Research Proposal:
Quantum Computation and Algebraic Structures in Semantics

Benoît Valiron

Abstract

La théorie des algèbres d'opérateurs est jointe à la fois au monde du calcul quantique, car celui-ci est basé sur les espaces de Hilbert, et aux modèles de la logique linéaire, les espaces d'opérateurs, de part leur richesse en terme topologique, offrant des possibilités extraordinaires pour caractériser finement les structures logiques. Le projet de recherche est le suivant. Le calcul quantique donnant un sens calculatoire à des processus physiques, la question est de donner un sens logique, sous l'angle d'une correspondance de Curry-Howard, au calcul ainsi obtenu. C'est une question qui, si elle est difficile, peut du moins se laisser attaquer en utilisant un modèl algébrique et vectoriel. En particulier, deux premières questions qui méritent qu'on s'y attarde sont les suivantes. Les catégories différentielles donnent une interprétation fine de la notion de linéarité. Quelle est la relation avec le calcul quantique ? Enfin, comme le calcul quantique trouve son interprétation dans les espaces d'opérateurs, peut-on construire une correspondance de Curry-Howard dans ce cas restreint ?

1 Introduction

My research interests are in the foundations of computer science. I enjoy working on the semantics of typed programming languages and on models of intuitionistic linear logic. I like applying categorical tools to these fields to examine the fundamental structures underlying them.

The main focus of my research has been the semantics of programming languages related to quantum computation. I am particularly interested in the combination of structures arising from the theory of operator spaces with logical structures. Much of my research has been concerned with studying a quantum lambda calculus and its type system, using methods from linear algebra, domain theory, and category theory. I am now working on the semantics of a lambda-calculus together with a structure of vector space.

These works on quantum and algebraic structures convinced me that research need to be done in order to relate in details the theory of operator spaces and proof theory, and that a ladder to get there is quantum computation.

2 Background

Semantics of programming languages. A semantics for a programming language is a mathematical representation of the set of valid terms. It serves several purposes: one can use it do decide on the validity of a given program, or to understand the possibilities of what can be done with the language in general.

Functional programming languages are languages intepreting programs as processes on wires, inputting some data and outputting some other data and without modifying the overall environment. In a typed setting, a program is a "function" whose domain is the datatype of input and whose codomain is the datatype of output. But, through the Curry-Howard correspondence (Howard, 1980), a program is also the proof of a proposition in a particular logic. The study of the corresponding logic gives precious informations on the language, and conversely, the study of the language helps understanding the structure of proofs in the logic.

A rich enough logic admits a notion of conjunction and a notion of implication. In the type system, these correspond to product and function types: this is the realm of higher-order computation. A higher order function is a function that inputs or outputs a "black box", which is itself a function. The canonical formalism for expressing higher order functions is the lambda-calculus developed by Church (1936) and Kleene (1935a,b) to characterize computable functions.

Quantum computation. In classical computation, the boolean structure is a finite, discret structure, usually composed of two elements. In quantum computation, the boolean structure is a smooth structure issued from the theory of Hilbert spaces. A quantum boolean is a normalized vector in a two-dimensional Hilbert space. The operations one can performed on a quantum boolean are well-known and described by the laws of quantum physics. One can perform unitary operations, that is, linear, isometric maps of Hilbert spaces, and measurements, which are probabilistic, destructive operations (Nielsen and Chuang, 2002). In particular, there is no possibility of cloning a quantum bit (Wootters and Zurek, 1982). From a programmer perspective, there are two potential problems: the mix of duplicable and non-duplicable data, and the probabilistic side-effect.

Semantics of quantum computation. Several authors have been studying the mathematical structure of quantum computation.

(Abramsky and Coecke, 2004) and (Selinger, 2005b) explore the logical structures behind Hilbert spaces using monoidal categories with coproduct and dagger compact closed structures. In a relatively general framework, notions of base, unitary maps, scalars and duals naturally appear. In (Coecke and Pavlovic, 2007), this setting is even more precised using the notion of "classical objects" to model measurements without the coproduct requirement. (Coecke and Paquette, 2006) is able to prove an abstract version of the theorem of Naimark in this categorical framework.

Without measurement, the question of duplicability versus non-duplicability vanishes since there is no classical object anymore. (Altenkirch, Grattage, Vizzotto, and Sabry, 2005) provides a full and complete semantics for a first-order functional language without measurements. This semantics is based on the category of finite dimensional Hilbert spaces and isometries, and the paper highlights its relation with the category of finite sets. Regarding higher order, (van Tonder, 2004) describes a purely quantum lambda-calculus but does not provide any denotational semantics.

In the case of quantum computation with measurements, a non-duplicable type (the quantum bit) and a duplicable type (the classical bit) appear. (Selinger, 2004b) shows that the notion of superoperator provides a full and complete model for first-order quantum computation with measurements. However, as shown in (Selinger, 2004c) this interpretation does not generalize easily at higher order. Indeed, the notion of normed vector space used in the first-order situation does not provide a satisfactory category for modelling higher-order quantum computation. (Valiron, 2004a,b) and (Selinger and Valiron, 2006a, 2005) describes a typed quantum lambda-calculus and its operational semantics. (Valiron, 2008a,b) and (Selinger and Valiron, 2006b, 2008) solve the many problems that occurs while defining a higher-order language and describing its semantics.

Algebra in logic. The study of the relation between algebraic and logical structure is not restricted to the realm quantum computation. Indeed, many works on semantics of linear logic, a resource-sensitive logic introduced by Girard (1987), make use of topological vector space and functional analysis to solve questions related to resource-sensitivity. The question of duplicability is captured in linear logic by controlling the occurrence of non-linear behavior (weakening, contraction) in the construction of the proof. In functional analysis and theory of operator spaces, the distinction between linearity and non-linearity is controlled by continuity and differentiability with the use of topological vector spaces.

(Blute, Panangaden, and Seely, 1993b) and (Girard, 2004) describe models of the exponential "!" of linear logic using a category of complex vector spaces and holomorphic functions. In this setting, linearity in the logic is interpreted as linear maps in the model and non-linearity in the logic

as differentiable maps in the model. In a similar vein, (Ehrhard and Regnier, 2003) proposes an algebraic lambda-calculus with explicit sums and differential operators. (Blute, Cockett, and Seely, 2006) axiomatizes this differential calculus and describes the notion of differential categories, capturing a categorical analog of differentiation in an additive symmetric monoidal category.

The notion of duality in linear logic is very important: each connective admits a dual one through the use of the negation operator. A notion of dual can be expressed algebraically in the theory of Hopf algebra (Kassel, 1995). (Blute, 1996; Blute and Scott, 1998; Ehrhard, 2002) draw a correspondence between the two approaches and model duality in linear logic using Hopf algebras.

In its work on geometry of interaction, Girard (1989a,b) provides an algebraic characterization of the "invariant" of a proof. In particular, it interprets proofs and cut elimination as operators on Hilbert spaces, and use the existence of traces on these spaces. The use of norms on operator spaces allows the interpretation of the subtle behavior of proof normalization in the context of the exponential operator "!". Many works such as (Danos and Regnier, 1995; Girard, 1995; Haghverdi and Scott, 2004, 2006) extend these ideas and study the algebraic invariants of proofs issued from this interpretation.

(Vaux, 2008) and (Arrighi and Dowek, 2008) are both concerned with untyped lambda-calculi endowed with a structure of vector space. The main issue they try to address is the question of normalization and confluence in such a system. Although they consider similar questions, these works come from very different approaches: the former paper builds on the differential calculus (Ehrhard and Regnier, 2003) whereas the latter one considers a generalization of the calculus of van Tonder (2004). (Valiron, 2009) develops a semantics for a typed algebraic language and sketches an understanding of the notion of divergence in the context of linear combinations of terms, using denotations based on the adjunction between the category of sets and various categories of modules. This study catches the subtle distinctions existing between the several notions of divergence occuring in the language.

3 Research Proposal

As stated by Deutsch (1985), quantum computation allows one to have "every finitely realizable physical system perfectly simulated by a universal model computing machine operating by finite means", this machine being a quantum Turing machine. In a sense, quantum Turing machines give an computational meaning to physical processes.

If quantum Turing machines provide an operational meaning to quantum physics, they are not giving a denotational semantics to it. In a Curry-Howard sense, what does "computable" mean for physical processes ? In particular, what is the logic behind a given physical system ? On another level, what about the computational power of a given physical system versus the a quantum one, versus classical computation ? What sense to give to the word "powerful" ? And what about the power of the mathematical description of a world "close enough" to ours ?

These questions are not new, are very hard, and maybe form a project for several lives. The proposed research project is, if not getting answers to all of these questions, at least looking at them with the powerful tool of algebraic structures and notions issued from the theory of operator spaces: norms, topological vector space, category theory... Indeed, quantum computation is a lense that gives computational meaning to these mathematical objects, and therefore, computational meaning to the quantum world. Second, these mathematical structures have already been heavily used in logic, as their structures reflect many structures encountered along the study of logical systems. I strongly believe that important pieces of information can be gathered by attacking these problems with this semantical lever.

As first steps towards these long-term objectives, the following can already be examined and sketch the beginning of a research path.

- Study the relation between differential categories and models of quantum computation. Since differential categories distinguish between linear and non-linear functions, it is natural to investigate how they relate to models provided by quantum computation, whether they consider measurement or not.

- Develop a Curry-Howard correspondence between resource-sensitive logical systems and algebraic structures issued from the theory of operator spaces. Quantum computation provides a natural computational interpretation of operators whereas the theory of operator spaces provide a rich variety of structures.

Having been in a competitive university in Canada for several years gives me a solid knowledge in mathematics and theoretical computer science, and a serious methodology. I worked on models of quantum computations and on various higher-order systems dealing with vectorial structures, I feel therefore confident in being able to attack this project. Bridging semantics of programming languages, physics and mathematics, this research is open to many collaboration from researchers in mathematics, computer science and physics, and should bring novel ideas and challenging twists and turns.

References

Samson Abramsky and Bob Coecke. A categorical semantics of quantum protocols. In *Proceedings of the 19th Symposium on Logic in Computer Science, LICS'04*, pages 415–425, 2004.

Thorsten Altenkirch, Jonathan Grattage, Juliana K. Vizzotto, and Amr Sabry. An algebra of pure quantum programming. In Selinger (2005a), pages 23–47.

Pablo Arrighi and Gilles Dowek. Linear-algebraic lambda-calculus: higher-order, encodings, and confluence. In *Proceedings of the 19th international conference on Rewriting Techniques and Applications (RTA'08)*, volume 5117 of *Lecture Notes in Computer Science*, pages 17–31, 2008.

Richard F. Blute. Hopf algebras and linear logic. *Mathematical Structures in Computer Science*, 6: 189–217, 1996.

Richard F. Blute and Philip Scott. The shuffle hopf algebra and noncommutative full completeness. *Journal of Symbolic Logic*, 63:1413–1435, 1998.

Richard F. Blute, Prakash Panangaden, and Robert A.G. Seely. Holomorphic models of exponential types in linear logic. In *Mathematical Foundations of Programming Semantics: Ninth International Conference*, volume 802 of *Lecture Notes in Computer Science*, pages 474–512, 1993a.

Richard F. Blute, Prakash Panangaden, and Robert A.G. Seely. Fock space: A model of linear exponential types. Manuscript, revised version of Blute, Panangaden, and Seely (1993a)., 1993b.

Richard F. Blute, J. Robin B. Cockett, and Robert A.G. Seely. Differential categories. *Mathematical Structures in Computer Science*, 16:1049–1083, 2006.

Alonzo Church. An unsolvable problem of elementary number theory. *American Journal of Mathematics*, 58:345–363, 1936.

Bob Coecke and Eric O. Paquette. POVMs and Naimark's theorem without sums. In Selinger (2006), pages 15–31.

Bob Coecke and Dusko Pavlovic. Quantum measurements without sums. In Goong Chen, Louis Kauffman, and Samuel J. Lomonaco, editors, *Mathematics of Quantum Computation and Quantum Technology*, pages 559–592. Taylor and Francis CRC Press, 2007.

Vincent Danos and Laurent Regnier. Proof-nets and the Hilbert space. In Jean-Yves Girard, Yves Lafont, and Laurent Regnier, editors, *Advances in Linear Logic*, pages 307–328. Cambridge University Press, 1995.

David Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences*, 400: 97–117, 1985.

Thomas Ehrhard. On Köthe sequence spaces and linear logic. *Mathematical Structures in Computer Science*, 12(5):579–623, 2002.

Thomas Ehrhard and Laurent Regnier. The differential lambda-calculus. *Theoretical Computer Science*, 309(1–2):1–41, 2003.

Jean-Yves Girard. Between logic and quantic: A tract. In Thomas Ehrhard, Jean-Yves Girard, Paul Ruet, and Philip Scott, editors, *Linear logic in computer science,*. Cambridge University Press, 2004.

Jean-Yves Girard. Linear logic. *Theoretical Computer Science*, 50:1–101, 1987.

Jean-Yves Girard. Towards a geometry of interaction. In J. W. Gray and Andre Scedrov, editors, *Categories in Computer Science and Logic*, volume 92 of *Contemporary Mathematics*, pages 69–108. American Mathematical Society, 1989a.

Jean-Yves Girard. Geometry of interaction 1: Interpretation of system f. In R. Ferro and al, editors, *Logic Colloquium 88*. North Holland, 1989b.

Jean-Yves Girard. Geometry of interaction iii: Accommodating the additives. In Jean-Yves Girard, Yves Lafont, and Laurent Regnier, editors, *Advances in Linear Logic*, pages 329–389. Cambridge University Press, 1995.

Esfandiar Haghverdi and Philip Scott. From geometry of interaction to denotational semantics. In Lars Birkedal, editor, *Proceedings of the Tenth International Conference on Category Theory and Computer Science, CTCS'04*, volume 122 of *Electronic Notes in Theoretical Computer Science*, pages 67–87, Copenhagen, Denmark, 2004.

Esfandiar Haghverdi and Philip Scott. A categorical model for the geometry of interaction. *Theoretical Computer Science*, 350:252–274, 2006.

W. Howard. The formulae–as–types notion of construction. In J. P. Seldin and J. R. Hindley, editors, *To H.B. Curry: essays on combinatory logic, lambda calculus, and formalism*, pages 479–490. Academic Press, 1980.

Christian Kassel. *Quantum Groups*, volume 155 of *Graduate Texts in Mathematics*. Springer Verlag, 1995.

Stephen C. Kleene. A theory of positive integers in formal logic, part I. *American Journal of Mathematics*, 57:153–173, 1935a.

Stephen C. Kleene. A theory of positive integers in formal logic, part II. *American Journal of Mathematics*, 57:219–244, 1935b.

Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2002.

Peter Selinger, editor. *Proceedings of the Second International Workshop on Quantum Programming Languages*, volume 33 of *TUCS General Publication*, 2004a.

Peter Selinger, editor. *Proceedings of the 3rd International Workshop on Quantum Programming Languages (QPL 2005)*, volume 170 of *Electronic Notes in Theoretical Computer Science*, Chicago, Illinois, US., 2005a.

Peter Selinger, editor. *Proceedings of the Fourth International Workshop on Quantum Programming Languages*, volume 210 of *Electronic Notes in Theoretical Computer Science*, Oxford, UK., 2006.

Peter Selinger. Towards a quantum programming language. *Mathematical Structures in Computer Science*, 14:527–586, 2004b.

Peter Selinger. Towards a semantics for higher-order quantum computation. In *Proceedings of the Second International Workshop on Quantum Programming Languages* Selinger (2004a), pages 127–143.

Peter Selinger. Dagger compact closed categories and completely positive maps. In *Proceedings of the 3rd International Workshop on Quantum Programming Languages (QPL 2005)* Selinger (2005a), pages 139–163.

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

Peter Selinger and Benoît Valiron. A lambda calculus for quantum computation with classical control. In *Proceedings of the Seventh International Conference on Typed Lambda Calculi and Applications, TLCA'05*, volume 3461 of *Lecture Notes in Computer Science*, pages 354–368, 2005.

Peter Selinger and Benoît Valiron. On a fully abstract model for a quantum linear functional language. In Selinger (2006), pages 123–137.

Peter Selinger and Benoît Valiron. A linear-non-linear model for a computational call-by-value lambda calculus. In *Proceedings of FOSSACS'08, Budapest, March 29 - April 6, 2008*, volume 4962 of *Lecture Notes in Computer Science*, pages 81–96. Springer Verlag, 2008.

Benoît Valiron. A functional programming language for quantum computation with classical control. Master's thesis, University of Ottawa, 2004a.

Benoît Valiron. Quantum typing. In Selinger (2004a).

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

Benoît Valiron. On quantum and probabilistic linear lambda-calculi (extended abstract). In *Proceedings of the joint 5th QPL and 4th DCM: Quantum Physics and Logic and Development of Computational Models (QPL/DCM 2008)*, Reykjavik, 2008b. To appear.

Benoît Valiron. About typed algebraic lambda-calculi. Draft, accessible on the author's website[1], 2009.

André van Tonder. A lambda calculus for quantum computation. *SIAM Journal of Computing*, 33: 1109–1135, 2004.

Lionel Vaux. Algebraic lambda-calculus. *Mathematical Structures in Computer Science*, 2008. To appear.

William K. Wootters and Wojciech H. Zurek. A single quantum cannot be cloned. *Nature*, 299: 802–803, 1982.

[1] `http://www.monoidal.net/research.html`