The Maths and Computer Proof discussion day

The Maths and Computer Proof discussion day took place on 15th April in the Informatics Forum at the University of Edinburgh. A mix of just over twenty mathematicians and computer scientists attended, with three talks in the morning and two panel discussions in the afternoon. Discussion centred around what sort of thing CS has done or could do for maths, and how mathematicians view their subject. In particular, computers were seen as having two possible roles in mathematics: assistants for mathematicians, and mathematicians in their own right.

Schedule

The schedule for the day was as follows.

10am Arrival, coffee, and introductions.

10.30 Sir Michael Atiyah (Edinburgh), What is intelligence?

11-1 John Harrison (Intel) and Georges Gonthier (Microsoft Research) will present an overview of the field of machine construction of proofs, including the state of the art and its present and hoped for achievements.

1-2 Lunch and more coffee.

2-3.30 Panel discussion, What is the role of machines in the future of research mathematics? Opening statements followed by discussion.

3.30 More coffee (and cake).

4-5 Panel discussion, What are we going to do about it? Opening statements followed by discussion.

5-7 Take a break, go to pub, etc.

7pm Reception in honour of 25 years of the Edinburgh Laboratory for the Foundations of Computer Science.

Talks

Sir Michael Atiyah: What is intelligence?

Sir Michael Atiyah discussed mathematical intelligence, defining it to be the capacity to create new maths; that is, new concepts, ideas, structures, frameworks, and finally theorems. He elaborated on how people create maths - suggesting that the process of making mistakes and learning from them is a fundamental part of a mathematician's thinking. He also emphasised the role of understanding; that is, having an overall structured picture, a range of interconnected arguments which support each other, so that if one collapses the edifice does not fall. This multi-dimensional picture was contrasted against a sequence of logical steps, where if a single link is broken then the chain is lost. A proof should be simple, and explain *why* a theorem is true.

John Harrison: Formalizing mathematical proofs by computer

John Harrison gave an introductory overview of formalisation, going back to Russell and Whitehead's *Principia Mathematica* and formalising proof in general, and discussing exactly what difference computers make. He went on to describe what theorem proving technology is and what can be automated, discussing theorem provers versus computer algebra systems, early research in automated reasoning and interactive proof and prover architectures. Finally, he outlined the applications of formalisation, including in pure mathematics, in computer system verification and the Flyspeck project.

Georges Gonthier: Applications of formalisation

Georges Gonthier continued where John left off, on the applications of formalisation, describing the background and architecture of his work on automating the proof of the odd-order theorem. Both John and Georges' talks were mainly slanted at the non-experts in the audience, who were encouraged to interrupt and interject along the way.

Discussion

We viewed the goal of the event as being to consider two main questions:
- "What is the role of machines in the future of research mathematics?"
- "What are we going to do about it?"

Two themes emerged during the discussion, computers as helping human mathematicians and as being seen as mathematicians in their own right.

Computers as mathematical assistants

The potential of computers as assistants was uncontroversial, and the mood of the day was that there is an enormous future for using machines to help mathematicians. It was suggested that mathematicians are happy to use tools which are useful to them (there aren't any yet - but there will be). In particular, it is hoped that these can help to take some of the drudgery out of the subject. Such capabilities might include storing mathematical knowledge: this is already in effect and search tools enable mathematicians to easily find important results in a subject - the danger of re-proving results which were published in an obscure journal has now passed (Ramanujan doesn't exist anymore). Enabling computers to find connections between different areas of maths by trawling through a database of results would be useful: there is so much mathematics now that no one person can keep track of it. The value of computers as proof-checkers was agreed, and a future envisaged in which a mathematician could develop a bit of maths, prove a theorem and the hand it over to a system to verify. Along similar lines, the idea of using proof-checkers to act as reviewers by checking proofs in submitted papers was very much welcomed as a valuable contribution. Using computers to keep track of a big proof was also seen as useful. Computers could be used to break a big proof down into small stages and manage it. Even if projects are always be guided by human mathematicians, it might be possible to automatically keep track of a proof. Here, a formal repository of formal proofs of fundamental theorems that everyone had access to was suggested. It was hypothesised that such a repository with proper structured arguments and a clear path through them that everybody can see reasonably easily might change the (normally organic) evolution of maths quite significantly. The value of simplications and explanations may also help to speed up the evolution.

The role of computers in enabling mathematicians to work together was also discussed. This might be in the form of large collaborative projects such as Gowers' Polymath project, or on a smaller scale of helping to find people and make suggestions about new collaborations. For instance, if people are using the same library as each other, then a computer could make suggestions based on who is using a given theorem to prove a particular result. Similarly, it might be possible (although not necessarily legal!) to keep track of who has read the same maths reviews. Developing computers as teachers, at every level, was also encouraged, especially at the research level.

Computers as autonomous mathematicians

The idea that computers could, one day, be mathematicians in their own right, and whether this would be desirable, was far more controversial. Many participants argued that they could not, and pointed out capabilities which humans have, which, they argued, computers could never have. These capabilities served as both supporting arguments for those against the idea and as valuable insights and grand challenges for those who thought it might be possible. Atiyah's thoughts on how humans do maths were discussed throughout the day. It was suggested that people make two kinds of error - logical errors, such as asuming a statement to be a theorem

when it isn't, and conceptual errors of understanding, such as misinterpreting what a theorem actually says. Atiyah's notion of structural as opposed to linear thinking was reinforced by other mathematicians present, and arose frequently during discussion. It was pointed out that despite mistakes being found in proofs, the proofs still work - there isn't an area of maths which suddenly collapsed because an error was found in a proof. Part of this is probably due to the fact that most mathematical results have lots of proofs, so the system is self-correcting when it comes to important results.

Further aspects involved in the human activity of mathematical thinking included finding the right starting point in a proof. Proofs seem to emerge naturally from a particular starting point (for example, the odd-order theorem, the n-group theorem and some parts of the classification of finite simple groups) - which seem to escape us if we start at the wrong point. A computer which were able to find such a starting point would be a great advance. Similarly, humans are able to make conceptual leaps between different frameworks: sophisticated problems arise when one is working in the wrong framework, and one should be able to think laterally, see when a particular framework is not the right one for a problem and switch to an appropriate framework. The ability to change focus partway through a proof was also highlighted, when a human realises that they're not going to be able to solve the problem the set out to do but can solve something useful nevertheless.

Next steps

The next steps can be divided into goals which are achievable in the forseeable future, and grand challenges; with the former mostly comprising the development of mathematical assistants, and the latter mostly the development of autonomous mathematicians.

Achievable goals included:

- introducing these ideas into mathematical culture, for example running a seminar on computational methods to maths postgraduates;
- developing tools which are able to perform some of the routine work in maths, such as checking proofs and refereeing papers;
- developing techniques and tools which enhance communication between mathematicians. Eg, the Polymath project simply uses blogging technology, this could be improved in various ways;
- performing datamining to find patterns in proofs and connections between different areas of mathematical thought, and
- enabling computers to provide useful visualisations of mathematical data

The grand challenges included:

- building computers which can change what they're working on partway through, to pursue an avenue which looks more promising to them;
- formalising other subjects, for example physics, which in some sense comes "before" maths;
- understanding the limits of computer maths, perhaps by analogy to the development of computers' game-playing abilities;
- building a computer which can adapt to individual mathematicians, and (of course)
- building a computer which can pass a mathematical Turing Test (or win a mathematical prize).

The day was a great success and people got a lot out of seeing and suggesting alternative viewpoints to those usually upheld by disciplinary boundaries. It seems a fair summary to say that mathematicians came away having seen a different perspective on their subjuect - perhaps not totally convinced yet of its value to them as mathematicians, but with the conviction that there is something there of interest. On the other hand, the computer scientists gained a lot from hearing insights about the sort of reasoning which is involved in mathematical thinking and what may be useful to mathematicians. Food for thought for both disciplines. We hope to organise a follow-up event in the near future to consolidate some of the new relationships formed.

Speakers and participants

Lead speakers included Georges Gonthier, who has produced a formal proof of the four colour theorem, and is well advanced on a formal proof of the odd-order theorem; John Harrison of Intel, who works on formalising mathematics needed to ensure correctness of hardware; and Fields medallist Sir Michael Atiyah.

Other participants included:

Participant	**Affiliation**
Alison Pease	QMUL
Andrew Ranicki	University of Edinburgh
Antony Maciocia	University of Edinburgh
Daniel Raggi	University of Edinburgh
Edmund Robinson	QMUL
Ekaterina Komendantskaya	University of Dundee
Elham Kashefi	University of Edinburgh
Emil Vaughan	QMUL
Geoff Robinson	University of Aberdeen
Georges Gonthier	Microsoft
Jacques Fleuriot	University of Edinburgh
James McKinna	Radboud University
John Harrison	Intel
Laura Meikle	University of Edinburgh
Marco Thiel	University of Aberdeen
Mark Adams	University of Edinburgh
Michael Atiyah	University of Edinburgh
Paul Jackson	University of Edinburgh
Rob Arthan	QMUL
Roy McCasland	University of Edinburgh
Soren Riis	QMUL
Steven Obua	University of Edinburgh
Ursula Martin	QMUL
Vincent Danos	University of Edinburgh