ARTICLE IN PRESS
Discrete Mathematics ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

New existence and nonexistence results for strong external difference families[☆]

Jingjun Bao[a], Lijun Ji[b,*], Reizhong Wei[c], Yong Zhang[d]

[a] Department of Mathematics, Ningbo University, Ningbo 315211, China
[b] Department of Mathematics, Soochow University, Suzhou, 215006, China
[c] Department of Computer Science, Lakehead University, Thunder Bay, ON P7B 5E1, Canada
[d] Department of Mathematics, Yancheng Teachers University, Yancheng 224051, China

ARTICLE INFO

Article history:
Received 26 December 2016
Received in revised form 28 October 2017
Accepted 28 October 2017
Available online xxxx

Keywords:
Strong external difference family
Algebraic manipulation detection code
Character theory
Cyclotomic number

ABSTRACT

In this paper, we use character-theoretic techniques to give new nonexistence results for (n, m, k, λ)-strong external difference families (SEDFs). We also use cyclotomic classes to give two new classes of SEDFs with $m = 2$.

1. Introduction

Motivated by applications to algebraic manipulation detection codes (or AMD codes) [2–4], Paterson and Stinson introduced strong external difference families (or SEDFs) in [11]. SEDFs are closely related to but stronger than external difference families (or EDFs) [10]. In [11], it was noted that optimal AMD codes can be obtained from EDFs, whereas optimal strong AMD codes can be obtained from SEDFs. See [11] for a discussion of these and related structures and how they relate to AMD codes.

Recently, Martin and Stinson [9] and Huczynska and Paterson [5] further investigated the existence of SEDFs and gave some new results about the nonexistence of certain SEDFs. Their results show that the existence of SEDFs is an interesting mathematical problem in its own right, independent of any applications to AMD codes. In [9], the authors presented some nonexistence results of SEDFs by using character theory. In this paper, we shall explore such a method to give some new nonexistence results for SEDFs. Let us recall the definition of SEDFs.

Let G be a finite abelian group of order n (written multiplicatively) with the identity $e \in G$. For any two nonempty subsets A_1, A_2 of G, the multiset

$$\Delta_E(A_1, A_2) = \{xy^{-1} : x \in A_1, y \in A_2\}$$

☆ Research supported by NSFC grants 11701303 (J. Bao), 11431003 (L. Ji), 11301457 (Y. Zhang), NSERC RGPIN- 16-05610 (R. Wei), the K. C. Wong Magna Fund in Ningbo University (J. Bao) and a project funded by the priority academic program development of Jiangsu higher education institutions (L. Ji).

* Corresponding author.
E-mail addresses: baojingjun@hotmail.com (J. Bao), jilijun@suda.edu.cn (L. Ji), rwei@lakeheadu.ca (R. Wei), zyyctc@126.com (Y. Zhang).

https://doi.org/10.1016/j.disc.2017.10.032

is called the external difference of A_1 and A_2. Let k, λ, m be positive integers and let $A_1, \ldots, A_m$ be (pairwise disjoint) k-subsets of G. If the following multiset equation holds:

$$\bigcup_{\{\ell:\ell\neq j\}} \Delta_E(A_\ell, A_j) = \lambda(G \setminus \{e\})$$

for each $1 \leq j \leq m$, then the collection $\{A_1, \ldots, A_m\}$ is denoted as an (n, m, k, λ)-SEDF.

Another combinatorial structure called a strong difference family has been introduced in [1], which can be used to construct other combinatorial structures. Note that there is no relationship between SEDFs and strong difference families.

When the multiset equation is replaced with

$$\bigcup_{\{\ell,j:\ell\neq j\}} \Delta_E(A_\ell, A_j) = \lambda(G \setminus \{e\}),$$

the collection $\{A_1, \ldots, A_m\}$ is denoted as an (n, m, k, λ)-EDF. Clearly, an (n, m, k, λ)-SEDF is an $(n, m, k, m\lambda)$-EDF.

From the definition of an SEDF, it is easy to see that $m > 1$, $mk \leq n$ and

$$(m-1)k^2 = \lambda(n-1). \quad (1.1)$$

Let us recall some known results for SEDFs.

Lemma 1.1 ([5]). *For an (n, m, k, λ)-SEDF, either*
(1) $k = 1$ and $\lambda = 1$; or
(2) $k > 1$ and $\lambda < k$.

Theorem 1.2 ([11]). *There exists an $(n, m, k, 1)$-SEDF if and only if $m = 2$ and $n = k^2 + 1$, or $k = 1$ and $m = n$.*

Recent paper [9], using character theory, has established various nonexistence results, including the following:

Theorem 1.3 ([9]). *If there is an (n, m, k, λ)-SEDF with $k > 1$, then $m \neq 3$ and $m \neq 4$.*

Theorem 1.4 ([9]). *If G is any group of prime order, $k > 1$ and $m > 2$, then there does not exist an (n, m, k, λ)-SEDF over G.*

Recent paper [5] gave some necessary conditions for the existence of SEDFs with $\lambda \geq 2$ as follows.

Theorem 1.5 ([5]). *Suppose there exists an (n, m, k, λ)-SEDF with $m \geq 3$ and $k > \lambda \geq 2$. Then the following inequality must hold:*

$$\frac{\lambda(k-1)(m-2)}{(\lambda-1)k(m-1)} \leq 1.$$

In [5], Huczynska and Paterson pointed out that an $(n, m, k, 2)$-SEDF can exist only when $m = 2$ and gave an infinite class of SEDFs.

Theorem 1.6 ([5]). *For any prime power q with $q \equiv 1 \pmod 4$, there exists a $(q, 2, \frac{q-1}{2}, \frac{q-1}{4})$-SEDF over the finite field $GF(q)$.*

Martin and Stinson showed that there does not exist an (n, m, k, λ)-SEDF with $n = mk$ and $k > 1$ [9]. This can be improved as follows.

Lemma 1.7. *There does not exist an (n, m, k, λ)-SEDF with $k > 1$ and n being divisible by k.*

Proof. From (1.1), we have $(m-1)k^2 = \lambda(n-1)$. As n is divisible by k, we have $\gcd(k, n-1) = 1$, thereby λ is divisible by k^2. Let $\lambda = tk^2$ for some positive integer t, and hence $m - 1 = t(n-1)$. This shows that $t = 1$ and $n = m$. As an SEDF contains m pairwise disjoint subsets, we have $n \geq mk$. This shows that $k = 1$. □

In this paper, we also use character theory to give some new necessary conditions for the existence of SEDFs and present two new families of SEDFs by using cyclotomic classes.

The rest of this paper is organized as follows. In Section 2, we review some basic facts about characters of finite abelian groups. In Section 3, we use character theory to present some new necessary conditions for the existence of SEDFs and to give some nonexistence results for SEDFs. In Section 4, cyclotomic classes are used to present two new classes of SEDFs with $m = 2$. Finally, Section 5 concludes this paper.

2. Preliminaries

We briefly review some basic facts about characters of finite abelian groups. These can be found, for example, in [8].

For a finite abelian group G, there are exactly $n = |G|$ distinct homomorphisms (called *characters*) from G to the multiplicative group of complex numbers. In particular, the character $\chi_0 : G \to \mathbb{C}$ defined by $\chi_0(g) = 1$ for all $g \in G$ is called