Commun. Math. Res.
doi: 10.4208/cmr.2020-0049

Vol. **38**, No. 2, pp. 123-135
May 2022

On the Nonexistence of Partial Difference Sets by Projections to Finite Fields

Yue Zhou*

Department of Mathematics, National University of Defense Technology, Changsha 410073, China.

Received 30 November 2020; Accepted 13 April 2021

Abstract. In the study of (partial) difference sets and their generalizations in groups G, the most widely used method is to translate their definition into an equation over group ring $\mathbb{Z}[G]$ and to investigate this equation by applying complex representations of G. In this paper, we investigate the existence of (partial) difference sets in a different way. We project the group ring equations in $\mathbb{Z}[G]$ to $\mathbb{Z}[N]$ where N is a quotient group of G isomorphic to the additive group of a finite field, and then use polynomials over this finite field to derive some existence conditions.

AMS subject classifications: 05B10, 05E30, 11T06

Key words: Partial difference set, strongly regular graph, finite field.

1 Introduction

Let G be a finite group of order v and D a k-subset of G. We call D a (v,k,λ,μ) - partial difference set in G if the expressions $d_1 d_2^{-1}$, for distinct $d_1,d_2 \in D$, represent each non-identity element contained in D exactly λ times and represent each non-identity element not contained in D exactly μ times. In particular, when $\lambda=\mu$, a partial difference set is just an ordinary difference set.

*Corresponding author. *Email address:* yue.zhou.ovgu@gmail.com (Y. Zhou)

Usually, (partial) difference sets are studied using the group ring $\mathbb{Z}[G]$ or $\mathbb{C}[G]$. Let $\mathbb{Z}[G]$ denote the set of formal sums $\sum_{g\in G} a_g g$, where $a_g \in \mathbb{Z}$ and G is a multiplicative group. The addition and the multiplication on $\mathbb{Z}[G]$ are defined by

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g := \sum_{g\in G} (a_g + b_g) g,$$

and

$$\left(\sum_{g\in G} a_g g\right)\cdot\left(\sum_{g\in G} b_g g\right) := \sum_{g\in G}\left(\sum_{h\in G} a_h b_{h^{-1}g}\right)\cdot g$$

for $\sum_{g\in G} a_g g, \sum_{g\in G} b_g g \in \mathbb{Z}[G]$. Moreover,

$$\lambda\cdot\left(\sum_{g\in G} a_g g\right) := \sum_{g\in G} (\lambda a_g) g$$

for $\lambda\in\mathbb{Z}$ and $\sum_{g\in G} a_g g \in \mathbb{Z}[G]$.

For an element $D = \sum_{g\in G} a_g g \in \mathbb{Z}[G]$ and $t\in\mathbb{Z}$, we define

$$D^{(t)} := \sum_{g\in G} a_g g^t.$$

An important case is $D^{(-1)} = \sum_{g\in G} a_g g^{-1}$. If D is a subset of G, we identify D with the group ring element $\sum_{d\in D} d$. A subset D in G is a (v,k,λ,μ)-partial difference set if and only if

$$DD^{(-1)} = \mu G + (\lambda-\mu) D + \gamma 1_G, \tag{1.1}$$

where 1_G denotes the identity element of G.

When $\lambda\neq\mu$, i.e. D is not a difference set, there is always $D^{(-1)} = D$, see [8]. Note that D is a partial difference set with $D^{(-1)} = D$ and $1_G \notin D$, if and only if, D generates a strongly regular graph $\mathrm{Cay}(G,D)$. Here $\mathrm{Cay}(G,D)$ is defined to be a graph with the elements in G as vertices, and in which two vertices g and h are adjacent if and only if $gh^{-1}\in D$. Usually, a partial difference set with $D^{(-1)} = D$ and $1_G\notin D$ is called regular.

Partial difference sets have been intensively investigated for decades. There are many known constructions and necessary conditions on their existence. We refer to [9] for a classical survey. More construction results could be found in [1,10–13]. For existence conditions and classification result, see [2–4,6,15,16].

The most powerful approach for the study of (partial) difference sets is to translate their definition into an equation over group ring $\mathbb{Z}[G]$ and to investigate