Using finite field cyclotomy to establish DPDF and EPDF constructions

Laura M Johnson

University of St. Andrews (United Kingdom) — Mathematics and Statistics

(Joint work with Sophie Huczynska)

Abstract

A Disjoint Partial Difference Family (or DPDF) is a collection of subsets of a group G, such that when you take the union of pairwise differences between elements contained within the same subset, you produce each non-identity element of G at one of two frequencies, dependant upon membership/non-membership of the component sets. An External Partial Difference Family (or EPDF) is an analogue of a DPDF in which the union of pairwise differences between elements contained within distinct subsets have the same property. Much of my research over the past three years has centered around these objects, owing to their interesting applications in design theory, coding theory and cryptography.

Finite field cyclotomy is an algebraic tool, which relates the additive and multiplicative properties of a finite field. Finite field cyclotomy has been used to establish a variety of different combinatorial combinatorial objects, including many different types of difference family.

In this talk, I will introduce both DPDFs and EPDFs, and explain how finite field cyclotomy can be used to establish constructions of these objects. I will also discuss how this work can be used to generate an algorithm, which speeds up the computation of cyclotomic numbers in certain finite fields.