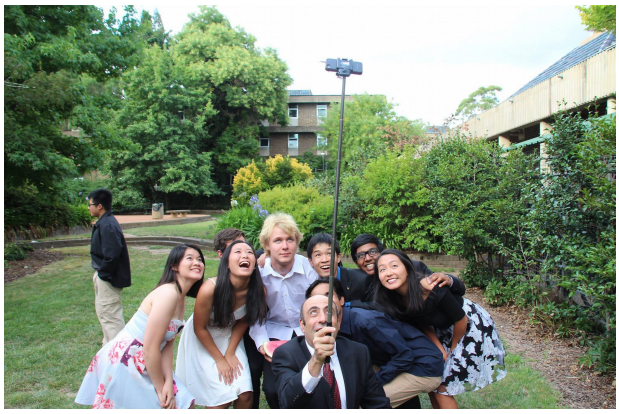
NeMeSiS News 2016

Newsletter of the

ANU-AAMT National Mathematics Summer School



Yumalundi!

Welcome to the 18th edition of NeMeSiS News! We hope that you enjoy reading it. Please let me know what you think.

This will be my last issue as editor. Kaela Armitage will be taking over as editor. Thank you for all of your submissions and feedback over the last 18 years. Putting the newsletter together each year has been an absolute pleasure.

Merryn Horrocks (editor)

In way of brief introduction, I had the pleasure and privilege of being a NMSS student in 2012 and an EG in 2013, and have returned as a tutor for the last two years. Currently I am finishing my final year of a Bachelor of Pharmacy and concurrent Honours in calcium signalling in breast cancer at the University of Queensland. While that may seem a little unrelated, NMSS has been an incredible part of my life; I have a great love and passion for mathematics and the pedagogy of the summer school, the pursuit of curiosity and the wonderful people that NMSS brings together. It has been a highlight to receive the wonderful newsletter Merryn has put together each year, and I'm excited to be a part of many editions to come!

We are always looking for contributions for NeMeSiS News, so please email me with any feedback, ideas or submissions that you may have. I would love to hear from you!

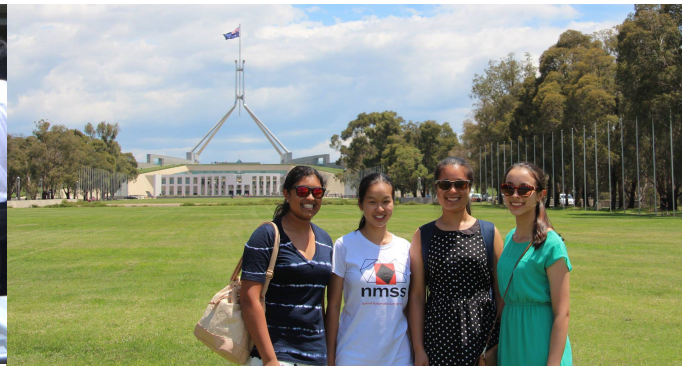
Kaela Armitage (editor)

newsletter@nmss.edu.au

A Year of Firsts

2016 was a very rewarding year for NMSS. We achieved many goals and firsts: a drop in fees (from $1400 to $1200), first ever online credit card payments, eliminated postage of information sheets, exceeded 3000 alumni, we heard a talk from Pip Pattison who attended the first ever NMSS, we welcomed a new Welfare Officer (the marvelous Michael Smith but sadly bid farewell to the great Garry Webb), and, most excitingly, we secured $5000 sponsorship from the School of Mathematics and Physics at Queensland University to cover travel costs of Qld students: our first major sponsor in over 20 years. However, we still need, and deeply appreciate, the financial support of our alumni as much as we always have. To celebrate the milestone in the number of alumni I've challenged our alumni on Facebook to donate at least $3014 and hope that our newsletter readers will match that same amount. All donations are tax deductible and you can chose to remain anonymous or not (See nmss.edu.au/donations/ or email director@nmss.edu.au for more information).

Leon Poladian



Social Network Analysis

Graph Theory is a branch of discrete mathematics sadly neglected in many curricula; thus, many students miss a chance to see exciting applications in computer science, business, psychology or sociology.

Social network analysis uses graphs to describe various situations: the nodes might represent people, organizations, or places, and the edges joining nodes can show friendship, financial interaction, academic collaboration, sexual encounters, co-starring in movies (with or without Kevin Bacon) or almost any interaction you can imagine.

Social network analysis has been used on everything from marketing and advertising, to predicting epidemics or collapse in financial networks, to tracing criminal networks. The Wikipedia page on sociograms has examples of primary school friendship networks that reveals some familiar patterns as kids get older (see if any of them remind you of your own experience).

There are mathematicians who work on developing randomly generated graphs that adequately resemble real ones. Simulating realistic networks first requires knowing which attributes of real graphs to measure. Some important features are the average number of edges joining a node, the number of particular shapes appearing in the graph, the diameter (the longest distance between any two parts of the graph, as in the famous six degrees of separation), the transitivity (how many of my friends are also friends of each other), the size and distribution of cliques (subgraphs where all nodes are connected to each other), cycles and clustering of nodes, and the tendency for nodes with similar features to be connected to each other. Psychologists and sociologists study how these features are correlated with human personality traits and behaviour patterns.

Being able to confidently simulate realistic networks allows organizations to test a variety of strategies and hypotheses (for example, for tracking criminals or managing epidemics) before actual implementation.

I really became a fan of using games for learning after seeing VAX (vax.herokuapp.com), a game that simulates an epidemic across a random social network. As the player, you get to decide which nodes get vaccinated before the epidemic and which nodes get quarantined during the epidemic (it even includes vaccine-refusers). Understanding some basic graph theory does, I believe, let you win more often!

You can read more on this topic on our NMSS website with links to tools and even research grants and papers by one of our alumni.

Leon Poladian

A Song by the 2016 EGs. Sung to the tune of "Let It Be"

When I find myself with a difficult problem
David Harvey comes to me
Tell me, can you prove it
In mod 3?

And in my hour of private study
Norm is standing next to me
Tell me, can you prove it
Just for me?

R or Q, or Z3
Satisfying, A,M, D
Tell me, can you prove it
Elegantly?

And all the confused students sitting
In projective geometry
And told to construct the line at Infinity

Even though it's second week
There's still a chance the IGs will see
Those planes are projective in
Topology

R or Q, or Z3
Satisfying, A, M, D
Tell me, can you prove it
QED

And when the room is empty,
There's a decent chance that there will be,
An assassin trying to kill me,
Brutally

R or Q, or Z3
Satisfying, A, M, D
Tell me, can you prove it
Rigorously

And though it's time for us to leave
We'll still have the memories
Signed, yours sincerely
The EGs

Private Information Retrieval

Sometimes mathematics seems magical. This article is about an idea which appears nonsensical at first glance, and impossible at second, yet mathematical ingenuity has made it possible, and advances in computational power are making it practical.

For thousands of years cryptography has protected secrets of military, political, commercial and amorous nature. Today cryptography is ubiquitous in our communications and data storage. The uses are wide and varied: providing *confidentiality* and *integrity* of information, *authentication* of identity, and *non-repudiation* of consent.

In a basic cryptographic scenario, Thanom wishes to send a secret message to her confidant David. Confidentiality means keeping the content of that message secret from a third party, mysteriously known as Leanne. Integrity means that Leanne should not be able to alter the message without David realising something is amiss. Authentication means that David can be sure it was actually Thanom who wrote the message, and non-repudiation means that Thanom cannot deny that fact later. David's reply (if there is one) can be protected in the same manner.

But there are other even less obvious uses for cryptography. "Private Information Retrieval" is a term coined in 1995 for one of those variations. In this scenario, Thanom asks dependable Leon for some information which he will dutifully look up and supply to her. Sadly, Leon is also prone to gossip. The challenge is to ensure that no-one but Thanom knows what the questions and answers are — *not even Leon!* It is the *retrieval* which is to remain private rather than the actual information. Typically Leon's database is public, which means that the information in it is already visible at least to Leon, and probably to Leanne as well.

For example, Thanom might be a network administrator and checking whether Leon (a computer) is infected with a virus. Or Leon might hold public trading data and Thanom is a broker who is monitoring the value of some shares. Alternatively Thanom may be looking up a prospective date's phone number, or the details of her embarrassing medical condition. For the sake of simplicity, let's say that Thanom is looking for the i-th entry in a list of numbers $\{x_1 , x_2 , x_3 , x_4 , \ldots , x_n\}$.

One obvious solution is for Leon to send the entire database to Thanom. This may be prohibitively expensive (do you want to download *all* of wikipedia just to hide your interest in 1980s boybands?) or Thanom may not be entitled to receive all the data (perhaps Thanom has a warrant to check on my suspicious internet habits, but not yours). It is possible to do much better.

Several methods of encryption have the special property that $E(m_1)E(m_2) = E(m_1+m_2)$. Here $E(m_1)$ means "the encryption of m_1". Such schemes are known as *homomorphic encryption* because they preserve arithmetic structure. In this case, addition of unencrypted messages corresponds to multiplication of the encrypted cipher. You can check that $E(m)^k=E(km)$ for any k as a consequence. In some circumstances, this homomorphic property of encryption is rather undesirable, because it may give Leanne a chance to modify Thanom's message without needing to know what it is. Perhaps Thanom sends E("Please donate $10 to NMSS.") and Leanne somehow multiplies it by E("1000000") in transit so that the Bank of David receives E("Please donate $1000010. to NMSS"). NMSS *will* be pleased!

Here's how Thanom can use homomorphic encryption to retrieve information privately. Thanom sends Leon a request consisting of n encrypted numbers, one for each entry in Leon's database. Underneath the encryption, the request is just a sequence of zeros, except for a number one in the desired i-th location. For example, if $i=4$ then Thanom's request to Leon is the sequence E(0), E(0), E(0), E(1), E(0), … , E(0). Leon merely raises each number in the request to the power of $x_1 , x_2 , x_3 , x_4 , \ldots , x_n$ respectively and multiplies the results together. Remember that for any value k we have $E(0)^k = E(0.k) = E(0)$ but $E(1)^k = E(1.k)=E(k)$. The end result of Leon's efforts is therefore $E(0x_1 + 0x_2 + 0x_3 + 1x_4 + \ldots + 0x_n)$, so he sends $E(x_4)$ back to Thanom without knowing quite what he has done. Magic!

The astute reader will notice that Leon or Leanne could simply examine Thanom's request, observe which entry is different from all the others, and hence determine the secret value of i. For this reason the encryption Thanom uses must also exhibit *semantic security*, which means that any given plain text has a multitude of equally valid encryptions. This is achieved by a variety of encryption algorithms. Additional features may be necessary if, for example, Leon wants assurance that Thanom got a single entry (pay per view), or if Thanom needs to prove her entitlement to the data.

You may also have noticed that Leon was forced to use the entire database in his computation. This is quite necessary, since if he ignores any entry then he knows he did not send that entry to Thanom. The aim of the game is to reduce the cost of communication. You may object that Thanom sent Leon a request which was as big as the entire database. It turns out that she can dramatically compress that request by using a recursive technique similar to binary search. Ironically we've run out of space to discuss the details.

The field of Private Information Retrieval is barely 20 years old, and has seen many exciting developments. Work continues, as researchers hope to invent a practical version of *fully homomorphic encryption*. This would allow arbitrary operations to be performed on data under encryption, not just addition. Such a breakthrough would theoretically "secure the cloud" and so be of great commercial significance. Plus, it would be exceedingly cool.

Zoltán Bácskai

Defence Science Technology Group

NMSS Past and Present

I attended NMSS in 2011 and 2012. I have great memories of hiding Zed in the lecture hall, drawing cartoons on the whiteboard, and seeing Terry's equations always just fit.

Since then, I've done a BSc and am now in my third year of medicine, doing a concurrent MPhil in translational research. One of the most helpful things I learnt in NMSS is how to approach a question. I remember distinctly that my tutor responded to 99% of my questions with "well, what do YOU think?" It was frustrating at the time, but thinking deeply about a question and using a variety of approaches, not only brings you to the answer, but to even more questions! Curiosity and the ability to view and solve a question in different ways were some of the most valuable lessons I learnt in NMSS.

NMSS showed me that there is more to maths than numbers (I loved topology, which I didn't even know existed before NMSS), and it also showed me that I can do a lot more than I thought I could. Solving a problem - after days of trying - was one of the best feelings!

I made some amazing friends in NMSS, who I still see. I meet NMSS alumni in the most unexpected places, so I hope to meet more of you in the future!

Ariel Ho

Hello readers! When I first headed to NMSS in 2011, I was unsure where mathematics would take me. I had always enjoyed it, but I enjoyed many other things too. It was in Terry Gagen's amazing number theory lectures and getting to know other people interested in mathematics that I felt a real connection to the area of study and with this in mind, I studied a Bachelor of Mathematics (adv.) at Wollongong Uni. I particularly enjoyed cryptography, artificial intelligence and real analysis.

Funnily enough, for now, that's about where my maths journey stops! Throughout my degree I played cricket with Sutherland. A few coaches recommended I pursue cricket a bit more earnestly so after my degree I started training pretty seriously. I found myself a few casual jobs, including as a pizza delivery guy, with the aim of flying across to the UK for 6 months after summer. I was not helping the (completely incorrect) stereotype that a mathematics degree isn't useful for finding full time work…

Anyway, as I'm writing this I'm looking out my window in Wickersley, UK, and getting paid (not much, but it's a start) to play cricket. I am loving my time over here; it will be an amazing experience and a great learning opportunity as well.

I hope all future students are as lucky as I have been in finding things that they love and are passionate about. I know NeMeSiS is a great place to start!

Tom Pinson

When I found out about NeMeSis halfway through last year, I knew that I wanted to be spending my holidays at the summer school. As well as being able to learn more maths, I would get to spend two weeks with people who I could really connect with – which is exactly what I did. From past experiences with long bus trips, I had expected to be spending a few hours reading or perhaps idly chatting with the people next to me. I definitely did not expect to partake in philosophical discussions and political debates for the entire bus trip! When we arrived on campus, I was met by a room full of people from different parts of the country, with various different backgrounds and personalities, all of whom were united by a love of learning. I had discovered a home away from home.

The math that I encountered was very different from the math we do in school, and the worksheets were challenging, but rewarding. I was discovering just how satisfying it was to struggle with a concept from the worksheet and then come to understand the topic better.

Something that I have learnt about life and people while at NeMeSiS, and have already been able to apply in my life, is that when a group of people come together with even one single common interest or passion, they then have the capacity to enjoy each other's company without discussing anything to do with that common interest. We all came together with a shared love for math, yet our time spent together saw a variety of discussions and activities, many of which were not math-related. To the NMSS cohort of 2016, the EGs and to all the staff, I want to take this last line to express my deepest thanks for the two weeks we shared, and I look forward to staying in touch and sharing more time and experiences in the future!

Nathaniel Knoll