] \) be a well-typed computation with typing judgement \( \Gamma \Vdash [Q, L, M] : A \). In this case we define the substitution \( C[P] \) by \([Q, L, C[M]]\), where \( M \) is syntactically replacing [-] in \( C[-] \). We linearly extend this definition to probabilistic distributions of programs of the form \( \Gamma \Vdash \sum_i \rho_i P_i : A \) by setting \( C[\sum_i \rho_i P_i] = \sum_i \rho_i C[P_i] \).

**Lemma 5.7** In Definition 5.6, the substitution is well typed and a valid typing judgement for it is \( \Vdash [Q, L, C[M]] : \text{bit} \).
Proof. A direct consequence of Lemma 5.5. \hfill \Box

Definition 5.8 Given two well-typed computations \( \Gamma \triangleright P, P' : A \), we say that \( P \) is operationally equivalent to \( P' \) with respect to \( \Gamma \) if for all closed typed operational contexts \( \triangleright C[\Gamma \triangleright \cdot : A] : \text{bit}, C[P] \downarrow 0 = C[P'] \downarrow 0 \) and \( C[P] \downarrow 1 = C[P'] \downarrow 1 \). In this case, we write \( \Gamma \triangleright P \approx_{\text{op}} P' : A \). If \( M, M' \) are terms, we say that \( \Gamma \triangleright M \approx_{\text{op}} M' : A \) if \( \Gamma \vDash [\cdot], [\cdot], M \approx_{\text{op}} [\cdot], [\cdot], M' : A \).

5.4 Denotational equivalence

The last equivalence we can define is the denotational equivalence. This equivalence relation is simply stated:

Definition 5.9 We say that two typing judgments \( \Gamma \triangleright M, M' : A \) are denotationally equivalent if \( [\Gamma \triangleright M : A] \) and \( [\Gamma \triangleright M' : A] \) are the same map in \( \text{CPM} \). In that case we write \( \Gamma \triangleright M \approx_{\text{den}} M' : A \).

We extend this definition to computations: \( \Gamma \vDash P \approx_{\text{den}} P' : A \) is true if \( [\Gamma \vDash P : A] = [\Gamma \vDash P' : A] \).

6 Soundness of the axiomatic equivalence and full abstraction of the denotational semantics

The three defined equivalence relations we have built have the expected behavior: The axiomatic equivalence is sound with respect to the operational equivalence and the denotational semantic is fully abstract with respect to the operational semantics:

Theorem 6.1 (Soundness) If \( \Gamma \vdash M \approx_{\text{ax}} M' : A \) then \( \Gamma \vdash M \approx_{\text{op}} M' : A \).

An immediate corollary is that the quantum context is not a side-effect, i.e., the order of evaluation does not affect the outcome.

Corollary 6.2 \( \Gamma \triangleright ((\lambda xy.P)M)N \approx_{\text{op}} ((\lambda yx.P)N)M \).

Proof. Using Lemma 5.2 and the soundness theorem. \hfill \Box

Theorem 6.3 (Full abstraction) The denotational semantics is fully abstract with respect to the operational equivalence of typing judgments, i.e.

\[ [\Gamma \triangleright M : A] = [\Gamma \triangleright M' : A] \text{ if and only if } \Gamma \triangleright M \approx_{\text{op}} M' : A. \]

Remark 6.4 The presence of the non-terminating term \( \Omega \) is necessary for full abstraction to hold. Without it, every program terminates with probability 1, and there is only one definable map \( \text{bit} \to \top \). Thus, although \( \lambda f.(f0) \) and \( \lambda f.(f1) \) of type \( \text{bit} \to \top \to \top \) have different denotations, no context will distinguish them.

6.1 Proof of the soundness theorem

Assume Theorem 6.3. It suffices to show that if \( \Gamma \triangleright M \approx_{\text{ax}} M' : A \) then \( \Gamma \triangleright M \approx_{\text{den}} M' : A \). We show this by structural induction on the proof of \( \Gamma \triangleright M \approx_{\text{ax}} M' : A \).

We detail the cases \((\beta^1_{\text{id}})\) and \((\eta)\).
For the \((\beta_1^1)\) case, let \(\Gamma \triangleright M, N : A = f, g : [\Delta] \rightarrow [A]\) and \(\triangleright 1 : bit\) = \((p, q) : 1 \rightarrow 1, 1\). Then \(\Gamma \triangleright if 1 then M else N : A\) : \(1 \otimes y \mapsto (p1)(fy) + (q1)(gy)\) which is \(y \mapsto fy\), namely \(\Gamma \triangleright M : A\).

The case \((\eta)\) is done as follows. Consider the proof tree

\[
\frac{\Gamma \triangleright M : A \rightarrow B \quad x : A \triangleright x : A}{\Gamma \triangleright \lambda x. (Mx) : A \rightarrow B}
\]

and set

\[
[x : A \triangleright x : A] = Id_A : [a] \rightarrow [A]
\]

\[
[\Gamma \triangleright M : A \rightarrow B] = \Phi(g) : [\Delta] \rightarrow [A] \otimes [B].
\]

Then

\[
[\Gamma, x : A \triangleright Mx : B] = f : [\Gamma] \otimes [A] \rightarrow [B]
\]

with \(f(x \otimes y) = g(x \otimes Id_A(y)) = g(x \otimes y)\), and we are done.

Note that cases \((\beta)\) and \((\lambda)\) are done using Lemma 4.2. \(\square\)

### 6.2 Full abstraction: preliminary lemmas

**Lemma 6.5** For any two valid closed computations \(P, P'\) of type \(bit\), they have the same denotation if and only if for all \(b \in \{0, 1\}\), \(P \downarrow b = P' \downarrow b\).

**Proof.** Consider two valid computations \(P, P' : bit\). Suppose they have the same denotation \(f\). Then from Lemma 4.3, \(f\) is also the denotation of \(prob_U P\) and of \(prob_U P'\). But by definition, \([prob_U P] = (p, q)\), where \(p = (prob_U P) \downarrow 0 = P \downarrow 0\) and \(q = (prob_U P) \downarrow 1 = P \downarrow 1\), and similarly for \(P'\). Thus \(P \downarrow b = P' \downarrow b\). The argument being reversible, we get the other implication. \(\square\)

**Lemma 6.6** If \(\Gamma \triangleright M : A = \Gamma \triangleright M' : A\) and \(C[\Gamma \triangleright - : A] : bit\) is a valid context, then \([C[M] : bit] = [C[M'] : bit]\).

**Proof.** The proof uses Lemma 4.2. \(\square\)

**Definition 6.7** Given a type \(A\), we define the **canonical first-order representation** \(\overline{A}\) of \(A\) by the following: \(\overline{bit} = bit, \overline{qbit} = qbit, \overline{\top} = \top, \overline{A \otimes B} = \overline{A} \otimes \overline{B}, \overline{A \rightarrow B} = \overline{A} \otimes \overline{B}\).

**Lemma 6.8** For all types \(A\), \([A] = [\overline{A}]\).

**Lemma 6.9** For all types \(A\), there exist two terms \(x : A \triangleright \gamma_A : A\) and \(x : A \triangleright \gamma_A : A\) and constants \(\lambda, \lambda' > 0\), such that \([\gamma_A] = \lambda \text{id}_{[A]}\) and \([\gamma_A] = \lambda' \text{id}_{[A]}\).

**Proof.** The terms \(\gamma_A\) and \(\gamma_A\) are simultaneously constructed by structural induction on \(A\). \(\square\)

**Lemma 6.10** For all types \(A\), let \(\sigma = [A]\) and let \(m, m'\) be hermitian positive elements in \(V_\sigma\), \(m \neq m'\). Then there exists a well-typed term \(x : A \triangleright M : bit\) such that \([M](m) \neq [M](m')\).

**Proof.** By Lemma 6.9, it suffices, without loss of generality, to consider the case where \(A = bit \otimes \ldots \otimes bit \otimes qbit \otimes \ldots \otimes qbit\). However, in this case, the claim follows easily from Proposition 4.4 on the fullness of the semantics in first order. \(\square\)
Lemma 6.11 Given any type $A$ and any hermitian positive $v \in V[A]$, there exists a closed term $M : A$ and $\lambda > 0$ such that $\llbracket M \rrbracket(1) = \lambda v$.

Proof. By Corollary 4.5 and Lemma 6.9. \hfill \Box

6.3 Proof of the full abstraction theorem

If $\llbracket \Gamma \triangleright M : A \rrbracket = \llbracket \Gamma \triangleright M' : A \rrbracket$, take any valid context $C[\Gamma \triangleright - : A] : bit$ for those two terms. Then from Lemma 6.6, $\llbracket \triangleright C[M] : bit \rrbracket = \llbracket \triangleright C[M'] : bit \rrbracket$. From Lemma 6.5, $C[M] \downarrow b = C[M'] \downarrow b$, for $b \in \{0,1\}$. Since this holds for arbitrary contexts, $M$ and $M'$ are operationally equivalent.

The opposite implication follows from Lemma 6.10 and Lemma 6.11. Consider two typing judgments $\Gamma \triangleright M, M' : A$ with denotations $F=\llbracket \Gamma \triangleright M : A \rrbracket$ and $G=\llbracket \Gamma \triangleright M' : A \rrbracket$, such that $F \neq G$. Since the vector space $V[\Gamma]$ is spanned by hermitian positive elements, there exists a hermitian positive $v \in V[\Gamma]$ such that $F(v) \neq G(v)$.

If $\Gamma = x_1 : A_1, \ldots, x_n : A_n$, let $B = A_1 \otimes \ldots \otimes A_n$. By Lemma 6.11, there exists a closed term $R : B$ such that $\llbracket R : B \rrbracket(1) = \lambda v$, for some $\lambda > 0$. By Lemma 6.10, there exists a term $x : A \triangleright S : bit$ such that $\llbracket x : A \triangleright S : bit \rrbracket(Fv) \neq \llbracket x : A \triangleright S : bit \rrbracket(Gv)$. Now consider $C[\Gamma \triangleright - : A] : bit$ defined by

$$let \langle x_1, \ldots, x_n \rangle = R \text{ in let } x = [-] \text{ in } S.$$  

Then $\llbracket C[M] \rrbracket(1) \neq \llbracket C[M'] \rrbracket(1)$, hence by Lemma 6.5, $C[M] \downarrow b \neq C[M'] \downarrow b$, for some $b \in \{0,1\}$. It follows that $M \neq_{op} M'$, which completes the proof of full abstraction. \hfill \Box

7 Conclusion

In this paper we have restricted our study to the linear fragment of the programming language of [4]. We gave a syntactic notion of equivalence of terms and an operational one, together with a fully abstract model for the latter.

Several questions remain open. First, the exact image of the denotational semantics is still to be characterized as a subset of the completely positive maps. Then it would be interesting to explore the categorical semantics of the linear language. Finally, we may want to add weakening and duplication and find a denotational semantics for the full quantum lambda calculus.

References

[1] Barendregt, H. P., “The Lambda-Calculus, its Syntax and Semantics,” Studies in Logic and the Foundation of Mathematics 103, North Holland, 1984, second edition.

[2] Danos, V. and R. S. Harmer, Probabilistic game semantics, ACM Transactional on Computational Logic 3 (2002), pp. 359–382.

[3] Selinger, P., Towards a quantum programming language, Mathematical Structures in Computer Science 14 (2004), pp. 527–586.

[4] Selinger, P. and B. Valiron, A lambda calculus for quantum computation with classical control, in: P. Urzyczyn, editor, Proceedings of the Seventh International Conference on Typed Lambda Calculus and Applications (TLCA 2005), Lecture Notes in Computer Science 3461 (2005), pp. 354–368.
