Carlo Emerencia

- Category Theory background:
    - Categories
    - Functors
    - Natural transformations
    - All types of (co)limits
    - Adjoint functors
    - Equivalence of categories
    - Localization
    - Applications in:
        - Algebraic Geometry
        - Algebraic Topology
        - Representations of finite/algebraic groups

- Background relevant for ACT:
    - Algebra: vector spaces, group and ring theory, …
    - Basics of quantum computing (qubits, states, superposition, tensor product of states, general measurements, quantum gates (in particular the Quantum Fourier transform), …)
    - Quantum algorithms (Shor, Simon, Grover, …)
    - Graph theory (vertices, edges, adjacency, degree of a vertex, directedness, connectedness, isomorphism of graphs, trees, bipartite graphs, matchings, planar graphs, …)

- PhD expected to be complete: 30th of September 2024

- Summary PhD:
  Post-Quantum Cryptography based on algebra and quantum annealing.

- Project preference order:
    1. "Simplifying quantum circuits using the ZX-calculus (Miriam Backens)
    2. "Complexity classes, computation and Turing categories (Pieter Hofstra)
    3. "Traversal optics and profunctors" (Bartosz Milewski)
    4. "Partial evaluations, the bar construction and second-order stochastic dominance (Tobias Fritz)
    5. Formal and experimental methods to reason about dialogue and discourse using categorical models of vector spaces (Mehrnoosh Sadrzadeh)
    6. Towards a mathematical foundation for autopoiesis (David Spivak)

- Coming to Oxford:
    - By train

- o Funding is possible
- o Available during the period between July 15 and July 26

- Motivation:

Current digital security is endangered by the evolution of quantum computers. They can run algorithms to break cryptosystems based on hard number-theoretical problems, such as RSA which relies on prime factorization. Shor's algorithm for example, which I studied thoroughly in my Master thesis, can efficiently solve this problem and also the discrete logarithm problem (the basis of ElGamal). The key lies within considering both problems as a specific instance of the so-called Hidden Subgroup Problem (HSP). The goal of my research lies within the study of the HSP for post-quantum cryptography: I will investigate the security of post-quantum candidates from an algebraic as well as a practical point of view. A promising way to reach this goal is by invoking the theory of diagrammatic reasoning (and in particular the classification of strongly complementary spiders). It allows us to not only perform our computations in a more compact way but also to gain more insight in the methodology. Both advantages are due to the graphical notation, while still having the ability to apply algebraic relations to obtain a reduced gate network. As tensor networks are suited to simulate spins according to the Ising model in condensed matter physics, we hope this will also lead us to implementations of our algorithm on a quantum annealer.
I believe that Category Theory is a clear and natural language to get a better understanding of the link between tensor networks, ZX-calculus and condensed matter physics. Moreover, attending this school can help me further develop a unique way of thinking in order to handle assignments in my future work. It also brings me in a very interesting environment of people with different ideas and experiences I can learn from.

Carlo Emerencia – Curriculum Vitae

1. Personal information

Place of birth: Etterbeek, Belgium

Date of birth: 14th of December 1994

Nationality: Dutch

Address: Terhulpensesteenweg 372, 3090 Overijse

Telephone Number: 0483 056 375

E-mail address: carlo.emerencia@gmail.com

Driver's License: not yet

Tutoring experience: Four years (Educadomo)

2. Education

Languages: Dutch (mother tongue), English (fluent)

School:

2007-2011: Koninklijk Instituut Woluwe, Economy

2011-2013: Sint Martinus Overijse, Math-Sciences

High School certificate: received

2013-2016: Vrije Universiteit Brussel (VUB), Bachelor Mathematics

Bachelor's degree Mathematics: obtained on the 1st of July 2016

2016-2018: Vrije Universiteit Brussel (VUB), Master Fundamental Mathematics

Master's degree Mathematics: obtained on the 5th of July 2018, with great distinction

From 2018 on: PhD student at VUB of Prof. dr. Ann Dooms

Prof. Dr. Ann Dooms
Vrije Universiteit Brussel (VUB)
Department of Mathematics
Digital Mathematics

Reference	**Date**
Recommendation letter Emerencia Carlo for the Applied Category Theory 2019 School	29-01-2019

Dear Organizers,

Thank you very much for organizing the Applied Category Theory 2019 School which I got to know through John Carlos Baez. The aim of the school is fantastic and fits perfectly within the research path my PhD student Carlo Emerencia is currently pursuing.

Carlo graduated in July 2018 as Master of Mathematics with specialty in Fundamental Mathematics (taking up courses like Category Theory). He did his Master Thesis under my guidance on the study of quantum algorithms that can break the security of current cryptosystems or candidates. He showed to be very independent and critical while delving into Shor's algorithm and extensions leading him to shortening arguments and alike. In October he started a PhD on post-quantum cryptography where our goal is to study the security of post-quantum candidates and the feasibility of quantum implementations, the latter in collaboration with our Applied Physics group working on quantum annealers based on condensed matter physics. Through discussions with my colleague De Commer (specialist operator algebras) we just started studying tensor networks in order to tie the links between theoretical quantum algorithms and their implementations.

We believe the school will enable Carlo to get better (and faster) insights in the possibilities of ZX-calculus and what it could mean to his research. We are also open to new research tracks in quantum circuits and ZX-calculus.

With kind regards,

Ann (actually former office neighbour of Bob Coecke at VUB)