
Downloaded from:

Usage Guidelines:
Please refer to usage guidelines at
contact lib-eprints@bbk.ac.uk.

or alternatively
Existence and Non-existence Results for Strong External Difference Families

Sophie Huczynska
School of Mathematics and Statistics, University of St Andrews, St Andrews, Scotland, U.K.
sh70@st-andrews.ac.uk

Maura B. Paterson
m.paterson@bbk.ac.uk

August 4, 2017

Abstract

We consider strong external difference families (SEDFs); these are external difference families satisfying additional conditions on the patterns of external differences that occur, and were first defined in the context of classifying optimal strong algebraic manipulation detection codes. We establish new necessary conditions for the existence of $(n,m,k,\lambda)$-SEDFs; in particular giving a near-complete treatment of the $\lambda = 2$ case. For the case $m = 2$, we obtain a structural characterization for partition type SEDFs (of maximum possible $k$ and $\lambda$), showing that these correspond to Paley partial difference sets. We also prove a version of our main result for generalized SEDFs, establishing non-trivial necessary conditions for their existence.

1 Introduction

Difference families are much-studied objects in combinatorial literature, and have been used to construct a range of combinatorial objects, including designs and strongly-regular graphs. They have also been applied in a variety of settings to provide a natural way of expressing various desirable properties of codes and sequences.

Given an additive abelian group $G$, a set of disjoint subsets of $G$ forms a disjoint difference family (DDF), where the differences between pairs of subset elements are called external differences if the elements lie in different subsets, and internal differences if the elements lie in the same subset. Additional properties may be imposed: for example all subsets in the family may be of the same size, the subsets may partition the group (sometimes, the non-zero elements of the group) or every non-zero element of $G$ may arise as a (internal/external) difference from the subsets of the family a constant number of times. A survey of the area is given in [11]. Historically, the external differences have been somewhat less studied than their internal counterparts. External difference families (EDFs) were introduced in [12] to construct optimal...
secret sharing schemes secure against cheating in the setting where the secrets are uniformly distributed. They are a special case of both difference systems of sets [4], and (weak) algebraic manipulation detection (AMD) codes [5]. AMD codes generalise certain known techniques for constructing secret sharing schemes secure against cheating, and it is established in [5] that such a code is equivalent to a type of DDF. In the setting of secret sharing schemes secure against sets of cheating participants who know the secret (sometimes referred to as the CDV assumption [3]) it is necessary to use a strong variant of these codes.

In this paper, we consider strong external difference families (SEDFs), introduced in [13]\(^1\). These are external difference families satisfying an extra condition, and correspond to the strong set-up in the AMD code situation. The existence of SEDFs is an active area of current investigation (for example, in [1], [7], [10], [15] and [16]). In this paper, we establish new necessary conditions for the existence of \((n, m, k, \lambda)\)-SEDFs; in particular this gives a near-complete treatment of the \(\lambda = 2\) case. For \(m = 2\), we obtain a structural characterization of partition type SEDFs (which have maximal possible \(k\) and \(\lambda\)), showing that these correspond to Paley partial difference sets. We also prove a version of our main result for generalized SEDFs, establishing non-trivial necessary conditions for their existence.

2 Preliminaries

The following definitions are given in [13]:

**Definition 2.1.** Let \(G\) be an additive abelian group. For any disjoint sets \(A_1, A_2 \subseteq G\), define the multiset
\[
\mathcal{D}(A_1, A_2) = \{x - y \mid x \in A_1, y \in A_2\}.
\]

**Definition 2.2** (External difference family). Let \(G\) be an additive abelian group of order \(n\). An \((n, m, k, \lambda)\)-external difference family (or \((n, m, k, \lambda)\)-EDF) is a set of \(m\) disjoint \(k\)-subsets of \(G\), say \(A_1, \ldots, A_m\), such that the following multiset equation holds:
\[
\bigcup_{\{i,j : j \neq i\}} \mathcal{D}(A_i, A_j) = \lambda(G \setminus \{0\}).
\]

**Definition 2.3** (Strong external difference family). Let \(G\) be an additive abelian group of order \(n\). An \((n, m, k, \lambda)\)-strong external difference family (or \((n, m, k, \lambda)\)-SEDF) is a set of \(m\) disjoint \(k\)-subsets of \(G\), say \(A_1, \ldots, A_m\), such that the following multiset equation holds for every \(i, 1 \leq i \leq m:\)
\[
\bigcup_{\{j : j \neq i\}} \mathcal{D}(A_i, A_j) = \lambda(G \setminus \{0\}).
\]

An \((n, m, k, \lambda)\)-SEDF is, by definition, an \((n, m, k, m\lambda)\)-EDF.

Various constraints on the parameters follow from the definition. The definition requires \(m \geq 2\). It is immediate that \(km \leq n\) and, as in the case of general EDFs, double-counting of the differences yields the necessary condition:
\[
\lambda(n - 1) = k^2(m - 1).
\]

Combining these yields the following lemma (see also [1]):

**Lemma 2.4.** For an \((n, m, k, \lambda)\)-SEDF, either

\(^1\)The use of the word strong in this context derives from the connection with strong algebraic manipulation detection codes. There is no connection to the concept of a strong difference family as in [2].
\[ \bullet \ k = 1 \text{ and } \lambda = 1; \text{ or} \]
\[ \bullet \ k > 1 \text{ and } \lambda < k. \]

\textbf{Proof.} Combining the two necessary conditions above yields \( \lambda(n-1) = k(km) - k^2 \leq kn - k^2 \), which rearranges to \( \frac{\lambda}{k} \leq \frac{(n-k)}{(n-1)} \), from which the result follows. \( \square \)

Note this implies that the \( k \)-sets \( A_i \) in an \( (n,m,k,\lambda) \)-SEDF \( \{A_1, \ldots, A_m\} \) can be pairs of elements only for \( \lambda = 1 \), triples only for \( \lambda = 1, 2 \), and so on.

In [13], a full description of possible parameters was obtained for the case \( \lambda = 1 \):

\textbf{Theorem 2.5 ([13])}. There exists an \((n,m,k,1)\)-SEDF if and only if \( m = 2 \) and \( n = k^2 + 1 \), or \( k = 1 \) and \( m = n \).

Constructions were given for both of these cases:

\[ \bullet \text{ Let } G = (\mathbb{Z}_{k^2+1}, +), \ A_1 = \{0, 1, \ldots, k-1\} \text{ and } A_2 = \{k, 2k, \ldots, k^2\}. \text{ This is a } (k^2 + 1, 2; k; 1)\text{-SEDF.} \]

\[ \bullet \text{ Let } G = (\mathbb{Z}_n, +) \text{ and } A_i = \{i\} \text{ for } 1 \leq i \leq n-1. \text{ This is an } (n, n; 1; 1)\text{-SEDF.} \]

Recent work by Martin and Stinson [10], using character theory, has established various SEDF non-existence results, including the following:

\textbf{Theorem 2.6}. Let \( \{D_1, \ldots, D_m\} \) form an \((n,m,k,\lambda)\)-SEDF. Then \( m \neq 3 \) and \( m \neq 4 \).

\textbf{Theorem 2.7}. If \( G \) is any group of prime order, and \( k > 1 \) and \( m > 2 \), then \( G \) admits no \( \{D_1, \ldots, D_m\} \) which form an \((n,m,k,\lambda)\)-SEDF.

3 SEDFs with \( \lambda = 2 \)

In this section, we give a substantially complete description of the case when \( \lambda = 2 \). This is based around the following non-existence result:

\textbf{Theorem 3.1}. Suppose there exists an \((n,m,k,2)\)-SEDF with \( m \geq 3 \) and \( k \geq 3 \). Then the following inequality must hold:

\[ \frac{2(k-1)(m-2)}{k(m-1)} \leq 1. \tag{2} \]

\textbf{Proof.} Suppose there exists an \((n,m,k,2)\)-SEDF with \( m \geq 3 \) and \( k \geq 3 \). We will show that, if (2) does not hold, then it is possible to find a point \( v \) in \( A_1 \) and two internal differences from \( v \) which correspond to a point \( v' \) in some \( A_i \) for \( i \neq 1 \) and two external differences from \( v' \), and thereby to construct three external differences from \( A_1 \) that are all equal.

Fix a point \( v \) in \( A_1 \). Let \( I \) be the set of internal differences from \( v \),

\[ I = \{v - a \mid a \in A_1, \ a \neq v\} \subseteq G \setminus \{0\}. \]

Then \( |I| = k-1 \), as \( |A_1| = k \).

For \( x \in A_i \) with \( i \neq 1 \) let \( E_x \) be the set of external differences from \( x \) to elements of \( A_j \) for any \( j \neq 1 \):

\[ E_x = \{x - a \mid a \in A_j, \ j \neq 1, i\}. \]

Then \( |E_x| = (m-2)k \) for any \( x \).
Figure 1: A point \( v \) in \( A_1 \) and two internal differences from \( v \), corresponding to a point \( v' \) in \( A_i \) and two external differences from \( v' \), give rise to three equal external differences from \( A_1 \).

From the definition of an \((n, m, k, 2)\)-SEDF, each nonzero group element appears twice in the multiset of external differences from \( A_j \) for each \( j = 1, 2, \ldots, m \), and hence \( 2m \) times in the multiset of all external differences

\[
\{a - b | a \in A_i, b \in A_j, j \neq i\} = 2m(\mathcal{G} \setminus \{0\}). \tag{3}
\]

Furthermore, since the multiset of external differences from \( A_1 \) comprises two copies of each nonzero group element, it is also the case that each nonzero group element occurs precisely twice as an external difference from some \( A_i \) for \( i \neq 1 \) into \( A_1 \) (since the multiset of such external differences can be obtained by negating the multiset of external differences out of \( A_1 \)). From this we can deduce that each nonzero group element occurs \( 2(m - 2) \) times as an external difference between sets \( A_i \) and \( A_j \) with \( i \neq j \) and \( i, j \neq 1 \), so

\[
\bigcup_{x \in A_i, i \neq 1} E_x = 2(m - 2)(\mathcal{G} \setminus \{0\}). \tag{4}
\]

Suppose we could find an element \( v' \in A_i \) for some \( i \neq 1 \) for which \( |E_{v'} \cap I| \geq 2 \).

Let \( \delta_1 \) and \( \delta_2 \) be distinct elements of \( E_{v'} \cap I \). Let \( u = v - \delta_1 \) and \( w = v - \delta_2 \). Then \( u \) and \( w \) are distinct elements of \( A_1 \), as \( \delta_1 \) and \( \delta_2 \) are distinct elements of \( I \). Let \( u' = v' - \delta_1 \) and \( w' = v' - \delta_2 \). Then \( u' \) and \( w' \) are distinct elements of \( \bigcup_{j \neq 1,i} A_j \) as \( \delta_1 \) and \( \delta_2 \) are distinct elements of \( E_{v'} \). (We note that \( u' \) and \( w' \) may lie in distinct \( A_j \) and \( A_\ell \), or they may both occur in a single \( A_j \) but that does not affect the rest of this argument.) Let \( v - v' = \gamma \in \mathcal{G} \setminus \{0\} \). We observe that

\[
u - u' = (v - \delta_1) - (v' - \delta_1),
= v - v',
= \gamma,
\]

and

\[
w - w' = (v - \delta_2) - (v' - \delta_2),
= v - v',
= \gamma.
\]

This would contradict the assumption that each nonzero group element occurs precisely twice as an external difference from \( A_1 \). (This situation is illustrated in Figure 1.) So we have proved that, for every \( v' \), \( |E_{v'} \cap I| \leq 1 \).
We now count the number $N$ of pairs $(\theta, E_x)$ where $\theta \in I \cap E_x$ and $x \in A_i$ for some $i \neq 1$. There are $k-1$ choices for $\theta$. As each nonzero element of $G$ occurs $2(m-2)$ times in $\bigcup_{x \in A_i, i \neq 1} E_x$, for each of these $\theta$ there are $2(m-2)$ values of $x$ for which $\theta \in E_x$, so $N = 2(k-1)(m-2)$.

The number of distinct sets $E_x$ with $x \in A_i$ for some $i \neq 1$ is $(m-1)k$. By the Pigeonhole Principle there exists $x$ for which the set $E_x$ contains at least

$$\frac{N}{(m-1)k} = \frac{2(k-1)(m-2)}{(m-1)k}$$

elements of $I$. If this quantity was strictly greater than one we would have $|E_{v'} \cap I| \geq 2$ for some $v'$.

Theorem 3.1 eliminates a wide range of values as potential parameters of an SEDF. Let us consider the regions in which (2) does not hold. These are illustrated in Figure 2. Theorem 3.1 applies for $m \geq 3$ and $k \geq 3$. When $m = 3$, the left-hand side of (2) evaluates to $k-1$, which is never greater than 1. For $m = 4$, it becomes $2 \frac{k-1}{3}$, which is greater than 1 whenever $k > 4$. For $m > 4$, the threshold is achieved when $k \geq 4$. When $k = 3$, the left-hand side of (2) evaluates to $2 \frac{2}{3} \frac{m-2}{m-1}$, which is greater than 1 whenever $m > 5$. For $k > 3$, the value of 1 is exceeded for $m \geq 5$.

These observations lead directly to the following corollary.

**Corollary 3.2.** An $(n, m, k, 2)$-SEDF can exist only when $m = 2$.

**Proof.** It is immediate from the discussion following Theorem 3.1 that, for an $(n, m, k, 2)$-SEDF to exist, its parameters must satisfy one of the following:

- $k \leq 2$;
- $m \leq 3$;
- $k = 3$ and $m = 4$;
- $k = 3$ and $m = 5$;
- Theorem 3.1 eliminates a wide range of values as potential parameters of an SEDF. Let us consider the regions in which (2) does not hold. These are illustrated in Figure 2. Theorem 3.1 applies for $m \geq 3$ and $k \geq 3$. When $m = 3$, the left-hand side of (2) evaluates to $k-1$, which is never greater than 1. For $m = 4$, it becomes $2 \frac{k-1}{3}$, which is greater than 1 whenever $k > 4$. For $m > 4$, the threshold is achieved when $k \geq 4$. When $k = 3$, the left-hand side of (2) evaluates to $2 \frac{2}{3} \frac{m-2}{m-1}$, which is greater than 1 whenever $m > 5$. For $k > 3$, the value of 1 is exceeded for $m \geq 5$.

These observations lead directly to the following corollary.

**Corollary 3.2.** An $(n, m, k, 2)$-SEDF can exist only when $m = 2$.

**Proof.** It is immediate from the discussion following Theorem 3.1 that, for an $(n, m, k, 2)$-SEDF to exist, its parameters must satisfy one of the following:

- $k \leq 2$;
- $m \leq 3$;
- $k = 3$ and $m = 4$;
- $k = 3$ and $m = 5$;
• \( k = 4 \) and \( m = 4 \).

By Lemma 2.4, we must have \( k > 2 \), so the cases \( k = 1, 2 \) cannot occur. By definition, \( m \geq 2 \), and the cases with \( m = 3, 4 \) cannot occur by Theorem 2.6. The case \( k = 3 \) and \( m = 5 \) corresponds to \( n = 19 \), and hence is ruled-out by Theorem 2.7. Hence only the case when \( m = 2 \) remains.

In the case when \( \lambda = m = 2 \), equation (1) shows that \( n = \frac{k^2}{2} + 1 \) (note this implies \( n \) and \( k \) are coprime). We have the following SEDF with \( k = 4 \) and \( n = 9 \):

Example 3.3. Let \( G = (\mathbb{Z}_3 \times \mathbb{Z}_3, +) \), let \( A_1 = \{(0,1), (0,2), (1,0), (2,0)\} \) and let \( A_2 = \{(1,1), (1,2), (2,1), (2,2)\} \). Then \( \{A_1, A_2\} \) is a \((9, 2, 4, 2)\)-SEDF.

The parameters \((9, 2, 4, 2)\) are currently the only parameters for which an SEDF with \( \lambda = 2 \) is known to exist. Example 3.3 can be viewed as part of a family of SEDFs with \( k = n - 1 \) (see Section 5); however, it is the only member of this family with \( \lambda = 2 \).

Recent work by Jedwab and Li [7] has ruled out the existence of all \((n, 2, k, 2)\) with \( n \leq 50 \) except for \( n = 33 \). The general existence question for SEDFs with \( \lambda = m = 2 \) remains open.

There are various number-theoretic constraints; for example, prime \( k \) are ruled-out by the following result.

Proposition 3.4. An \((n, 2, p, \lambda)\)-SEDF, where \( p \) is prime, can exist only for \( \lambda = 1 \).

Proof. Suppose there exists an \((n, 2, k, \lambda)\)-SEDF where \( k = p \), a prime. By equation (1), \( \lambda(n - 1) = p^2 \), and \( \lambda < p \) by Lemma 2.4. Since \( \lambda \) must divide \( p^2 \), we must have \( \lambda = 1 \). \( \square \)

4 SEDF non-existence results for general \( \lambda \)

The approach which was successful in establishing non-existence in the \( \lambda = 2 \) case can readily be generalized for larger values of \( \lambda \).

Theorem 4.1. Let \( \lambda \geq 2 \). Suppose there exists an \((n, m, k, \lambda)\)-SEDF with \( m \geq 3 \) and \( k \geq \lambda + 1 \). Then the following inequality must hold:

\[
\frac{\lambda(k - 1)(m - 2)}{(\lambda - 1)k(m - 1)} \leq 1. \tag{5}
\]

Proof. The proof of Theorem 3.1 can readily be adapted to the case of general \( \lambda \). In this setting, if (5) does not hold, then it is possible to find a point \( v \in A_1 \) and \( \lambda \) internal differences from \( v \), which correspond to a point \( v' \) in some \( A_i \) with \( i \neq 1 \) and \( \lambda \) external differences from \( v' \). This would then allow the construction of \( \lambda + 1 \) equal external differences from \( A_1 \) by the same approach we used in the proof of Theorem 3.1.

The definitions and cardinalities of \( I \) and \( E_x \) carry over exactly. Equations (3) and (8) become

\[
\{a - b \mid a \in A_i, \ b \in A_j, \ j \neq i\} = \lambda m(G\ \setminus \{0\}),
\]

and

\[
\bigcup_{x \in A_i, i \neq 1} E_x = \lambda(m - 2)(G\ \setminus \{0\}).
\]

The situation illustrated in Figure 1 carries over for general \( \lambda \) in the natural way, and our conclusion is that, for every \( v' \in A_i \ (i \neq 1) \), we must have \(|E_{v'} \cap I| \leq \lambda - 1 \).
Figure 3: A plot depicting the surface consisting of values of $m$, $k$ and $\lambda$ for which $\frac{\lambda(k-1)(m-2)}{(\lambda-1)(m-1)} = 1$. By Theorem 4.1, if there exists an $(n, m, k, \lambda)$-SEDF then the point $(k, m, \lambda)$ lies on or above the surface.

We count the number $N$ of pairs $(\theta, E_x)$ where $\theta \in I \cap E_x$ and $x \in A_i$ for some $i \neq 1$. There are $k - 1$ choices for $\theta$. Since each nonzero element of $G$ occurs $\lambda(m - 2)$ times in $\bigcup_{x \in A_i, i \neq 1} E_x$ we see that for each of these $\theta$ there are $\lambda(m - 2)$ values of $x$ for which $\theta \in E_x$, so $N = \lambda(k-1)(m-2)$. Applying the Pigeonhole Principle as before, there exists $x$ for which $E_x$ contains at least

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

elements of $I$. If this was strictly greater than $\lambda - 1$ we would have $|E_{v'} \cap I| \geq \lambda$ for some $v'$.

Theorem 4.1 applies for $m \geq 3$ and $k \geq \lambda + 1$. When $k = \lambda + 1$, the left-hand side of (5) evaluates to $\left(\frac{\lambda^3}{\lambda^3 - 1}\right) \left(\frac{m-2}{m-1}\right)$, which is greater than one whenever $m > \lambda^2 + 1$. For $k > \lambda + 1$, we observe that the left-hand side of (5) can be written $\left(\frac{\lambda k - \lambda}{\lambda k - k}\right) \left(\frac{m-2}{m-1}\right) > \left(\frac{\lambda k - k + 1}{\lambda k - k}\right) \left(\frac{m-2}{m-1}\right)$, which is greater than one if $m - 2 > (\lambda - 1)k$.

As before, if $m = 3$ the left-hand side of (5) cannot be greater than one, as $\frac{\lambda}{\lambda - 1} \leq 2$. When $m = 4$, it evaluates to $\left(\frac{2 \lambda^2}{2 \lambda^2 - 1}\right) \left(\frac{k-1}{k}\right)$, which is greater than one only in the case where $\lambda = 2$ and $k > 4$. For larger values of $m$, express the left-hand side as $\left(\frac{(\lambda m - \lambda) - \lambda}{(\lambda m - \lambda) - (m-1)}\right) \left(\frac{k-1}{k}\right)$; we would need $m - 1 > \lambda$ in order for this to be greater than one. In this case we have $\left(\frac{(\lambda m - \lambda) - \lambda}{(\lambda m - \lambda) - (m-1)}\right) \left(\frac{k-1}{k}\right) \geq \left(\frac{(\lambda m - \lambda) - (m-1) + 1}{(\lambda m - \lambda) - (m-1)}\right) \left(\frac{k-1}{k}\right)$, and for $k - 1 > (\lambda - 1)(m-1)$ the value is greater than one. The situation is illustrated in Figure 3.

**Corollary 4.2.** If there exists an $(n, m, k, \lambda)$-SEDF, then its parameters must satisfy at least one of the following:

- $\lambda = 1$;
\begin{itemize}
  \item $m = 2$;
  \item $k = \lambda + 1$ and $m \leq \lambda^2 + 1$;
  \item $k > \lambda + 1$ and $m \leq (\lambda - 1)k + 2$;
  \item $m \geq 5, \quad 2 \leq \lambda \leq m - 2$ and $k \leq (\lambda - 1)(m - 1) + 1$.
\end{itemize}

**Proof.** The following small cases are outside the scope of Theorem 4.1 and hence cannot be ruled out by the theorem:
\begin{itemize}
  \item $\lambda = 1$;
  \item $m \leq 2$;
  \item $k \leq \lambda$.
\end{itemize}
However, $m \geq 2$ by definition, and by Lemma 2.4, the case $k \leq \lambda$ cannot occur. By the discussion following the proof of the theorem, we know that any $(n, m, k, \lambda)$-SEDF within the scope of the theorem must have parameters satisfying one (or more) of the following:
\begin{itemize}
  \item $k = \lambda + 1$ and $m \leq \lambda^2 + 1$;
  \item $k > \lambda + 1$ and $m \leq (\lambda - 1)k + 2$;
  \item $m = 3$;
  \item $m = 4$, and either $\lambda > 2$ or $k \leq 3$;
  \item $m \geq 5, \quad 2 \leq \lambda \leq m - 2$ and $k \leq (\lambda - 1)(m - 1) + 1$.
\end{itemize}
The cases with $m = 3$ and $m = 4$ are ruled out by Theorem 2.6.

The number of unresolved parameter sets increases with $\lambda$. Recently, a $(243, 11, 22, 20)$-SEDF was found independently by two sets of authors ([7] and [15]). Other non-existence results have been established in numerous papers; for a summary see Jedwab and Li [7].

5 Existence results and characterizations when $m = 2$

In this section, we consider the $m = 2$ case in full generality, i.e. for all $\lambda > 1$. We consider $(n, 2, k, \lambda)$-SEDFs with largest possible value of $k$ (and hence $\lambda$).

For number-theoretic reasons, it is not possible to have an SEDF comprising two sets of size $k = \frac{n}{2}$. In this case, equation (1) would require $\lambda(2k - 1) = k^2$; this cannot happen as $2k - 1$ is coprime to $k$. The largest possible value of $k$ is therefore $k = \frac{n-1}{2}$ (here $n$ must be odd); this corresponds to the largest possible value of $\lambda = \frac{n-1}{4}$.

Denote by $G^*$ the non-identity elements of $G$. We consider constructions comprising two sets, each of size $\frac{n-1}{2}$, which partition $G^*$.

**Example 5.1.** For any prime power $q$ with $q \equiv 1 \mod 4$, there exists a $(q, 2, \frac{q-1}{2}, \frac{q-1}{4})$-SEDF in the additive group of $GF(q)$ given by $\{A_1, A_2\}$ where

\[
A_1 = \{\text{the set of squares in } GF(q)^*\}
\]
\[
A_2 = \{\text{the set of non-squares in } GF(q)^*\}.
\]
It is known that \{A_1, A_2\} is a \((q, 2, \frac{q-1}{2}, \frac{q-3}{2})\)-EDF (see for example [17]). To see that each non-zero element must arise \(\frac{q-1}{4}\) times in the multiset \(A_1 - A_2\) and \(\frac{q-3}{4}\) times in the multiset \(A_2 - A_1\), we reason as follows. Let \(x \in GF(q)^*\), and define \(D_1(x) := \{(g, h) : x = g - h, g \in A_1, h \in A_2\}\) and \(D_2(x) := \{(g, h) : x = g - h, g \in A_1, h \in A_2\}\). We exhibit a bijection between \(D_1(x)\) and \(D_2(x)\): let \((x_1, x_2) \in D_1(x)\). Then \(x = x_1 - x_2 = (-x_2) - (-x_1)\). Since \(-1\) is a square, we have \(A_1 = -A_1\) and \(A_2 = -A_2\), so that \((-x_2, -x_1) \in D_2(x)\) as required.

**Definition 5.2.** A \(k\)-element subset \(D\) of an additive group \(G\) of order \(v\) is a \((v, k, \lambda, \mu)\) partial difference set (PDS) if the multiset \(D(D) = \{d_1 - d_2 \mid d_1, d_2 \in D, d_1 \neq d_2\}\) contains each non-identity element of \(D\) exactly \(\lambda\) times and each non-identity element of \(G \setminus D\) exactly \(\mu\) times. A PDS is called abelian if the group \(G\) is abelian. A PDS \(D\) is called regular if \(D\) does not contain the identity and \(D = -D\). A regular PDS with parameters \((v, \frac{v-1}{2}, -\frac{v-5}{4}, -\frac{v-1}{4})\), where \(v \equiv 1 \mod 4\), is said to be of Paley type.

The set of non-zero squares in \(GF(q)\) when \(q \equiv 1 \mod 4\) is known to form a partial difference set (in fact, a Paley-type partial difference set). Further details on Paley PDSs can be found in [9]. The approach of constructing EDFs by partitioning with PDSs is introduced in [5]; in particular, Theorem 3.4 of [6] establishes that any set of \(u \in (v, k, \lambda, \mu)\) PDSs which partition the non-identity elements of \(G\) will form an EDF in \(G\) with parameters \((ku + 1, u, ku - 1 - \lambda - (u - 1)\mu)\). We will show that the PDS approach, applied in the \(m = 2\) setting using Paley PDSs, will in fact yield SEDFs.

We will use the following result (details may be found in [9]):

**Proposition 5.3.** Let \(G\) be an additive group of order \(v\). Let \(D_1\) be a Paley \((v, \frac{v-1}{2}, -\frac{v-5}{4}, -\frac{v-1}{4})\) PDS in \(G\), and set \(D_2 = G^* \setminus D_1\). Then \(D_2\) is also a Paley PDS with the same parameters as \(D_1\).

**Theorem 5.4.** Let \(G\) be an additive abelian group of order \(v\), let \(D_1\) be a Paley \((v, \frac{v-1}{2}, -\frac{v-5}{4}, -\frac{v-1}{4})\) PDS in group \(G\) and set \(D_2 = G^* \setminus D_1\). Then \(\{D_1, D_2\}\) is a \((v, 2, \frac{v-1}{2}, -\frac{v-1}{4})\)-SEDF.

**Proof.** Since \(D_1\) is a Paley difference set with parameters \((v, \frac{v-1}{2}, -\frac{v-5}{4}, -\frac{v-1}{4})\), so is \(D_2\), by Proposition 5.3. The fact that \(\{D_1, D_2\}\) forms an EDF is a consequence of Theorem 3.4 of [6], and can readily be seen directly, as each element of \(G^*\) occurs \(\frac{v-5}{4} + \frac{v-1}{4} = \frac{v-3}{2}\) times in the set of internal differences, and hence \((v - 2) - \frac{v-3}{2} = \frac{v-1}{2}\) times in the set of external differences. To see that this EDF is strong, let \(c \in D_1\); then the number of times \(c\) occurs in the multiset \(D_1 - D_2\) is given by \(|D_1| - 1 - \frac{v-5}{4} = \frac{v-1}{4}\). Now let \(d \in D_2\); the number of times \(d\) occurs in \(D_1 - D_2\) is \(|D_1| - 0 - \frac{v-1}{4} = \frac{v-1}{4}\). Thus \(D_1 - D_2\) comprises every element of \(G^*\) precisely \(\lambda = \frac{v-1}{2}\) times, and reversal yields the same property for \(D_2 - D_1\). \(\square\)

**Example 5.5.** Taking the set of squares and non-squares in \(GF(9)\) yields a \((9, 2, 4, 2)\)-SEDF as in Example 3.3.

It transpires that Paley PDSs offer, not simply a class of examples, but a characterization of SEDFs of partition type when \(m = 2\).

**Theorem 5.6.** Let \(G\) be an additive abelian group of order \(v\) and let \(D_1, D_2\) be two sets of size \(\frac{v-1}{2}\) which partition the non-identity elements of \(G\). Then \(\{D_1, D_2\}\) is an EDF in \(G\) if and only if \(D_1\) (and hence \(D_2\)) is a Paley PDS in \(G\).

**Proof.** \((\Rightarrow)\) Suppose \(\{D_1, D_2\}\) is an EDF. The condition \(\lambda(v - 1) = k^2(m - 1)\) of equation (1) with \(m = 2\) and \(k = \frac{v-1}{4}\) yields \(\lambda = \frac{v-1}{4}\). Since \(\lambda \in \mathbb{N}\), we must have \(v \equiv 1 \mod 4\). Hence a Paley PDS with appropriate parameters is defined for all values of \(v\) for which such an EDF can exist.
We show that if \( \{D_1, D_2\} \) is a \((v, 2, \frac{v-1}{2}, \frac{v-1}{4})\)-SEDF in \( G \), then \( D_1 \) is a Paley \((v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4})\) PDS. Consider the number of times an element \( c \) of \( D_1 \) occurs in the multiset of internal differences of \( D_1 \). In \( D_1 - G^* \), \( c \) occurs \( |D_1| - 1 \) times, while in \( D_1 - D_2 \) it occurs \( \frac{v-1}{4} \) times. Hence, if \( D_1 - D_1 \), it occurs \( \frac{v-1}{4} \) times, \( \frac{v-1}{4} = \frac{v-5}{4} \) times. An element \( d \in D_2 \) occurs \( |D_1| \) times in \( D_1 - G^* \) and \( \frac{v-1}{4} \) times in \( D_1 - D_2 \), i.e. \( \frac{v-1}{4} \) times in \( D_1 - D_1 \), as required.

We must check that \( D_1 \) is regular. By definition, \( 0 \notin D_1 \). To see that \( D_1 = -D_1 \), we show that if \( x \) lies in \( D_1 \) then so does \( -x \). Note that the elements of \( D_1 \) are precisely those elements of \( G^* \) which occur \( \frac{v-5}{4} \) times as a difference in \( D(D_1) \). Let \( x \in D_1 \), and observe that every pair \((a_1, b_1) \in D_1 \times D_1 \) such that \( x = a_1 - b_1 \), is in correspondence with the pair \((b_1, a_1) \in D_1 \times D_1 \) such that \(-x = b_1 - a_1 \). Since there are precisely \( \frac{v-5}{4} \) pairs, \(-x \notin D_1 \).

Proposition 5.3 now implies that \( D_2 \) is also a Paley PDS with the same parameters. 

\((\Leftarrow)\) This direction is established in Theorem 5.4.

This characterization tells us that an \((n, 2, \frac{n-1}{2}, \lambda)\)-SEDF can be constructed whenever an abelian Paley PDS of order \( n \) can be constructed. For example, constructions are given in [8] for groups of the form \((\mathbb{Z}_{p^r})^2 \times (\mathbb{Z}_{p^r})^2 \times \cdots \times (\mathbb{Z}_{p^r})^2 \) for \( r, r_2, \ldots, r_s \in \mathbb{Z}^+ \), and in [14] for groups of the form \( \mathbb{Z}_q^2 \times \mathbb{Z}_q^2 \) for any odd prime. 

We may ask whether there exists an \((n, 2, k, \lambda)\)-SEDF with \( k < \frac{n-1}{2} \). This is answered in the affirmative in [1] and [16] where cyclotomic constructions yield SEDFs with parameters \((q, 2, \frac{q-1}{2}, \frac{q-1}{4}) \) and \((q, 2, \frac{q-1}{6}, \frac{q-1}{36}) \) for prime powers \( q \) of certain specific forms. It is an open question which other parameter sets are possible.

6 Generalized SEDFs

In the definition of a strong external difference family, we may relax the condition on uniform set size to obtain the following, introduced in [13]:

**Definition 6.1** (Generalized Strong External Difference Family). Let \( G \) be an additive abelian group of order \( n \). An \((n, m; k_1, \ldots, k_m; \lambda_1, \ldots, \lambda_m)\)-generalized strong external difference family (or \((n, m; k_1, \ldots, k_m; \lambda_1, \ldots, \lambda_m)\)-GSEDF) is a set of \( m \) disjoint subsets of \( G \), say \( A_1, \ldots, A_m \), such that \( |A_i| = k_i \) for \( 1 \leq i \leq m \) and the following multiset equation holds for every \( i, 1 \leq i \leq m \):

\[
\bigcup_{j: j \neq i} D(A_i, A_j) = \lambda_i(G \setminus \{0\}).
\]

An \((n, m, k, \lambda)\)-SEDF is, by definition, an \((n, m; k_1, \ldots, k_m; \lambda, \ldots, \lambda)\)-GSEDF.

Two examples of GSEDFs were given in [13]:

- Let \( G = (\mathbb{Z}_n, +) \), \( A_1 = \{0\} \) and \( A_2 = \{1, 2, \ldots, n - 1\} \). This is an \((n, 2; 1, n - 1; 1, 1)\)-GSEDF.

- Let \( G = (\mathbb{Z}_7, +) \), \( A_1 = \{1\} \), \( A_2 = \{2\} \), \( A_3 = \{4\} \) and \( A_4 = \{0, 3, 5, 6\} \). This is a \((7, 4; 1, 1, 4; 1, 1, 1, 2)\)-GSEDF.

Recently, new constructions of GSEDFs based on cyclotomy have appeared in [16].

The proof strategy of Theorem 4.1 may be extended to obtain a necessary condition for the existence of a GSEDF:

**Theorem 6.2.** Suppose \( \{A_1, \ldots, A_m\} \) is an \((n, m; k_1, \ldots, k_m; \lambda_1, \ldots, \lambda_m)\)-GSEDF, where \( m \geq 3 \). Let \( \Lambda = \lambda_1 + \cdots + \lambda_m \) and \( K = k_1 + \cdots + k_m \). Then for any \( i \in \{1, \ldots, m\} \) for which
\(k_i > \lambda_i > 1\) and \(\lambda_i \leq \frac{A}{2}\), the following inequality holds:

\[
\frac{(k_1 - 1)(\Lambda - 2\lambda_1)}{(K - k_i)(\lambda_i - 1)} \leq 1.
\]  

(6)

**Proof.** Suppose, without loss of generality, that \(i = 1\) satisfies the conditions of the theorem statement, i.e. \(k_1 > \lambda_1 > 1\) and \(\lambda_1 \leq \frac{A}{2}\). We will show that if (6) does not hold, then it is possible to find a point \(v\) in \(A_1\) and \(\lambda_1\) internal differences from \(v\) which correspond to a point \(v'\) in some \(A_i\) for \(i \neq 1\) and \(\lambda_1\) external differences from \(v'\), and thereby to construct \(\lambda_1 + 1\) external differences from \(A_1\) that are all equal.

Fix a point \(v\) in \(A_1\). Let \(I\) be the set of internal differences from \(v\),

\[
I = \{v - a \mid a \in A_1, \ a \neq v\} \subseteq G \setminus \{0\}.
\]

Then \(|I| = k_1 - 1 \geq \lambda_1 > 0\).

For \(x \in A_i\) with \(i \neq 1\) let \(E_x\) be the set of external differences from \(x\) to elements of \(A_j\) for any \(j \neq 1\):

\[
E_x = \{x - a \mid a \in A_j, \ j \neq 1, i\}.
\]

Then \(|E_x| = K - k_1 - k_i\), for any \(x \in A_i\).

From the definition of an \((n, m; k_1, \ldots, k_m; \lambda_1, \ldots, \lambda_m)\)-GSEDF, each nonzero group element appears \(\lambda_j\) times in the multiset of external differences from \(A_j\) for each \(j = 1, 2, \ldots, m\), and hence \(\sum_{j=1}^{m} \lambda_j = \Lambda\) times in the multiset of all external differences:

\[
\{a - b \mid a \in A_i, \ b \in A_j, \ i \neq j\} = \Lambda(G \setminus \{0\}).
\]  

(7)

Furthermore, since the multiset of external differences from \(A_1\) comprises \(\lambda_1\) copies of each nonzero group element, it is also the case that each nonzero group element occurs precisely \(\lambda_1\) times as an external difference from \(\cup_{j \neq 1} A_i\) into \(A_1\) (since the multiset of such external differences can be obtained by negating the multiset of external differences out of \(A_1\)). Hence each non-zero group element occurs \(2\lambda_1\) times as an external difference involving \(A_1\). From this we can deduce that each nonzero group element occurs \(\Lambda - 2\lambda_1\) times as an external difference between sets \(A_i\) and \(A_j\) with \(i \neq j\) and \(i, j \neq 1\), so

\[
\bigcup_{x \in A_i, i \neq 1} E_x = (\Lambda - 2\lambda_1)(G \setminus \{0\}).
\]  

(8)

Observe that \(\Lambda - 2\lambda_1 \geq 0\) is guaranteed by the initial conditions.

Suppose we could find an element \(v' \in A_i\) for some \(i \neq 1\) for which \(|E_{v'} \cap I| \geq \lambda_1\).

Let \(\delta_1, \ldots, \delta_{\lambda_1}\) be distinct elements of \(E_{v'} \cap I\). Let \(u_t = v - \delta_t\) for \(1 \leq t \leq \lambda_1\). Then \(u_1, \ldots, u_{\lambda_1}\) are distinct elements of \(A_1\), as \(\delta_1, \ldots, \delta_{\lambda_1}\) are distinct elements of \(I\). Let \(u'_t = v' - \delta_t\) for \(1 \leq t \leq \lambda_1\). Then \(u'_1, \ldots, u'_{\lambda_1}\) are distinct elements of \(\cup_{j \neq 1, i} A_j\) as \(\delta_1, \ldots, \delta_{\lambda_1}\) are distinct elements of \(E_{v'}\). (We note that the \(u'_t\) may lie in different \(A_j\) and \(A_{ij}\), or they may all occur in a single \(A_j\) but that does not affect the rest of this argument.) Let \(v - v' = \gamma \in G \setminus \{0\}\). We observe that, for each \(1 \leq t \leq \lambda_1\),

\[
u_t - u'_t = (v - \delta_t) - (v' - \delta_t),
\]

\[
= v - v',
\]

\[
= \gamma.
\]

So \(\gamma \in G \setminus \{0\}\) occurs as an external difference from \(A_1\) a total of \(\lambda_1 + 1\) times - a contradiction. Thus for all \(v' \in A_i\ (i \neq 1)\), we must have \(|E_{v'} \cap I| \leq \lambda_1 - 1\).
We now count the number $N$ of pairs $(\theta, E_x)$ where $\theta \in I \cap E_x$ and $x \in A_i$ for some $i \neq 1$. There are $|I| = k_1 - 1$ choices for $\theta$. As each nonzero element of $G$ occurs $\Lambda - 2\lambda_1$ times in $\bigcup_{x \in A, i \neq 1} E_x$, we see that for each of these $\theta$ there are $\Lambda - 2\lambda_1$ values of $x$ for which $\theta \in E_x$, so that $N = (k_1 - 1)(\Lambda - 2\lambda_1)$.

The number of distinct sets $E_x$ with $x \in A_i$ for some $i \neq 1$ is $\sum_{j=2}^{m} k_j = K - k_1$. By the Pigeonhole Principle there exists $x$ for which the set $E_x$ contains at least

$$\frac{N}{K - k_1} = \frac{(k_1 - 1)(\Lambda - 2\lambda_1)}{K - k_1}$$

elements of $I$. Whenever this quantity is at least $\lambda_1$, i.e. strictly greater than $(\lambda_1 - 1)$, we have $|E_v' \cap I| \geq \lambda_1$ for some $v'$. Thus no such GSEDF will exist if

$$\frac{(k_1 - 1)(\Lambda - 2\lambda_1)}{K - k_1} > \lambda_1 - 1.$$

It is clear that the same argument will hold with 1 replaced by any appropriate $i \in \{1, \ldots, m\}$ for which the conditions in the theorem statement are satisfied.

Observe that taking $k_i = k$ and $\lambda_i = \lambda$ for all $1 \leq i \leq m$ yields Theorem 4.1, while further setting $k_i = k$ and $\lambda_i = 2$ for all $1 \leq i \leq m$ yields Theorem 3.1.

7 Concluding remarks

This paper establishes various conditions under which SEDFs and GSEDFs can exist, and establishes a structural characterization of partition type SEDFs in the $m = 2$ case. Future directions are two-fold; the fine-tuning of such necessary conditions, with the aim of completely characterising the possible parameters sets, and the development of further construction methods and structural characterizations. One specific open problem concerns the existence of SEDFs with $\lambda = m = 2$ when $k$ is less than the maximum possible size of $\frac{n-1}{2}$. It would be desirable to gain further understanding of the general case when $m = 2$. By [10], the next-smallest $m$ for which SEDFs may exist is $m = 5$; further investigation of this case would be another natural focus.

Acknowledgements

Thanks to Siaw-Lynn Ng for helpful discussions, and to the anonymous referees for their comments. The first author is supported by a Research Incentive Grant from The Carnegie Trust for the Universities of Scotland.

References


