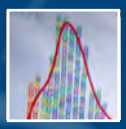
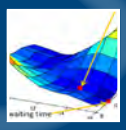
IMAGES NZ
ISSUE FOURTEEN

INSIDE


3 Online visual stats course wins praise


4 Optimising hospitals and the cloud

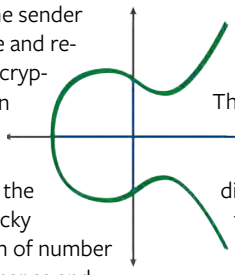

6 *In silico* experiments on human bodies


8 Models of breathing in birds and people

The speed of elliptic curves

If you shop online, get cash from an ATM, use an iPhone or an anti-virus programme, then your security relies partly on the cryptography skills of people like Steven Galbraith.

Unlike traditional cryptography, where the sender and receiver use the same key to create and receive coded messages, users of public key cryptography (PKC) need no secret information to keep our online banking secure. PKC is based on hard computational problems, and Steven, a professor of mathematics at the University of Auckland, has staked out a tricky corner. Elliptic curves lie at the intersection of number theory, algebra and algebraic geometry; "shapes and formulae – they have geometric and algebraic aspects at the same time", he says. The field is 150 years old, but became "very popular 30 years ago for digital security".



Steven says that the big questions are "which problems are hard for computers to solve and why?" and "what are the core principles that make it hard?" The standard technique is to try to simplify these hard computational problems. "We use abstract models or formalisms that strip away a lot of the detail to home in on the most fundamental aspects of a problem. Simplifying can show you how something can be done more efficiently."

Mathematicians in PKC constantly try to make cryptosystems work faster because, as he says, "you don't want to take over a minute to log into the bank". Security systems have to work quickly on small devices like smart cards as well as on web servers handling thousands of transactions at once.

Steven has worked with other mathematicians to "combine special features of elliptic curve mathematics applied in a particular way" to set a speed record for elliptic curve cryptography. Speed records are tested by the ECRYPT benchmarking site, which runs submitted code on multiple computers and posts the statistics online. The 'GLS method' has since become a standard tool in elliptic curve crypto. Another collaboration improved the speed of the discrete logarithm problem, a key problem in the field.

In another original contribution, with Mark Holmes at the University of Auckland, he generalised the birthday paradox from probability theory to analyse a key algorithm: "If you have 23 or more people in a room there's a better than even chance that two people will be born on the same day of the year. It was good to learn more about probability theory, and Mark is an expert. I couldn't do it by myself, and he didn't know anything about the computational application, so together we worked out the solution."

Steven runs a specialist blog, *Ellipticnews*, which was an attempt "to make our discussion of new ideas more open, more helpful for other researchers," he says. It is a leading site for announcing new results in elliptic curve cryptography before they are published by an academic journal. He often comments on draft papers; "if there's a controversy, it'll go from 40 hits a day to about 200."

Steven could have worked for security firms, but he chose to teach young people and do research. "I like my area because it connects with number theory, algorithms which leads to probability theory, combinatorics. I need to know a lot of different mathematics and I'm always learning new maths."

In his spare time, Steven (above right) has played bass guitar for five years in Five Wheel Drive, a punkish rock covers band which does about six gigs a year for parties, corporate events and weddings. "It's a hobby for all of us; we've been playing for decades and do it for fun. We do a punk version of 'Dominion Rd', and cover songs by bands like the Foo Fighters, Green Day, Buzzcocks, Shihad, Supergroove, Queens of the Stone Age and Royal Blood."

Welcome

We hope you enjoy reading these articles highlighting a range of contributions by New Zealand mathematicians. We are grateful to the sponsors of this issue. Sadly, however, unless this publication gains some long-term sponsorship, this issue may be the final one. See page 3 for more details.

Co-Editors:
Marston Conder and James Sneyd

See also
Steven's blog: https://ellipticnews.wordpress.com/
Cryptography benchmarking: http://bench.cr.yp.to/

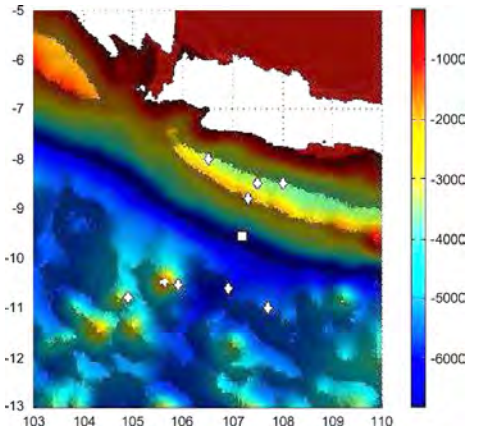
Tsunamis and other waves

Dimitrios Mitsotakis, of the Victoria University of Wellington, works with other mathematicians to improve tsunami early warning systems.

Some of those he works with are part of the Pacific Tsunami Warning Center (PTWC), operated by the US National Oceanic and Atmospheric Administration (NOAA, pronounced Noah). Seismic waves from earthquakes can be detected almost at once, as they travel at around 4km per second; this is much faster than tsunamis, which move in open water at the speed of a jet - about 0.2km/s.

However, tsunamis generated by local earthquakes will still arrive at the New Zealand coast before a warning can be given. New Zealand relies on the PTWC for warnings of distant earthquakes, and mathematicians strive constantly to make the models in these systems simpler, faster and more accurate. "When you need results in a couple of minutes, you have to use a very simplified model, which may not be very accurate" says Dimitrios; "more advanced models may take several days to analyse results."

Below: Sea depth around the island of Java (white) showing the epicentre of the 2006 earthquake (□) and wave gauges (✧). All distances are in degrees.



"The NOAA team gets alerted when earthquakes are detected, and run a computational model to check whether a tsunami is likely and in which direction," he says. "The results are matched with satellite data from ocean buoys and an early warning is issued if they match – red for evacuation, orange to keep people from the coastline, and yellow for a tidal increase but no danger."

Dimitrios is working with mathematicians from NZ, USA, France, Greece and Spain, with a grant by the Marsden Fund, to extend their tsunami model, which calculates a wave's spread through the water, its speed and how it is affected by the movement or collapse of the ocean floor from the earthquake. Mathematicians working in early warning systems are considering including the model for the first five minutes in the life of tsunamis.

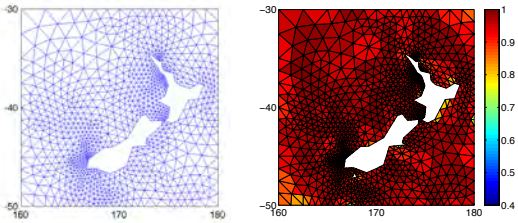
The model uses numerical methods to solve nonlinear partial differential equations. It is useful for tsunamis generated by local earthquakes and "is quite new with many open problems – its accuracy, solving it numerically, its conditions and boundaries". If simulations to test the model will take more than a fortnight to run, even on desktop computers with several cores, Dimitrios uses the Bluefern supercomputer at the University of Canterbury.

He is also using similar mathematical methods to model internal waves between water layers of different temperatures or merging tides. "You can sometimes see internal waves from a boat, the shore or in satellite images – they look like very large grey shadows of straight lines. We've known about them for a long time, but their maths and physics are very complicated."

His team has "some theoretical and computational developments of a new model for internal solitary waves" which will be useful for submarines. "If a sub interacts with an internal solitary wave, it may expend a lot of energy but remain unmoving for hours. One day we hope to design ways that subs won't be affected. When the surface of an internal wave becomes very steep it becomes very complicated mathematically - we can describe it but it's difficult to approximate with a computer code. When a steep internal wave breaks it generates high frequency oscillations."

The same mathematical techniques also apply to superfluids like liquid helium, where matter behaves like a fluid with no viscosity and can seem to defy gravity and surface tension. Superfluids are found in suns and neutron stars, in high-energy physics and theories of quantum gravity.

"The physics of this are new to me," says Dimitrios. "We want to develop numerical methods that will solve these complicated mathematical models. I like applying maths to real-world problems; I like the combination of computers, maths and physics."



Dimitrios uses triangles to discretise the ocean, and calculates the solution to the equations on the vertices of each triangle. Red indicates good quality triangles, greater than 0.6.

See also

Poseidon, a free collection of Fortran subroutines for solving partial differential equations using finite element methods: https://sites.google.com/site/dmitsot/poseidon

ISSN: 1177-4819
Co-editors
Marston Conder
and James Sneyd

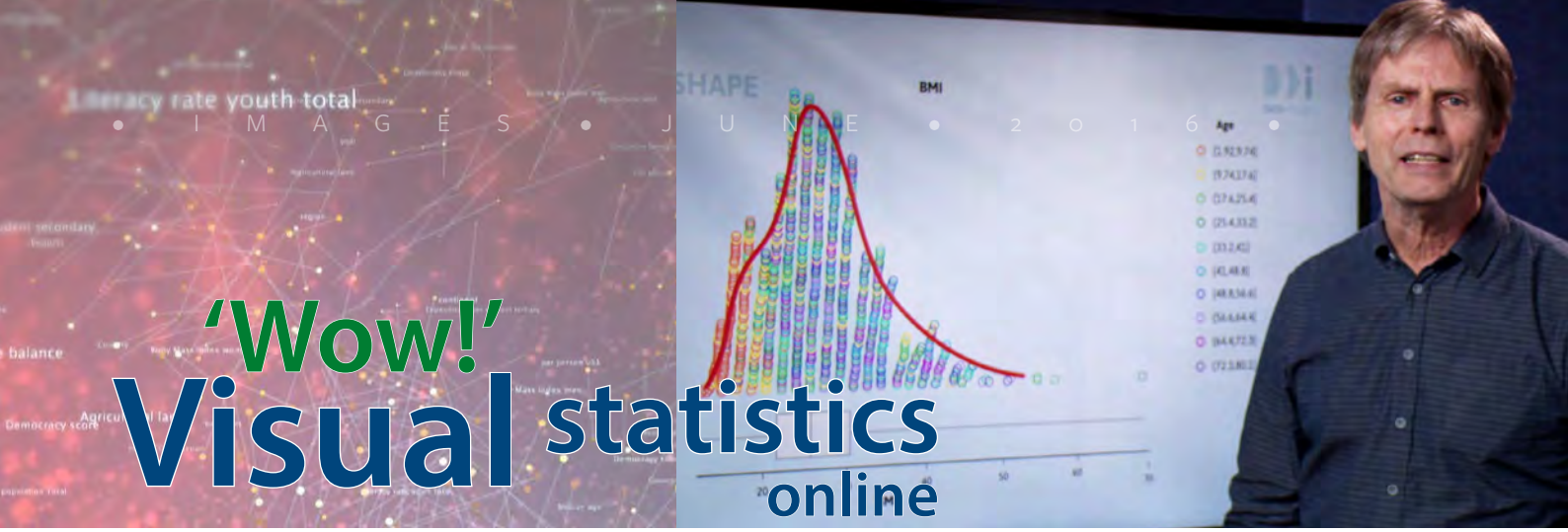
Writing and design:
Jenny Rankine,
Words and Pictures

University of Auckland,
Private Bag 92019, Auckland

P +64 (0)9 923 8879
or 923 7474

W www.mathsreach.org

E m.conder@auckland.ac.nz;
j.sneyd@auckland.ac.nz



'Wow!' Visual statistics online

Organising a free online statistics course for people unfamiliar with the subject changed Professor Chris Wild's ideas about teaching statistics at university and in schools.

The massive open online course (MOOC) – *Data to insight: An introduction to data analysis* – was one of the first MOOCs produced by the University of Auckland and has been so successful that it will run for the third time in October. It was produced with university audio-visual staff, learning designers from the university's Centre for Learning and Research in Higher Education, and Tom Elliot, lead iNZight programmer.

"The world of data is moving very fast and standard approaches to teaching introductory statistics are moving far too slowly," says Chris. "The MOOC was an attempt to expand the vision of introductory stats."

The course provides the free Department of Statistics data visualisation software iNZight, so that newcomers to statistics can quickly begin working with data; it aims to get participants thinking like statisticians after eight weeks.

Data to insight attracted 20,000 people in 2014 and 16,000 people last year. Like all MOOCs, the proportion who were able to devote three hours a week and finish the course was around ten percent, but the feedback was very positive.

One person started their comments on the last page with: "Wow! Wow! Wow!" and another said "You've given me the best 3 weeks of my life." Chris says: "I've never had students talk about 'falling in love' with statistics before". They were enthusiastic about the "beautiful visualisations". The iNZight software enables beginners to understand complex data stories, to "spot messages in statistical graphics".

Most of the teaching videos, featuring Chris and then staff member Tracey Week, are between five and eight minutes long. "We were aiming to present easily digestible chunks of ideas, and then get people to do something with them immediately. I was very sceptical about it at the start, but by the end I thought this was the way the world should be."

He wants to apply that principle to undergraduate classroom teaching, introducing more exercises, interaction and thinking, "rather than just receiving content. Our first-year team is moving towards group discussions in lecture theatres."

"Some of these ideas could help PhD students. I'm also much more a fan of online elements in teaching than when I started."

Secondary school maths teachers were one of the key audiences for the MOOC and "they're very receptive - even the ones who described themselves as dyed-in-the-wool calculus people. The visualisations are so different from the world that they had learnt in."

Other participants have included linguists, economists, data managers, marketers, scientists, journalists and PhD researchers from other areas, many of whom "start using ideas straight away in their work", says Chris. Many engage "at a deeper level than many of his university students". Participants are concentrated in New Zealand, the UK and the USA but enrol from all over the world. The self-paced course includes the limitations of data and how to avoid being misled by numbers.

Chris will make minor improvements to the course this year, to better link the first and second segments and redo some graphics with the updated iNZight.

MOOCs don't make money for the university, says Chris, as staff need to provide feedback on exercises and quizzes, manage the blogs and comments, and monitor any problems with the software. But the benefits outweigh the costs.

The iNZight software is written with the free, open-source software R, which was developed by staff members at the University of Auckland (see *IMAges* 3, 2007). iNZight's development began in 2010; "it continues to improve and grow as I find good students to work on it. I would love to build an iNZight user community - they'd need to be good R programmers."

See the *Data to insight* webpage:
https://www.futurelearn.com/courses/data-to-insight

Above: Chris Wild discusses a graph of Body Mass Index for 2,000 US people.

> This is the first online course I have done, and the only statistics course I have ever done, that actually left me feeling empowered, emboldened, and prompted me to have many 'lightbulb moments'.
> *NZ scientist*
>
> I used to consider the subject a bit monotonous, but not anymore! There's a lot of magic here.
>
> I find it amazing how visualization of data in these graphs helps so much in under-standing it.

Sponsorship

We are grateful to the University of Auckland (Engineering Science, Mathematics and Statistics), Massey University (IMS Albany), Victoria University of Wellington and the University of Canterbury for sponsorship of this issue.

Sadly, however, we cannot continue to produce *IMAges* without substantial long-term sponsorship. If you know of any likely sources of suitable funding to keep it going, please let one of us know.

Marston Conder (m.conder@auckland.ac.nz) and **James Sneyd** (j.sneyd@auckland.ac.nz)