The potential of automated reasoning tools to assist the working mathematician

Visiting Researcher: Case for Support

Bogdan Grechuk, Alan Bundy, David Aspinall, Lucas Dixon

1. Abstract

Most of the recently proved important mathematical theorems have proofs of several hundreds of pages and cannot be reliably verified by referees. In this context, developing a user-friendly, formal, proof assistant, where everyone can check a proof of his result, becomes vital for the future of mathematics. There exist several proof assistants, such as Isabelle, HOL, Coq, etc., but they are currently unattractive for working mathematicians [1,2,3]. As a result, libraries of formalized mathematical results are not sufficiently rich to formalize most serious mathematical results, and, more importantly, developers of these proof assistants do not have sufficient feedback from mathematicians.

In this project, we aim to formalize the theory of convex analysis and optimization in Isabelle, which is one of the areas of expertise of the VR. This will significantly improve Isabelle's library, since convex optimization techniques are currently one of the central techniques for addressing optimization problems in mathematics and applications, and will form the basis for further important mathematical formalisations. More importantly, we aim to provide detailed feedback to Isabelle and Proof General developers, describing what should be improved in the system to make it more attractive to mathematicians. Building on this critique, we will revise the documentation of Isabelle, and its Proof General interface, to produce versions targeted at working mathematicians.

2. Previous Research Track Records

Institution

The Edinburgh School of Informatics obtained the highest volume of 4* activity in its unit of assessment in RAE 2008. It contains world-class research groups in the areas of theoretical computer science, artificial intelligence and cognitive science.

The Mathematical Reasoning Group in the School of Informatics has been engaged on the computational analysis, development and application of mathematical reasoning processes and their interactions since the mid 1970s (http://dream.inf.ed.ac.uk/). Its work is characterised by its unique blend of computational theory with artificial intelligence. It has pioneered work on proof planning, tactic learning, and ontology construction and evolution.

Investigators

Prof. Alan Bundy has been active in automated mathematical reasoning research since 1971 and has become a world authority. His international reputation is witnessed by his being made a founding fellow of both of the two international AI societies: AAAI and ECCAI, in addition to the UK society, AISB, and serving terms as Chair of both IJCAI Inc and CADE Inc. He is also a Fellow of the Royal Society of Edinburgh, the British Computer Society and the Institution of Engineering and Technology. He won the SPL Insight Award in 1986, was an SERC Senior Fellow (1987-92), a member of the Hewlett-Packard Research Board (1989-91), Head of the Division of Informatics at Edinburgh (1998-2001), a member of the ITEC Foresight Panel (1994-96), a member of both the 2001 and 2008 Computer Science RAE panels (1999-2001) and (2005-2008), and was the founding Convener of UKCRC (2000-2005). He is currently a member of the Scottish Scientific Advisory Committee, which advises the Scottish Government on scientific matters. He is the author of over 200 publications and has held over 50 research grants.

Dr. David Aspinall is a Senior Lecturer in the School of Informatics at the University of Edinburgh where he also received his PhD in 1997. During and since his PhD, David Aspinall has worked on interactive reasoning systems. He developed Proof General which is the official interface for the Isabelle theorem prover, and the de

facto one for several other systems. It is in widespread worldwide use, and is being taken forward as vehicle for further research into the maintenance and development of large proofs. Aspinall has co-organised two international workshops on User Interfaces for Theorem Provers and edited a special edition of J. Automated Reasoning on the topic. He is co-Investigator on several related projects, including the European Co-ordination Action “Types for Proofs and Programs” and the European Integrated Project “Mobius” which is applying Proof-Carrying Code to mobile devices.

Dr. Lucas Dixon completed a PhD with the Mathematical Reasoning Group at the University of Edinburgh in 2006 where he is now a research associate. For his PhD work, he developed the IsaPlanner system, which is now the central platform for proof planning research in the Edinburgh Mathematical Reasoning Group. In this work, he has provided a generic and fully formal foundation for proof planning as well as an efficient inductive prover for Isabelle. He was the programme chair for both the 2007 Isabelle Workshop and Calculemus 2009. He has taught Isabelle at various workshops. He has also published research in user interfaces for theorem provers, proof planning, middle-out reasoning, program synthesis, linear logic and reasoning tools for quantum information.

Visiting Researcher

Dr. Bogdan Grechuk was awarded a Ph.D. in mathematics at Stevens Institute of Technology, USA, in May 2009. Before this, he was awarded another Ph.D. at Moscow Institute of Physics and Technology, Russia, June 2006. In 1997 and 1998, he won a Gold Medal and a Silver Medal at the International Mathematical Olympiad. In June 2009, Dr. Grechuk visited the Mathematical Reasoning Group at the University of Edinburgh. During this visit he formalized part of the theory of convex analysis in Isabelle.

The research interests of Dr. Grechuk are in the following areas:

1) convex analysis and optimization, deviation measures, risk management
2) discrete mathematics and algorithms.

His mathematical intuition and experience in developing mathematical proofs will be helpful in making machine-based proofs closer to human-made proofs.

The VR defended his Ph.D. thesis “Deviation Measures: Theory and Application” at the Stevens Institute of Technology, USA, in May 2009. Mathematically, the topic of the thesis is closely connected with the area of convex optimization. Part of the content of this Ph.D. work was published [5,6] in the leading American mathematical journals, such as “Mathematics of Operation Research”. With such experience in the area, the VR will be able to formalize convex optimization theory with the highest level of expertise.

In June 2009, the VR joined the Mathematical Reasoning Group for a one-month academic visit, during which he formalized several important theorems from convex analysis in Isabelle. These results will be added to the Isabelle library. Also, he provided feedback to the Isabelle developers, suggesting what should be improved in the program. Some of the comments and suggestions were found very interesting, and will be considered for implementation (Tobias Nipkow, personal communication).

In June 2006, the VR defended another Ph.D. “Algorithms for scheduling and optimal restarts in real-time systems” in Moscow Institute of Physics and Technology, Moscow, Russia. The thesis is devoted to development of efficient algorithms for several optimization problems arising from the scheduling theory. Also, in 2002-2004 he was a Java-Programmer at NetCracker Technology. This significant experience in algorithm theory and practical programming will help the VR both to work with Isabelle and, more importantly, to suggest reasonable, achievable improvements to the system.

In summary, this project beings a visiting researcher who is a talented mathematical researcher, who is enthusiastic about the potential application of automated reasoning tools to mathematical research, but can look with fresh eyes at the difficulties that a mathematician might face when first confronted by such tools, i.e., who is not already part of the automated reasoning community. Such criteria are extremely hard to meet. We are very lucky to have identified someone who meets them so perfectly, complementing the expertise of the investigators and, indeed, that of most of the researchers in automated reasoning. During his visit in June 2009 the VR built an excellent rapport with the members of the Mathematical Reasoning Group and we are very keen to continue to build on this extremely promising start. As Prof. Nipkow argues in his supporting letter, the VR made a flying start during his June visit, making real contribution in a very short period.

3. Description of the proposed visit and its context

Scientific/Technological Relevance

The proposed work focuses on the formalization of the theory of convex analysis and optimization in Isabelle. Mathematically, this will significantly enlarge Isabelle's library and provide the necessary lemmas for further formalization in the many areas of mathematics that involve optimization. Convex minimization has a broad range of applications, e.g. in statistics, data analysis and modelling, signal processing, automatic control systems and finance. In particular, the VR in his Ph.D. thesis applied convex optimization techniques to risk analysis and portfolio optimization. Also, as noted by one of the Isabelle developers (Amine Chaieb, personal communication), the formalization of convex optimization "...is of particular interest for us, since with enough infrastructure, some new proof-methods could be easily derived. For instance, using (generalized) geometric programming to prove Isabelle/HOL formulas involving division and nth-roots."

Also, in this project, we will provide detailed feedback for Isabelle and Proof General developers. This will include:

1) **Revised documentation for Isabelle and Proof General.** Currently, it takes several weeks to become more or less comfortable with Isabelle starting from scratch, which is the first important reason why the program is not attractive for most mathematicians. We will write revised versions of the documentation, focusing on those parts of the tutorial that are most important for mathematicians and should be extended or clarified, and shortening or removing those parts that are less attractive.

2) **Critique of Isabelle and Proof General and recommendations for improvements.** What should be improved in these systems to make the process of theorem proving more convenient and intuitive for a mathematician. We provide feedback on which tactics do not do their job well and should be improved, comments about relevant lemma suggestion, and other desirable improvements.

3) **Critique and recommendations about proof readability and understandability.** Ideally, theorem provers, such as Isabelle, and their interfaces, such as Proof General, should provide a language and interface such that the resulting proof can be easily understood by a mathematician.

Clearly, Isabelle and Proof General developers understand all these problems and are working in these directions. However, lack of feedback from mathematicians is a serious problem. They may work hard to improve one aspect of the system, but it would remain unattractive for working mathematicians for completely different reasons.

In conclusion, this project will significantly improve Isabelle's library by introducing convex optimization techniques into it, and will provide the Isabelle and Proof General developers with important feedback from a mathematician.

Academic Beneficiaries

The most immediate beneficiaries of this project will be the developers and users of the Isabelle proof assistant and its Proof General interface. They will be provided with an addition to the current Isabelle Library in an increasingly important area of mathematics. Such formalised mathematics not only provides a platform for mathematical research, but often proves a useful basis for software verification, for instance, the use of Grobner Basis by Harrison at Intel. They will also receive feedback on ways in which Isabelle and Proof General can be improved to make them more useful for mathematical research, including revised versions of the documentation aimed at mathematicians. Currently, most users are computer scientists interested in formal methods, and library developments and feedback has been focussed on this application. This project will help open up the important, but relatively neglected application area of mathematical research, bringing to bear the mathematical experience and authority of a mathematical olympiad gold-medallist.

In the longer term, we hope that professional mathematicians will benefit from access to a proof development and checking environment that will significantly increase the reliability of mathematical theorems and improve the quality of the refereeing process. We believe that this development is essential and inevitably due to the increasing size and complexity of modern mathematical proofs. The UK is world leading in automated theorem proving. The access to a world-class mathematician, keen to play a key role in this development, will accelerate the impact of UK research in this area.

Impact Summary

- **Who will benefit from this research?** The beneficiaries will be users of interactive proof systems, especially Isabelle and Proof General, as discussed in the Academic Beneficiaries section.
- **How will they benefit from this research?** These tools will be improved to make them better suited to support mathematical research. In particular, there will be a new library, more targeted documentation and feedback and recommendations for further improvements.
- **What will be done to ensure that they have the opportunity to benefit from this research?** The deliverables listed in the previous bullet will be developed in close consultation with both the Isabelle and Proof General developers and user communities in order to maximise their impact. Soundings will also be taken amongst a small, local community of mathematicians interested in the use of automated proof tools within mathematics. Consultation will be by both face to face and electronic communication. There will be visits to the key labs: Cambridge, Munich and Birmingham, plus a presentation at a relevant conference or workshop and a journal paper. We hope that the library and revised documentation will be circulated with the standard Isabelle release.

The Programme

The theory of convex analysis is almost absent in Isabelle's Library and will be developed almost from scratch. Only definitions of convex sets and convex functions with some very basic properties were present in the Library before June 2009, more theorems about convex functions were formalized in June 2009 by the VR . In the first month of his visit, the VR will come to an agreement with members of the Isabelle team about all the basic definitions of the theory, and a particular list of results for formalization. These results will include practically all important theorems from a standard textbook (see eg. [4]) about convex analysis and optimization plus, possibly, some special results that Isabelle developers will be interested in in order to derive new proof-methods. Also, during this first month, the VR will learn more about Isabelle, to be able to develop the simplest possible proofs which will use the full strength of Isabelle. Comprehensive feedback about Isabelle's and Proof General's help systems will be provided, and revised documentation will be developed. The rest of the visit will be devoted to the formalization itself, which will be done in close coordination with the Isabelle developers.

During the project, the VR plans to have a one-week visit to Munich to discuss his work in Isabelle with system developers directly, and also two one-week visits to leading research teams in the area in the UK: the University of Cambridge Computer Laboratory (Prof. Michael Gordon, Prof. Lawrence Paulson) and the School of Computer Science in the University of Birmingham (Dr. Manfred Kerber, Dr. Volker Sorge).

In the last month of the visit, the VR will prepare a paper about the results achieved, and this paper will be submitted for publication in a major automated theorem proving journal. There will also be an interim report at a conference or workshop during FloC 2010 in July.

References

[1] Harrison, J., *Formal Proof – Theory and Practice.* Notices of the American Mathematical Society, vol. 55, pp. 1395-1406, 2008.

[2] Bundy, A., *A Very Mathematical Dilemma.* The Computer Journal, vol. 49, no 4, pp 480-486, 2006.

[3] *The nature of mathematical proof.* Phil Trans of the Royal Society A. Eds Bundy, A., Atiyah, M., Macintyre, A. and MacKenzie, D., Vol. 363, No. 1835, pp 2329-2461, 2005.

[4] Bertsekas, D., Nedic, A., Asuman E., *Convex Analysis and Optimization.* Ozdaglar, 2003, ISBN 1-886529-45-0, 560 pages.

[5] Grechuk, B., Molyboha, A., Zabarankin, M., *Chebyshev Inequalities with Law Invariant Deviation Measures,* Probability in the Engineering and Informational Sciences, accepted.

[6] Grechuk, B., Molyboha, A., Zabarankin, M., *Maximum Entropy Principle with General Deviation Measures,* Mathematics of Operations Research, Vol. 34, No. 2, May 2009, pp. 445-467.