MAURA PATERSON, Birkbeck, University of London

Reciprocally-weighted external difference families and unconditionally secure authentication

Let G be a finite abelian group of order n. An (n, k, λ) m-External Difference Family (EDF)is a collection of m disjoint subsets of G each of size k, with the property that each nonzero group element occurs precisely λ times as a difference between group elements in two different subsets from the collection. These have use as Algebraic Manipulation Detection (AMD) codes that can be viewed as a special case of an authentication code, which are structures which have long been studied as a tool for authenticating the sender of a message in an unconditionally secure setting. The AMD codes arising from EDFs have the nice feature that the success probability of an adversary in the worst case is equal to the average case success probability.

It is possible to generalise the notation of an EDF to allow subsets of different sizes. However, if we wish to keep the worst case=average case property, then we need to count the number of times that group elements arise as external differences using a weighted sum. Specifically, a reciprocally-weight EDF (RWEDF) is defined to be a generalisation of an EDF in which the subsets may have different sizes, and the differences are counted with a weighting given by the reciprocal of the set sizes. In this talk I will describe a construction of an infinite families of nontrivial RWEDFs, and discuss some open problems relating to these structures.