University of Western Sydney
Bringing knowledge to life

CENTRE FOR RESEARCH IN MATHEMATICS

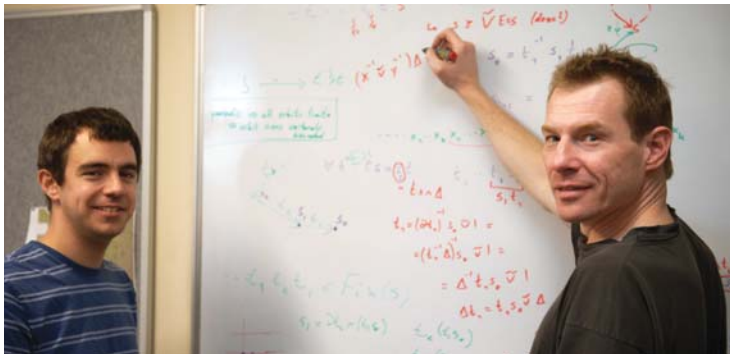
BRAID AND GARSIDE THEORY

Dr Volker Gebhardt and Dr Stephen Tawn from the Centre for Research in Mathematics at the School of Computing, Engineering and Mathematics, together with their international collaborators, explore the properties of braids and related mathematical objects called *Garside monoids*.

This programme is basic research in algebra, an area of pure mathematics, with the primary objective of gaining a better understanding of the structure of these abstract objects. Braids and Garside monoids have many applications in other areas of mathematics, in theoretical physics, but also in data security.

"Everyone can imagine a braid: Take three or more strands that are initially parallel; you get a braid by repeatedly intertwining adjacent strands", says Dr Gebhardt. "Braids are first of all geometric objects, but algebraists have found a way to describe them combinatorially and algebraically, and it is this algebraic description that has yielded many insights into their properties. The algebraic description also lends itself to a natural generalisation, namely so-called *Garside monoids*." There are still many open questions about the structural properties of these objects, and the research programme at the Centre for Research in Mathematics aims at resolving some of those.

Braids and their generalisations have applications in many areas of mathematics and theoretical physics, but have also received considerable interest for the purposes of data security. "Many modern schemes used to protect data or to authenticate users are based on number theory, another area of pure mathematics", says Dr Gebhardt. "Braids are an interesting alternative, since they are *non-commutative* (that is, the equality a·b=b·a does in general not hold for braids) and hence in some sense have a more complicated



structure than the objects used in traditional cryptographic schemes. This could make cryptographic schemes based on braids harder to break, and one can thus hope to achieve a given level of security with systems that are cheaper to build and faster than current systems."

The research team has expertise in pure mathematics (group theory and combinatorics), computational algebra, and software development. "The lack of good intuition is a huge limitation for this field, one that we want to address using our strengths", says Dr Gebhardt. Traditional theoretical mathematical investigations will be coupled with systematic and large scale computer experiments to both develop and test conjectures.

People at the Centre for Research in Mathematics:

- Dr Volker Gebhardt
- Dr Stephen Tawn

External Collaborators:

- Professor Patrick Dehornoy, University of Caen
- Professor Eddy Godelle, University of Caen
- Professor Juan González-Meneses, University of Seville

Recent Research Grants:

- Australian Research Council, Discovery Project grant 2010–2012, $150,000
- Spanish Ministry of Science and Innovation, Plan Nacional 2010–2013, €37,000.