Partial geometric difference sets and their links to codes and cryptography *

Oktay OLMEZ

ANKARA UNIVERSITY oolmez@ankara.edu.tr

Abstract

One of the main construction method of combinatorial designs is called difference set method. This method served as a powerful tool to construct symmetric designs, error correcting codes, graphs and cryptographic functions. In this talk we will explore a certain difference set called partial geometric difference sets. Partial geometric difference sets can be used to construct symmetric partial geometric designs. The well-known examples of partial geometric designs include 2-designs, transversal designs, and partial geometries.

Let G be a group of order v and let $S \subset G$ be a k-subset. For each $g \in G$, we define

$$\delta(g) := |\{(s,t) \in S \times S \colon g = st^{-1}\}|.$$

A k-subset S of G is called a partial geometric difference set (PGDS) in G with parameters $(v, k; \alpha, \beta)$ if there exist constants α and β such that, for each $x \in G$,

$$\sum_{y \in S} \delta(xy^{-1}) = \begin{cases} \alpha & \text{if } x \notin S, \\ \beta & \text{if } x \in S. \end{cases}$$

Difference sets (DS) and semi-regular relative difference sets (RDS) are subfamilies of PGDS. A (v, k, λ)-DS is a $(v, k; k\lambda, n + k\lambda)$-PGDS and an (m, u, k, λ) semi-regular RDS is a $(mu, k; \lambda(k-1), k(\lambda+1)-\lambda)$-PGDS.

In this talk we will explore properties of partial geometric difference sets and their links to other areas of combinatorics.

*Acknowledgement: This research is supported by TUBITAK project no: 115F064