For favour of Posting
Revised (*)

THE HONG KONG UNIVERSITY OF SCIENCE & TECHNOLOGY

Department of Mathematics

SEMINAR ON PURE MATHEMATICS

Nonexistence of Strong External Difference Families in Abelian Groups

by

Prof. Ka Hin LEUNG
National University of Singapore

Abstract

Let G be an abelian group. Suppose $m \geq 2$ and $|G| = v$. Let $D_1, D_2, \cdots, D_m$ be mutually disjoint k-subsets of G. $\{D_1, D_2, \cdots, D_m\}$ is called a (v, m, k, λ)-*strong external difference family* (SEDF) in G if

$$D_j\left(\sum_{t \neq j} D_t^{(-1)}\right) = \lambda(G - 1_G)\ for\ each\ 1 \leq j \leq m.$$

The study of SEDFs is motivated by the so called algebraic manipulation detection (AMD) codes, which can be regarded as a variation of classical authentication codes. Moreover, further cryptographic applications of AMD codes have been discovered later.

So far, only one nontrivial example exists for $m \geq 3$. In this talk, I will present some recent non-existence results on abelian SEDF for $m \geq 3$. Namely, we will show that if v is a product of three (not necessarily) primes, there is no SEDF unless G is p-elementary with prime $p \geq 3 \times 10^{12}$ [1]. We also consider the case $\lambda = pq$ where p, q are primes. It can be shown that for any fixed q, no SEDF exists if p is sufficiently large.

References

[1] K. H. Leung, S. Li, and T. F. Prabowo. Nonexistence of strong external difference families in abelian groups of order being product of at most three primes. J. Combin. Theory Ser. A, 2020

[2] K. H. Leung and T. F. Prabowo. Nonexistence of Nontrivial (v, m, k, pq)-SEDF. Preprint

Date : 16 December 2021 (Thursday)*

Time : 4:00pm – 5:00pm

Zoom Meeting : https://hkust.zoom.ust/j/97394233372 (Passcode: 857784)*

All are Welcome!