Title: Formalised Mathematics and its Applications in Computing

Speaker: Georg Struth, University of Sheffield, UK

Abstract: The idea of programming mathematical structures and verifying mathematical proofs on a computer has captivated computer scientists and mathematicians for almost a century. Tools ranging from expressive proof assistants based on higher-order logics and set theories to automated proof-search engines, counterexample generators, domain specific solvers or decision procedures have emerged over the last few decades. With increasing infrastructure for designing and using mathematical hierarchies and with increasingly powerful proof automation, these tools have recently become popular with computer scientists, predominantly for hardware and software verification. But what can they offer to mathematicians?

This talk reflects on my own experience in formalising algebraic structures and their models with the Isabelle/HOL proof assistant. I will present a series of basic examples from the context of semirings, formal languages and relational structures to illustrate the different styles of formalising, verifying and falsifying mathematical statements which are supported by Isabelle. I will show how one such semiring plays a central role in a tool for verifying simple while programs, which is itself correct by construction in Isabelle. I will summarise these examples by pointing out the potential and limitations of state-of-the-art proof assistants for various mathematical tasks and outline some desirable features which would increase their value in mathematical practice.