Theory at Cambridge

Anuj Dawar | Marcelo Fiore | Timothy Griffin | Mateja Jamnik

Neel Krishnaswami | Lawrence Paulson | Andrew Pitts | Thomas Sauerwald

Peter Sewell | Jamie Vicary *(that's me)*

Not taking PhD applications

Postgraduate Open Day
Department of Computer Science and Technology, University of Cambridge
3 November 2021

Logic and Algorithms *(led by Anuj Dawar)*

- Study *Complexity Theory* by means of *Logic.*
- Complexity-theoretic questions (such as $P \neq NP$) are about proving *lower bounds* on hard problems.
- Aim to classify complexity of computational problems by means of their *definability* in logic.
- Study definability of problems using methods from:
  - *combinatorics; algebra; topology; category theory.*
- Establish lower bounds for *abstract, symmetric* models of computation.

Marcelo Fiore

Type theory and foundations of computer science

https://www.cl.cam.ac.uk/~mpf23/
https://arxiv.org/abs/2101.02994
https://arxiv.org/abs/1904.06538

Mateja Jamnik

Human-explainable artificial intelligence, diagrammatic reasoning

https://www.cl.cam.ac.uk/~mj201/

Project suggestions:
Concept Learning for Human-Like Explanation in Machine Learning
Machine Learning Explainability in Integrative Cancer Medicine
What Have You Learnt? Knowledge Discovery Using Deep Neural Networks

Neel Krishnaswami: Types, Semantics, Verification

- Type Theory and Structural Proof Theory
  - Integrating Linear and Dependent Types
  - Bidirectional Type Inference
  - Types for Parser Combinators (!)
- Applications of Denotational Semantics
  - Functional Reactive Programming
  - Categorical Semantics of Incremental and Differentiable Programming
  - Comonadic Semantics of Capabilities
- Program Verification
  - Separation Logic for WebAssembly
  - Transfinite Step-Indexing
  - Ongoing verification of the pKVM hypervisor

Taking hammers from many toolboxes lets us smash many windows!

Lawrence Paulson

Automated theorem proving and applications

https://www.cl.cam.ac.uk/~lp15/

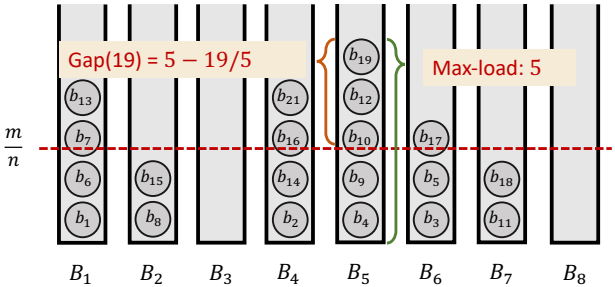
Balls and Bins under incomplete Information

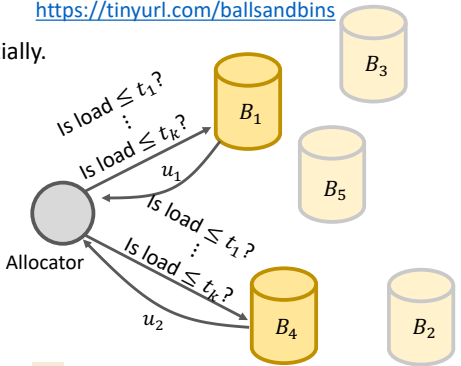
Dimitrios Los, Thomas Sauerwald, John Sylvester

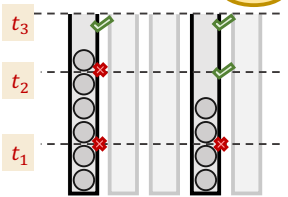
https://arxiv.org/abs/2110.10759
https://tinyurl.com/ballsandbins

Input: Given n servers (bins) and m jobs (balls) to allocate sequentially.

Goal: Minimise the load of the heaviest bin, i.e. $\max_{1 \le j \le n} x_j$.







Threshold model: For each ball, the allocator

1. Samples two bins randomly.
2. Sends queries of the form "Is load at most t_i?" to the bins.
3. Receives replies and allocates to "better" of the two bins.

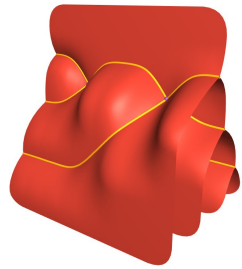
Peter Sewell – REMS, Sail, C, pKVM, CHERI

How can we develop mathematically rigorous semantics that accurately captures mainstream computing abstractions, that helps clarify what they are/should be, and that helps engineer them to be more robust and secure?

- relaxed-memory concurrency: what is/should be the concurrency semantics of Armv8-A, RISC-V, IBM Power, x86, C, C++ ? (with Arm, RISC-V, IBM, ISO WG21)
- Sail instruction semantics + Isla symbolic execution: how can we express and work with *complete* instruction-set architecture definitions? (with Arm, RISC-V, CHERI)
- Cerberus C semantics: how can we express the real semantics of C? What should the C memory object semantics be? (with ISO WG14)
- pKVM verification: how can we use the above to verify an in-progress production Google Android hypervisor? (with Krishnaswami, MPI-SWS, Radboud, Aarhus, SNU, Google)
- CHERI: adding *hardware capabilities* to Armv8-A, RISC-V, C, C++, etc., for fine-grained memory safety and secure compartmentalisation
  - Arm Morello prototype ISA, processor, board, and software, from £170m DSbD programme, with machine-proved ISA security properties (with Watson & S.Moore; Arm; Edinburgh)

Jamie Vicary

I use *category theory* to solve problems in the foundations of computer science and mathematics.



- How can we use *geometrical representations* to make higher category theory easier to work with and understand? arXiv:1902.03831, arXiv:1610.06908
- Proof assistant *homotopy.io* (Rust/WASM) allows construction and visualization of high-dimensional categorical composites `https://ncatlab.org/nlab/show/homotopy.io`
- How can we use type theory to *simplify* algebraic reasoning in higher category theory? arXiv:2007.08307, arXiv:2109.01513

$$(j \circ h) \circ (\mathrm{id} \circ g \circ f) \rightsquigarrow j \circ h \circ g \circ f$$

- What is the type-theoretic content of higher-dimensional directed paths, and how can we reason about them abstractly? (If $\mathcal{C}$, $\mathcal{D}$ are ∞-categories, why is $\mathrm{Hom}(\mathcal{C}, \mathcal{D})$ an ∞-category?)

- How can we use category theory to reason structurally about *quantum computation*?