# 5 minutes with Maura Paterson

*Maura Paterson (Birkbeck, University of London) visited our Department to present her seminar on "Applications of Disjoint Difference Families". She also kindly took time out with Julia Böttcher (LSE) to answer a few questions on her research interests and how she takes a break from mathematics.*

---

**Late last year, you gave a talk in our Seminar on Discrete Mathematics and Game Theory here at LSE on Disjoint Difference Families. Can you explain in layman terms what this is about?**

It's probably easiest to illustrate this with an example. Suppose you have a circular pond surrounded by a 7m long circular path. If you make two marks across the path that are one metre apart then to get from one mark to the other you either walk for one metre or, if you go around the other side of the pond, you walk for six metres. Now suppose we make a mark labelled 0, walk clockwise 1 metre and make a mark labelled 1, then walk clockwise another two metres and make a mark labelled 3. It turns out that by using just these three marks we can measure distances of any whole number of metres between 1 and 6: Walking from mark 0 clockwise to mark 1 gives a distance of 1m, walking from mark 1 clockwise to mark 3 gives 2m, walking from 0 clockwise to 3 gives 3m, walking from 3 clockwise to 0 gives 4m, walking from 3 clockwise to 1 gives 5m, and walking from 1 clockwise to 0 gives 6m (this is much easier when presented pictorially (Figure 1)).

The concept of a Disjoint Difference Family is a slightly more general version of this type of system. We are interested in considering "ponds" of different sizes, and possibly marks of different colours as well. For example, you could have a circular pond (Figure 2) surrounded by a 5m long circular path with a blue mark labelled 0, a second blue mark one metre clockwise from the first that we label 1, a red mark a further metre along clockwise labelled 2, and a second red mark two metres clockwise from the first red mark that we label 4. Then by walking between the two blue marks, or between the two red marks it is possible to go every distance that is a whole number of metres between 1 and 4.

Finding these types of systems of numbers may seem like a slightly silly puzzle, but it turns out that they can be useful in constructing other mathematical objects, many of which have interesting applications.

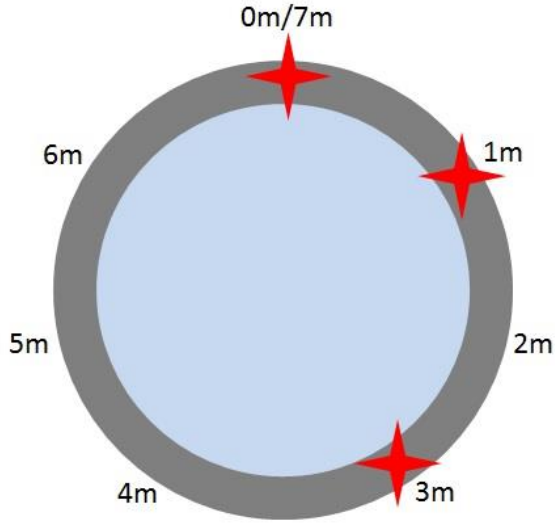


Figure 1. A circular pond surrounded by a 7m long circular path

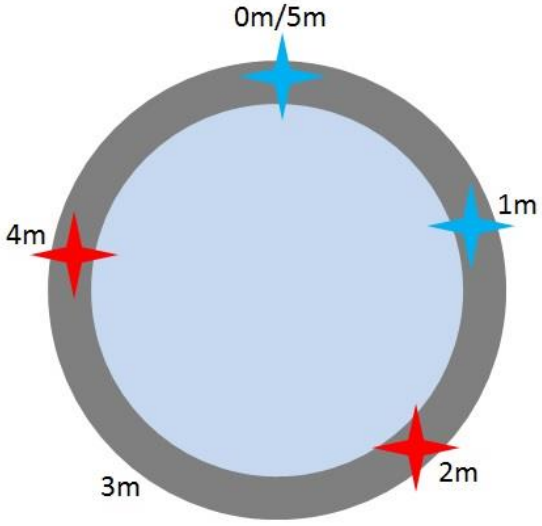


Figure 2. A circular pond surrounded by a 5m long circular path

**I particularly enjoyed the wide range of applications this has. Can you tell us something about that which you find most important?**
One important application is a situation where different users wish to communicate with a base station over a radio network where there is a fixed number of frequencies available. If two users broadcast over the same frequency at the same time, then there can be problems with interference. In the case where users don't coordinate their broadcasts ahead of time we need a system for the users to decide which frequencies to use that ensures they are not constantly interfering with each other. We can design such a system based on a Disjoint Difference Family: suppose a user walks around the 5m pond from the previous example, and whenever they pass a blue mark they broadcast on one frequency, and whenever they pass a red mark they use an alternative frequency. Now suppose a second user comes and starts walking around the pond a meter behind the first user. When they are passing the blue marks 0 and 1 their broadcasts will interfere, but the rest of the way around the pond this will not happen, due to the fact that the difference of 1m occurs only once between two marks of the same colour. Similarly, if the second user were 2, 3 or 4 m behind the first user, then their broadcasts would interfere only in one place when going around the pond. (Of course we can think of this "pond" construction as simply being a recipe for deciding how to vary the broadcast frequency over time, the users do not literally have to be walking around a pond to use it!)

**Are these ideas actually used in practice?**
Yes, systems very similar to this are used in mobile phone networks.

**Which other directions of research in information security do you specialise in. What are currently the big developments in the field? And what are the challenges – what is not yet well understood?**
I usually study systems that are "unconditionally secure" – this means that their security is not affected by the computational power of an attacker. This is in contrast to "computationally secure" systems whose security relies on the attacker being unable to perform the calculations needed to solve some problem that is believed to be hard. The security of many cryptosystems we use in practice is based on such computational assumptions, because this can enable the creation of more efficient systems, or systems with properties that are impossible to achieve in an unconditionally secure setting. However, some of the hard problems underlying cryptosystems that are widely used in practice could in fact be easily solved by a quantum computer. (For example, it is believed to be difficult for a standard computer to factorise a number that is the product of two large primes, but a quantum computer could do this quickly.) So one significant challenge for cryptographers is to devise new systems that will still be secure even if an effective quantum computer is built. To date, many of these "post-quantum" systems which have been proposed have subsequently been shown to be insecure, although there is considerable interest at the moment in developing new cryptosystems based on hard problems related to lattices.

**What other interests do you have? How do you "switch off" from mathematics?**
Listening to music and cooking help me to relax during the week. I also enjoy rock climbing, cycling, and growing vegetables.

---

LSE Mathematics

**This article was published on the Maths at LSE blog in February 2016**
http://blogs.lse.ac.uk/maths/2016/02/03/5-minutes-with-maura-paterson/