# Tutorial on Quantum Lambda-Calculus

Benoît Valiron

November 4, 2019

**Abstract**

In this tutorial, we shall discuss higher-order in quantum computation. First we shall briefly present the general concept of quantum computation and expose the problems arising while mixing quantum data with higher-order. We shall present the various attempts and their possible shortcomings. We will then present a lambda-calculus for quantum computation with classical control. We shall discuss its operational semantics, its expressivity and develop a type system based on linear logic, enforcing safety properties.

In a second step, we shall investigate denotational semantics of quantum higher-order based on completely positive maps. We shall consider the case of strictly linear programs (i.e. without duplication) and, as an example, discuss the interpretation of Bell's inequality in this context. We will then turn to the question of extending the semantics to support the interpretation of duplicable objects. Finally, if time permits, we shall sketch the direction taken by recent advances in quantum programming languages, with the development of circuit-description languages, and the problem of quantum control.

# 1 Quantum Computation

## 1.1 Mathematical Formalism of the Quantum Memory

See [8, pp. 17-19].

1. Notion of Hilbert space
2. Tensor product
3. Basis and order of basis elements
4. Matrix representation of operators; block-representation

## 1.2 Quantum Data and Quantum Operations

See [8, pp. 19-20.23-26].

1. One quantum bit; several quantum bits
2. Unitary operation [8, Lem. 2.1.15]. The following are equivalent:
   - $A^* = A^{-1}$
   - $\|Ax\| = \|x\|$ for all $x \in \mathbf{H}$
   - $\langle Ax | Ay \rangle = \langle x | y \rangle$
   - $\|Ax\| = 1$ for all unit vectors $x \in \mathbf{H}$
3. Measurement; notion of mixed state

### 1.3 Standard Model

1. Density matrix as equivalence class representative of mixed states
2. Positive matrix; positive and completely positive map, superoperator
3. Löwner ordering; the zero-matrix as diverging program; bdcpo
4. Characteristic matrix; Choi theorem [8, Th. 3.1.24].
   *Let $F : \mathbb{C}^{n\times n} \longrightarrow \mathbb{C}^{k\times k}$ linear, and let $\chi_f$ be its characteristic matrix. Then the following are equivalent:*
   - *$F$ is completely positive*
   - *$\chi_F$ is positive*
   - *$F$ is of the form $F(A) = \sum_i U_i A U_i^*$ for some finite sequence of matrices $U_i \in \mathbb{C}^{k\times n}$*

### 1.4 Quantum Effects

1. No-cloning
2. Entanglement
3. Teleportation: See [8, pp. 28-30]; speak of dense coding
4. Bell's inequality: See [8, p. 27] (and [9])
   - Notion of measure according to a basis
   - Alice and Bob get each a qubit from the entangled pair

$$\frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$$

   - Bases of measurements to choose from for Alice and Bob:

$$\begin{aligned} a &= \left(|0\rangle, \qquad\qquad |1\rangle\right) \\ b &= \left(\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle, \qquad \frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle\right) \\ c &= \left(\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle, \qquad \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right) \end{aligned}$$

   - Let $P_{x,y}$ be the probability to measure the same output when Alice chooses basis $x$ and Bob basis $y$.
   - With classical probabilities:

$$P_{a,b} + P_{b,c} + P_{c,a} \geq 1$$

   - But if one computes it we get $\frac{3}{4}$

## 2 Programming with Quantum Computation

1. Quantum circuits; measurements at the end
2. Quantum data & classical control; Knill's QRAM model [4]
3. Classical control versus quantum control

## 3 Functional Quantum Computation

Main idea: a circuit is a function from qubits to qubits.

### 3.1 Classical Control

1. What we would like to do: $\lambda f.(fq)$ where $q$ is a qubit.
2. First idea : add one constant per possible qubit state.
3. Problem: entangled elements, such as

$$(g(fp))(hq) \qquad \text{where} \qquad |pq\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big).$$

4. Solution: separating the quantum state from the term
5. Problem: $(\lambda xf.(fx)x)q$, duplicating $q$
6. Solution: use of a *linear* type system (see later)

### 3.2 Quantum Control

1. Controling a gate can be regarded as a *quantum test*
2. There must therefore be a notion of *quantum control*
3. Formalizing q-tests: QML [1]
   - Compositional tests
   - Basic type system with qubits and tensors
   - No loop, low expressivity
4. Attempt at going higher-order: van Tonder [10].
   - With a unitary evolution
   - Hard to keep norm, orthogonality
   - Requires to keep history; term in superpositions all alike!

### 3.3 Mixing Quantum and Classical

1. Löwner order — i.e. measures — not compatible with quantum tests:
   See Badescu & Panangaden's "*Quantum Alternation*" [2]
2. Provided one goes "full quantum", it can work — see Sect. 8
3. Caveat: Termination is a classical concept!

## 4 A Quantum $\lambda$-Calculus with Classical Control

See [7].

1. Terms; Abstract machine
2. Operational semantics with probabilistic behavior
3. Call-by-value versus call-by-name with the probabilistic effect:
   Is `new tt` duplicable?
4. Destructive measurement and garbage collection
5. Quantum memory: side-effect or purely functional?
6. Run-time errors and linear type system:
   - Duplicable and non-duplicable data
   - Subtyping
   - Affine versus strict type systems
7. Safety properties

8. Example: teleportation [8, pp. 64-68]
   A pair of non-duplicable functions, inverse one of the other.
9. Example: Bell inequalities [9, Sect. 4]
   A purely classical type!

# 5 CPMs as a Denotational Model

1. Notion of category
   - Objects; morphisms; homset; (bi)functor
   - Example: **Set**, **FinVec**, any poset, syntactic category
   - Product; coproduct; biproduct; internal hom (notion of adjunction)
   - Monoidal structure; internal hom; SMCC
2. CPM as a category
   - First-order types: qubits, monoidal structure
   - CPM as a SMCC category; compact-closure
   - Interpreting bits: the biproduct completion
   - Explicit presentation with signature ; examples

# 6 The Strictly Linear Fragment

See [9, pp. 70-...].

1. Terms; types (with trits)
2. CPM as a denotational model [9, pp. 83-...]
3. Adequacy
4. Fullness up to a scalar
   - Correspondence between H-O and F-O types
   - Give an example for $bit$ and $(bit \multimap 1) \multimap 1$
5. Full abstraction [9, pp. 89-...]
   - Context ; observational equivalence ; statement of the result
   - Denotation is compositional: "$[\![MN]\!] = [\![M]\!][\![N]\!]$"
   - Denotation is adequate with respect to $bit$.
   - Let $v \neq w$ be two elements of $[\![A]\!]$. There exists $x : A \vdash M : bit$ such that $[\![M]\!](v) \neq [\![M]\!](w)$
   - Denotational equivalence implies observational equivalence
     - Suppose $[\![M : A]\!] = [\![N : A]\!]$
     - Take any context $C[- : A] : bit$
     - By compositionality: $[\![C[M]]\!] = [\![C[N]]\!]$
     - Conclude by adequacy
   - Observational equivalence implies denotational equivalence
     - Suppose that $[\![x : A \vdash M : B]\!] \neq [\![x : A \vdash N : B]\!]$
     - Then there is $v \in [\![A]\!]$ such that $[\![M]\!](v) \neq [\![N]\!](v)$
     - By fullness up to a scalar, there exist $P : A$ and $\varepsilon > 0$ such that $[\![P]\!] = \varepsilon \cdot v$.
     - Let $R$ be the term mapping $B$ to its first-order image
     - Morally, take the context $C[-] = R((\lambda x.[-])P)$

6. Bell inequalities: Non-conservativity of quantum over prob. $\lambda$-calculus
    - Structure of a deterministic program of type

$$(trit \multimap bit) \otimes (trit \multimap bit)$$

    - There are $3^6 = 729$ distinct such programs
    - Generate a polytope in $3 \cdot 2 \cdot 3 \cdot 2 = 36$ dimensions
    - (very small 0/1-polytope : $2^{36}$ possible vertices)
    - With respect to the canonical basis:

$$\left(\frac{1}{2}, 0, \frac{1}{8}, \frac{3}{8}, \frac{1}{8}, \frac{3}{8}, 0, \frac{1}{2}, \frac{3}{8}, \frac{1}{8}, \frac{3}{8}, \frac{1}{8}, \frac{1}{8}, \frac{3}{8}, \frac{1}{2}, 0, \frac{1}{8}, \frac{3}{8}, \right.$$
$$\left. \frac{3}{8}, \frac{1}{8}, 0, \frac{1}{2}, \frac{3}{8}, \frac{1}{8}, \frac{1}{8}, \frac{3}{8}, \frac{1}{8}, \frac{3}{8}, \frac{1}{2}, 0, \frac{3}{8}, \frac{1}{8}, \frac{3}{8}, \frac{1}{8}, 0, \frac{1}{2}\right)$$

# 7 Adding Non-duplication

See [5]. Example of program we care about representing:

```
val entangle : qubit ⊸ qubit ⊗ qubit
let entangle x = CNOT (x, new ff)

val qlist : qubit ⊸ qubit list
let rec qlist q = if (cointoss) then [q]
                  else let (x,y) = entangle q in x::(qlist y)
```

## 7.1 The Problem

1. Consider $t : !(1 \multimap qubit)$. What is one copy of $t$? Two copies?
2. Representing all of $!(1 \multimap qubit)$
3. Going from finite dimension to infinite dimension: composability of functions.
4. Denotation of recursion

## 7.2 Solution

1. Start with vanilla CPM without biproducts
2. **CPMs** : positive cones modulo a permutation of lines and rows.
3. $\overline{\textbf{CPMs}}$: D-completion of the Löwner order.
    - Let $P$ a poset
    - Let $\Gamma(P)$ be the set of all Scott-closed subsets of $P$.
    - This is a dcpo under subset-ordering
    - Let $c(P)$ be the smallest sub-dcpo of $\Gamma(P)$ containing all $\downarrow x$.
    - If $P$ is a bdcpo, then $c(P)$ preserves existing limits.
4. $\overline{\textbf{CPMs}}^{\oplus}$: infinite biproduct-completion

## 7.3 Properties

1. Adequacy
2. No infinite elements in the representation of a program

# 8 Moving Forward

1. Circuit description languages
2. Higher-order and quantum control
    - Quantum switch [3]
    - Quantum pattern matching and iteration [6]

# References


[1] Thorsten Altenkirch and Jonathan Grattage. A functional quantum programming language. In Prakash Panangaden, editor, *Proceedings of the 20th Symposium on Logic in Computer Science (LICS'05)*, pages 249–258, Chicago, Illinois, US., June 2005. IEEE, IEEE Computer Society Press.

[2] Costin Badescu and Prakash Panangaden. Quantum alternation: Prospects and problems. In Chris Heunen, Peter Selinger, and Jamie Vicary, editors, *Proceedings of the 12th International Workshop on Quantum Physics and Logic, QPL 2015*, volume 195 of *EPTCS*, pages 33–42, Oxford, UK, 2015.

[3] G. Chiribella, G. M. D'Ariano, P. Perinotti, and B. Valiron. Quantum computations without definite causal structure. *Physical Review A*, 88:022318, 2013.

[4] Emanuel H. Knill. Conventions for quantum pseudocode. Technical Report LAUR-96-2724, Los Alamos National Laboratory, 1996.

[5] Michele Pagani, Peter Selinger, and Benoît Valiron. Applying quantitative semantics to higher-order quantum computing. In Suresh Jagannathan and Peter Sewell, editors, *Proceedings of the 41st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL'14)*, pages 647–658, San Diego, California, USA, 2014. ACM.

[6] Amr Sabry, Benoît Valiron, and Juliana Kaizer Vizzotto. From symmetric pattern-matching to quantum control. In Christel Baier and Ugo Dal Lago, editors, *Proceedings of the 21st International Conference on Foundations of Software Science and Computation Structures (FOSSACS'18)*, volume 10803 of *Lecture Notes in Computer Science*, pages 348–364, Thessaloniki, Greece, 2018. Springer.

[7] Peter Selinger and Benoît Valiron. A lambda calculus for quantum computation with classical control. *Mathematical Structures in Computer Science*, 16:527–552, 2006.

[8] Benoît Valiron. *Semantics for a Higher Order Functional Programming Language for Quantum Computation.* PhD thesis, University of Ottawa, 2008.

[9] Benoît Valiron. On quantum and probabilistic linear lambda-calculi (extended abstract). In B. Coecke, I. Mackie, P. Panangaden, and P. Selinger, editors, *Proceedings of the Joint 5th International Workshop on Quantum Physics and Logic and 4th Workshop on Developments in Computational Models (QPL/DCM 2008)*, volume 270 of *Electronic Notes in Theoretical Computer Science*, pages 121–128, Reykjavik, Iceland, 2011.

[10] André van Tonder. A lambda calculus for quantum computation. *SIAM Journal on Computing*, 33(5):1109–1135, 2004.