Asst. Prof. Peter LeFanu Lumsdaine
Dept. of Mathematics
Stockholm University
SE-106 91, Stockholm, Sweden

p.l.lumsdaine@math.su.se

February 1, 2019

To whom it may concern,

I am very happy to write in support of Martin Lundfall's application to participate in the ACT 2019 school.

I supervised Martin's masters thesis on categorical semantics of linear dependent type theory in 2017–18 (which received an A). Before this, he had taken an introductory Category Theory with me (receiving an A), and took part in a mostly student-organised Homotopy Type Theory reading group under my supervision.

Through the masters project, Martin showed impressive potential as a researcher. He displayed not only a strong mathematical talent and a good general background in logic and category theory, but also independent and imaginative thinking and a mature perspective on the subject — the main project topic was his own proposal, and he obtained substantial novel results.

Since his masters work, he has been working largely on formal verification in the cryptocurrency setting. He therefore has a strong combination of experience and interest in the application of logical tools to computer science, both theoretically and in practice. I believe he would be excellently suited as an ACT participant: it would broaden his toolbox for such applications, either in industry or if he chooses to pursue a PhD in future.

Sincerely yours,

Peter LeFanu Lumsdaine

MARTIN LUNDFALL

January 28, 2019, Stockholm
martin.lundfall@protonmail.com

EDUCATION

Stockholm University *Dec 2017*
MSc in Mathematics
Particular focus on Logic, (Homotopy) Type Theory and Category Theory

SELECTED EXPERIENCE

Programming Language specification 2018 - present
K framework *DappHub*

- Developing formal, executable specifications of programming languages and virtual machines together with analysis and formal verification tools using the 𝕂 framework (`http://www.kframework.org`).
- Involved in the specification of: Ethereum Virtual Machine (EVM), Web Assembly (WASM), Rho-calculus
- Theoretical underpinnings in rewriting theory, type theory and matching logic.

Blockchain development 2015 - present
Development and verification of smart contracts *ConsenSys, MakerDAO, CirclesUBI*

- Designing smart contracts for Ethereum, combining game theory, cryptography and distributed computing to create systems for a (hopefully) more equitable, fair and inclusive economy.
- Research and development of for tooling for formal verification of smart contracts. Flagship project is a specification format and symbolic execution explorer: `https://github.com/dapphub/klab`
- Regular public speaking on these topics at various blockchain conferences.

Master Thesis 2017
A diagram model of linear dependent type theory *Stockholm University*

- Developed a type theory combining linear and dependent types and explored some categorical models of this theory under the supervision of Peter Lumsdaine.
- The model can be seen as an extension of the groupoid model of dependent type theory to the linear setting, taking a tentative first step towards "higher dimensional" models of linear, dependent type theory.
- Full article at `https://arxiv.org/pdf/1806.09593.pdf`

Bachelor Thesis 2015
Formalising Real numbers in Agda *Stockholm University*

- Following Bishop's work on constructive analsysis, I formalized real numbers as Cauchy sequences of rational numbers and their equivalence relation in Agda.
- Full article at `https://goo.gl/6i5neU`

TECHNICAL STRENGTHS

Computer Languages and tools	K framework, Agda, Javascipt, Haskell, Emacs, Solidity, Java
LaTeX, Git, SMT solvers	
Mathematics	Category theory, Type theory, Cryptography, Game theory
Human Languages	Swedish, English, German

Relevant category theory background:

- Introductory course in category theory taught by Peter Lumsdaine at Stockholm University, following Awodey's book. *The basics, Yoneda's lemma, monoidal categories, adjoints, monads*
- Categorical logic, a week long course taught by Henrik Forsell at The Third Nordic Logic Summer School, 2017. *Cartesian categories, Reulgar categories, coherent categories, topos*
- My master thesis exploring categorical models of linear dependent type theory; *Comprehension categories, Grothendieck fibrations, Kan extensions*
- Many guest lectures and seminars hosted by the logic faculty at Stockholm University have been focused on category theory. *Path categories, model categories, polynomial functors*

Outside these traditional academic contexts, I have had the privilege of being able to continue study category theory as part of my job as a formal methods researcher in the blockchain space.

- Perhaps of particular relevance to the course on Partial evaluations, I have studied Petri nets, (enriched) Lawvere theories and rewrite theory. This has been tangentially related to my work on formal verification, but is maybe most accurately framed as a desire to form a deeper understanding on what programming languages are, what "finitely representable" means in some general sense, and how to understand mathematical objects constructively.

At the moment I am not pursuing a PhD, but would like to apply mathematics to provide a more predictable, sustainable and fairer economy.

1 Motivation

> There was a passionate craving among all the intellectuals ... for a means to express their new concepts. They longed for philosophy, for synthesis. Some dreamed of a new alphabet, a new language of symbols through which they could formulate and exchange their new intellectual experiences.
>
> *Herman Hesse*
> *The Glass Bead Game*

I was reading the Glass Bead Game as I first started studying category theory in earnest. When Hesse speaks of a language through which "mathematics, philosophy, physics and music" could be expressed and unified in an exercise of pure aesthetics, what would be a better candidate than the language of categories?

My current work as a blockchain researcher is to design, develop and analyze systems in which people can coordinate around value. I do this because I think that an open infrastructure for the tools we use to organize our economy is a necessary condition to reach an inclusive, sustainable and fair society. At a surface level, it may not seem like the obvious domain for applied category theory. But in practice, there are many ways in which a category theoretic thinking comes in helpful; consensus protocol analysis, game theoretic analysis of smart contracts, and operational semantics of the programming languages used to build them.

Operational semantics in particular is a domain with a lot of room for improvement. The current methods for formal verification suffers from a significant gap between implementation heuristics and theoretic underpinnings; a divide that can result both in theoretical developments that are unusable or irrelevant in practice and possibly unsound proving systems. A long outstanding research goal of mine is to better understand the theory of programming languages, virtual machines and their behavior, develop languages and analsysis tools based on sound theoretical principals. I would like to draw from the relevant research in rewriting theory, lawvere theory and type theory to develop practical methods to specify and verify the behavior of programs, and tactics for proof search.

Finally, there is a significant lack of academic influence over the blockchain space as a whole. There are many novel problems in the space that are largely being tackled through rough engineering heuristics, often to great detriment. Participating in the ACT2019 school would not only be beneficial for me personally — but would also serve as a bridge that can connect the academic sphere to these problems.

2 Project preference

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