Pairwise balanced designs from finite fields

Marco Buratti

Dipartimento di Ingegneria Elettrica, Università de L’Aquila, I-67040 Poggio di Roio, L’Aquila, Italy

Received 5 March 1997; revised 26 May 1998; accepted 1 June 1998

Abstract

Developing previous work by R.C. Bose, R.M. Wilson, M. Greig and the author, we give a general construction for difference families over finite fields. All the DFs constructed before were generated by a single initial base block so that they were uniform. Here we also consider DFs generated by two or more initial base blocks. These DFs give rise to pairwise balanced designs which of course are balanced block designs exactly when the initial base blocks have constant size. © 1999 Elsevier Science B.V. All rights reserved.

Keywords: Pairwise balanced design; Balanced incomplete block design; Difference family

1. Introduction

A \((v, K, \lambda)\) pairwise balanced design (PBD) is a pair \((V, \mathcal{B})\) where \(V\) is a \(v\)-set whose elements are called points and \(\mathcal{B}\) is a family of subsets of \(V\) (blocks) with sizes from \(K\) such that any 2-subset of \(V\) is contained in exactly \(\lambda\) blocks. The integer \(\lambda\) is the index of the PBD. A PBD of index 1 is a linear space and its blocks are usually called lines. A \((v, K, \lambda)\)-PBD where \(K = \{k\}\) is a singleton is a balanced block design and is denoted by \((v, k, \lambda)\)-BIBD. A \((v, k, 1)\)-BIBD is also called a Steiner 2-design.

An automorphism group of a PBD is a group of permutations on the point-set \(V\) which leaves invariant the block-family \(\mathcal{B}\).

Given an additive group \(G\) of order \(v\) and a set \(K\) of positive integers, a \((v, K, \lambda)\) difference family (DF) over \(G\) is a family of subsets of \(G\) (base blocks) having sizes belonging to \(K\) and such that each non-zero element of \(G\) can be represented as the difference of two elements of some base block in exactly \(\lambda\) ways. Also here, in the case where \(K = \{k\}\) we simply speak of \((v, k, \lambda)\) difference family.

The connection between \((G, K, \lambda)\)-DFs and PBDs is explained by the following theorem.
Theorem 1.1. Let \( F \) be a \((v,K,\lambda)\)-DF over \( G \) and let \( \mathcal{B} = \{ A + g \mid A \in F, \ g \in G \} \). Then \((G, \mathcal{B})\) is a \((|G|,K)\)-PBD admitting \( G \) as an automorphism group acting regularly on the point-set.

Note that a \((v,k,\lambda)\)-DF (uniform DF) gives rise to a BIBD, that a \((v,K,1)\)-DF (simple DF) gives rise to a linear space and hence that a \((v,k,1)\)-DF gives rise to a Steiner 2-design.

Let \( F \) be a difference family over the additive group of a ring \( R \). Following Abel [7], we say that certain base blocks \( A_1, \ldots, A_t \) are initial base blocks of \( F \) if any other base block is a multiple of a suitable \( A_i \), namely of type \( \{ ra \mid a \in A_i \} \) where \( r \) is an element of \( R \). Also, we say that a base block \( A \) admits \( w \) as a multiplier (of order \( n \)) if \( w \) is a unit of \( R \) (of order \( n \)) such that \( wA := \{ wa \mid a \in A \} \) is a translate of \( A \). A multiplier is said to be proper if distinct from 1. When \( w \) is a multiplier of all the base blocks, then \( w \) is a multiplier of \( F \). In this case the map \( \hat{w} : x \in R \to wx \in R \) is an automorphism group of the PBD associated with \( F \).

A DF over the additive group of a finite field \( \text{GF}(q) \) is radical when admits a set \( \{ A_1, A_2, \ldots, A_t \} \) of initial base blocks each of which is a subgroup of \( \text{GF}(q) \) and possibly zero. So, in a radical difference family each base block of size \( k \) has a multiplier of order \( k - 1 \) or \( k \) according to whether it contains or not zero.

There are several papers concerning the direct construction of uniform DFs over the additive group of a finite field. Mostly, these DFs are simple and generated by a single initial base block. We briefly summarize the content of these papers.

More than one century ago, although notation and terminology were different, it was proved that \((q,3,1)\) radical DFs exist for any admissible \( q \). This result is usually associated with Netto [24] but Anderson [1] recently pointed out that there are remarkable papers by Anstice [2,3] preceding 40 years the work of Netto.

In 1939 Bose [10] gave sufficient conditions for the existence of \((q,k,1)\) radical DFs in the cases \( k = 4 \) and \( k = 5 \). \((q,k,1)\) radical difference families with \( k \) arbitrary were considered in 1969 by Bhat [8] and, more deeply, in 1972 by Wilson [25]. Bhat gave few examples of radical \((q,k,\lambda)\)-DFs with \( \lambda > 1 \) and Wilson gave a series of radical DFs having \( k \) or \( k - 1 \) divisible by \( 2\lambda \). Also, Wilson gave constructions for \((q,6,1)\)-DFs generated by an initial base block with a multiplier of order 3.

But the deepest result of the paper of Wilson is that a \((q,k,\lambda)\)-DF generated by an initial base block without proper multipliers (we will refer to such a family as a Wilson difference family) exists for any admissible prime power \( q \) sufficiently large \( q > \left( \frac{k}{2} \right)^{k(k-1)} \). Unfortunately, the asymptotic existence-proof of a Wilson difference family is not constructive, in the sense that it does not give a general method for finding concretely the initial base-block. Anyway, it seems that for small values of \( k \), a \((q,k,\lambda)\) Wilson difference family almost always exists, namely it is not necessary that \( q \) is so large. This has been shown by the author in the cases \( k = 4,5 \) [11] and by Abel [4,7], in the cases \( k = 6, 7, 8, 9 \).
The author [12,13] revived and improved the previously known constructions for simple radical DFs giving a sufficient condition for their existence. The author conjectures that his condition is also necessary, but he is able to prove it only for block size \( k < 9 \).

In 1990 Greig [19], following the way indicated by Wilson, gave constructions for \((q,k,1)\)-DFs generated by a suitable initial base block with a multiplier of order \( n \). Greig has also given some \((q,k,2)\)-DFs for values of \( q \) and \( k \) for which he did not succeed in constructing a \((q,k,1)\)-DF.

The author [14] has presented a construction for simple DFs which is slightly more general than Greig’s one. This more general construction yields, for instance, a \((577,9,1)\)-DF whose existence was previously in doubt. The DF in question has a multiplier of order 3 and has been used by Greig himself [22] for constructing several other designs.

Abel [5] has recently constructed new BIBDs some of which are generated by small DFs over finite fields (they require at most four base blocks). The parameters of these families are: \((67,12,4)\), \((97,9,3)\), \((121,10,3)\), \((121,16,4)\), \((181,10,2)\).

We also recall that Furino [20] has considered \((v,k,\lambda)\)-DFs over finite rings (which are not fields) generated by a single initial base block.

In this paper we propose a very general construction for \((q,K,\lambda)\)-DFs over finite fields removing the restriction \(|K| = 1\). Also, even in the case of a uniform difference family \(\mathcal{F}\), we consider the possibility that \(\mathcal{F}\) is generated by at least two initial base blocks. Indeed, in the case of a non-uniform DF, we are obviously obliged to construct it in this way (at least one initial base block of size \( k \) for each \( k \in K \)).

**Notation.** Throughout the paper, given a prime power \( q \) we will use the standard notation introduced by Wilson:

- \( H \) is the multiplicative group of \( \text{GF}(q) \).
- \( \omega \) is a fixed primitive root in \( \text{GF}(q) \), i.e. a fixed generator of \( H \).
- \( \text{ind} \) is the map from \( H \) to \( \mathbb{Z}_{q-1} \) defined by \( \text{ind}(\omega^i) = i \).

For a fixed divisor \( d \) of \( q - 1 \), \( H^d \) is the group of \( d \)th powers of \( H \). One can think to this group also as the group of \( [(q - 1)/d] \)th roots of unity in \( \text{GF}(q) \).

For a given \( \epsilon \in H \), \( \langle \epsilon \rangle \) is the subgroup of \( H \) generated by \( \epsilon \). Lists, i.e. multiset, will be denoted by parentheses \( () \) while, as usual, sets will be denoted by braces \( \{ \} \). For given lists \( A, A' \) defined on \( \text{GF}(q) \) we set \( AA' := (aa' \mid a \in A, a' \in A') \). Analogously, for given lists \( X, X' \) defined on \( \mathbb{Z}_n \) we set \( X + X' := (x + x' \mid x \in X, x' \in X') \).

The **strong union** of given lists \( L_1, \ldots, L_t \) is the list denoted by \( L_1 \cup \cdots \cup L_t \) where every element is counted a number of times equal to the sum of its respective multiplicities in \( L_1, \ldots, L_t \). In particular, \( \lambda L \) is the strong union of \( n \) copies of \( L \), i.e. the list in which every element of \( L \) is repeated exactly \( \lambda \) times.

A list \( L \) defined on \( \text{GF}(q) \) is **evenly distributed over the \( d \)th power cosets of \( \text{GF}(q) \)** if all the cosets of \( H^d \) contain the same number, say \( \lambda \), of elements from \( L \). This happens provided that \( \text{ind} L = \lambda \mathbb{Z}_n (\text{mod } d) \).
For a given subset \( A \) of \( \text{GF}(q) \), \( \Delta A \) is the list of differences from \( A \), i.e. \( \Delta A = (a - a' \mid a, a' \in A, a \neq a') \). Finally, for a given family \( \mathcal{F} \) of subsets of \( \text{GF}(q) \), \( \Delta \mathcal{F} \) is the list of differences from \( \mathcal{F} \), i.e. \( \Delta \mathcal{F} = \bigcup_{A \in \mathcal{F}} \Delta A \).

We need the following useful lemma.

**Lemma 1.2.** Let \( q \) be a prime power and let \( e \) be a divisor of \( q - 1 \). Let \( \zeta \) be a primitive \( e \)-th root of unity in \( \text{GF}(q) \) and let \( B = \{ b_1, b_2, \ldots, b_f \} \) be a set of distinct representatives for the cosets of \( \langle \zeta \rangle \) in \( H \). Then we have:

\[
\Delta(H^{\frac{q-1}{e}} B) = H^{\frac{q-1}{e}} L,
\]

where

\[
\sigma = \begin{cases} 
2 & \text{if } q \text{ and } e \text{ are odd}, \\
1 & \text{otherwise},
\end{cases}
\]

and where

\[
L = \left( b_i (\zeta^j - 1) \mid 1 \leq i \leq f; 1 \leq j \leq \frac{e-1}{\sigma} \right) \cup \left( b_i - b_j \zeta^h \mid 1 \leq i < j; 1 \leq h \leq \frac{2e}{\sigma} \right).
\]

Also, we have:

\[
\Delta(H^{\frac{q-1}{e}} B \cup \{0\}) = H^{\frac{q-1}{e}} (B \cup (2 - \sigma)(-B) \cup L)
\]

where \( \sigma \) and \( L \) are defined like above.

The easy proof is omitted.

### 2. The general construction

The following theorem gives a general method for obtaining a DF admitting a prescribed set \( \{A_1, A_2, \ldots, A_t\} \) of initial base blocks.

**Theorem 2.1.** Let \( A_1, A_2, \ldots, A_t \) be subsets of \( \text{GF}(q) \) with sizes from a set \( K \). Let \( \Delta A_h = H^{n_h} L_h \) for suitable divisors \( n_h \) of \( q - 1 \) and suitable lists \( L_h \)'s defined on \( \text{GF}(q) \), \( i = 1, \ldots, t \). Set \( n = \gcd(n_1, \ldots, n_t) \) and \( \text{ind}(L_h) = X_h \pmod{n} \) for \( h = 1, \ldots, t \). Assume that \( I_1, I_2, \ldots, I_t \) are multisets defined on \( \mathbb{Z}_n \) such that \( (X_1 + I_1) \cup (X_2 + I_2) \cup \cdots \cup (X_t + I_t) = \mathbb{Z}_n (\pmod{n}) \). Then, the family

\[
\mathcal{F} := \left( A_h \zeta^{i+jn} \mid 1 \leq h \leq t, i \in I_h, 0 \leq j < \frac{n_h}{n} \right)
\]

is a \((q, K, \lambda)\)-DF.

**Proof.** We have to prove that \( \Delta \mathcal{F} = \lambda H \).

Setting \( B_h = \{ \omega_i \mid i \in I_h \} \) and \( C_h = \{ \omega^{jn} \mid 0 \leq j < \frac{n_h}{n} \} \) for \( h = 1, \ldots, t \), we have:

\[
\Delta \mathcal{F} = \left( \Delta A_1 B_1 C_1 \cup (\Delta A_2) B_2 C_2 \cup \cdots \cup (\Delta A_t) B_t C_t \right)
\]

\[
= H^{n_1} L_1 B_1 C_1 \cup H^{n_2} L_2 B_2 C_2 \cup \cdots \cup H^{n_t} L_t B_t C_t.
\]
Then, observing that $C_h$ is a complete set of representatives for the cosets of $H^n$ in $H$ and hence that $H^n C_h = H^n$, we have:

$$\Delta \mathcal{F} = H^n (L_1 B_1 \cup L_2 B_2 \cup \cdots \cup L_t B_t).$$

Now note that $\text{ind}(L_1 B_1 \cup L_2 B_2 \cup \cdots \cup L_t B_t) = (\text{ind} L_1 \cup \text{ind} B_1) \cup (\text{ind} L_2 \cup \text{ind} B_2) \cup \cdots \cup (\text{ind} L_t \cup \text{ind} B_t) = (X_1 + I_1) \cup (X_2 + I_2) \cup \cdots \cup (X_t + I_t) = \lambda \mathbb{Z}_n$. This means that $L_1 B_1 \cup L_2 B_2 \cup \cdots \cup L_t B_t$ has exactly $\lambda$ elements in each coset of $H^n$ in $H$, i.e. that $H^n (L_1 B_1 \cup L_2 B_2 \cup \cdots \cup L_t B_t) = \lambda H$. \hfill \Box

We will apply the previous theorem in conjunction with Lemma 1.2 assuming that each $A_h$ is of type $H^{(q-1)\varepsilon_b} B_h$ or $H^{(q-1)\varepsilon_b} B_h \cup \{0\}$ for suitable divisors $e_b$ of $q - 1$. Of course each $A_h$ admits $H^{(q-1)\varepsilon_b}$ as a group of multipliers. Consequently, setting $d = \gcd(e_1, e_2, \ldots, e_t)$, it is easy to see that $H^{(q-1)\varepsilon_b}$ is a group of multipliers for the resultant difference family. By way of illustration, we begin to show some examples.

**Example 2.2.** Let $q = 71$. We can take $\omega = 7$ as a primitive root (mod $q$) Then $\varepsilon := \omega^{(q-1)/7} = 710$ is a primitive 7th root of unity in $\mathbb{F}(q)$. Consider the sets $A_1 = \langle \varepsilon \rangle$ and $A_2 = \langle \varepsilon \rangle \cup \{0\}$. By Lemma 1.2 we have $\Delta A_1 = \mathbb{F}^5 L_1$ and $\Delta A_2 = \mathbb{F}^5 L_2$ with $L_1 = (\varepsilon - 1, \varepsilon^3 - 1, \varepsilon^5 - 1)$ and $L_2 = \{1\} \cup L_1$.

Here, $n = 5$. We have: $X_1 = \text{ind} L_1 = \text{ind}(710 - 1, 720 - 1, 740 - 1) = \text{ind}(44, 36, 31) = (43, 64, 11) = (3, 4, 1) \pmod{5}$.

Hence $X_2 = (0, 3, 4, 1) \pmod{5}$.

Since $[X_1 + (3, 4)] \cup X_2 = 2Z_5 \pmod{5}$, applying Theorem 2.1 we have that $\mathcal{F} := \langle 7^3 A_1, 7^4 A_1, A_2 \rangle$ is a $(71, \{7, 8\}, 2)$-DF admitting the 7th roots of unity as a group of multipliers.

**Example 2.3.** Let $q = 109$. We can take $\omega = 6$ as a primitive root (mod $q$). Then, $\varepsilon := \omega^{(q-1)/9} = 6^{12}$ is a primitive 9th root of unity in $\mathbb{F}(q)$. Consider the set $A = \langle \varepsilon \rangle$. By Lemma 1.2 we have $\Delta A = \mathbb{F}^6 L$ with $L = (\varepsilon - 1, \varepsilon^2 - 1, \varepsilon^3 - 1, \varepsilon^4 - 1)$.

Here, $n = 6$. We have:

$X = \text{ind} L = \text{ind}(6^{12} - 1, 6^{24} - 1, 6^{36} - 1, 6^{48} - 1) = \text{ind}(15, 37, 62, 26) = (44, 5, 71, 16) = (2, 5, 5, 4) \pmod{6}$.

Since $X + (0, 2, 4) = 2Z_6 \pmod{6}$, applying Theorem 2.1 we have that $\mathcal{F} := \langle A, 6^2 A, 6^4 A \rangle$ is a $(109, 9, 2)$-DF admitting the 9th roots of unity as a group of multipliers.

**Example 2.4.** Let $q = 631$. We can take $\omega = 3$ as a primitive root (mod $q$).

Then $\varepsilon := \omega^{(q-1)/5} = 3^{126}$ and $\phi := \omega^{(q-1)/7} = 3^{50}$ are primitive 5th and 7th roots of unity (mod $q$), respectively. Consider the sets $A_1 = \langle \varepsilon \rangle$ and $A_2 = \langle \phi \rangle$. By Lemma 1.2 we have $\Delta A_1 = H^{63} L_1$ and $\Delta A_2 = H^{45} L_2$ with $L_1 = (\varepsilon - 1, \varepsilon^2 - 1)$ and $L_2 = (\phi - 1, \phi^2 - 1, \phi^3 - 1)$. 

\[\begin{align*}
\begin{array}{cccc}
\varepsilon & \phi & \varepsilon^2 & \phi^2 \\
3^{126} & 3^{50} & 3^{126} & 3^{50} \\
\end{array}
\end{align*}\]
Here, \( n = \gcd(63, 45) = 9 \). We have:

\[
X_1 = \text{ind } L_1 = \text{ind}(3^{126} - 1, 3^{252} - 1) = \text{ind}(241, 511) = (551, 556) = (2, 7) \pmod{9}.
\]

\[
X_2 = \text{ind } L_2 = \text{ind}(3^{90} - 1, 3^{180} - 1, 3^{270} - 1) = \text{ind}(268, 426, 20) = (344, 391, 142) = (2, 4, 7) \pmod{9}.
\]

Since \([X_1 + (1, 7, 8)] \cup X_2 = Z_9 \pmod{9}\), applying Theorem 2.1 we have that the family \( \mathcal{F} : = (3^{i+9}A_1 | i = 1, 7, 8) \cup (3^9A_2 | 0 \leq j < 5) \) is a \((631, f_5, 7, g_1)-DF\).

The initial base blocks \( A_1 \) and \( A_2 \) admit the 5th and the 7th roots of unity as respective groups of multipliers, but \( \mathcal{F} \) has not multipliers.

The previous examples are of radical DFs. Let us see an example of nonradical DF obtainable using Theorem 2.1.

Example 2.5. Let \( q = 73 \). We can take \( \omega = 5 \) as a primitive root \( \pmod{q} \). Then \( \varepsilon := \omega^{(q-1)/3} = 5^{24} \) is a primitive 3rd root of unity \( \pmod{q} \).

Consider the sets \( A_1 = \langle \varepsilon \rangle \cup \{0\} \) and \( A_2 = \langle 3, 5 \rangle \). By Lemma 1.2 we have \( \Delta A_1 = H^{12}L_1 \) and \( \Delta A_2 = H^{12}L_2 \) with \( L_1 = (1, \varepsilon - 1) \) and \( L_2 = (3(\varepsilon - 1), 5(\varepsilon - 1), 2, 5 - 3\varepsilon, 5 - 3\varepsilon^2) \).

Here, \( n = 12 \). We have:

\[
X_1 = \text{ind } L_1 = \text{ind}(1, 7) = (0, 33) = (0, 9) \pmod{12}
\]

\[
X_2 = \text{ind } L_2 = \text{ind}(21, 35, 2, 54, 32) = (39, 34, 8, 26, 40) = (3, 10, 8, 2, 4) \pmod{12}
\]

Since \( X_1 \cup [X_2 + (0, 3)] = Z_{12} \pmod{12} \), we have that the family \( \mathcal{F} : = (A_1, A_2, 3A_2) \) is a \((73, \{4, 6\}, 1)-DF\) admitting the 3rd roots of unity as a group of multipliers.

3. Simplifying the general construction

The general construction given in the previous section leads to the following problem:

**Problem.** Given a \( t \)-ple \( (X_1, X_2, \ldots, X_t) \) of lists defined on \( Z_n \) and given an integer \( \lambda \), determine a \( t \)-ple \( (I_1, I_2, \ldots, I_t) \) of lists on \( Z_n \) such that \( (X_1 + I_1) \cup (X_2 + I_2) \cup \cdots \cup (X_t + I_t) = \lambda Z_n \).

This problem appears to be extremely difficult. We have already studied it in the particular case where \( t = \lambda = 1 \) (see [15] and, for further generalizations, [16]). Our investigation led to the following result:

**Theorem 3.1.** Let \( X \) be an \( m \)-subset of \( Z_n \) and let \( (d_0, \ldots, d_{2s+1}) \) be a chain of divisors of \( n \) satisfying the following conditions:

1. \( \prod_{x=0}^{s} d_{2x+1}/d_{2x} = n/m; \)
2. \( \forall x, y \in X, x - y \) is divisible by \( d_{2x-1} \) but not by \( d_{2x} \) for some \( x \).

Then, if

\[
I := \left\{ \prod_{x=0}^{s} d_{2x}i_x \left| 0 \leq i_x < d_{2x+1}/d_{2x}, x = 0, 1, \ldots, s \right. \right\},
\]

we have that \( X + I = Z_n \).
Now we show how the previous result helps in finding a practical method of using Theorem 2.1.

**Theorem 3.2.** With the same notation as in Theorem 2.1, set \( L := L_1 \cup L_2 \cup \cdots \cup L_t \). Then, assume that \( m := \frac{|L|}{\lambda} \) is an integer dividing \( n \) and that there is a chain \((d_0, \ldots, d_{2s+1})\) of divisors of \( n \) and a partition \((L = S_1 \cup S_2 \cup \cdots \cup S_t)\) of \( L \) in \( m \)-subsets of \( \text{GF}(q) \) satisfying the following conditions:

(i) \( \prod_{z=0}^{s} d_{2z+1}/d_{2z} = n/m; \)

(ii) \( \forall h = 1, \ldots, \lambda, \forall x, y \in S_h, \text{ind} x - \text{ind} y \) is divisible by \( d_{2s-1} \) but not by \( d_{2s} \) for some \( x \).

Then, defining \( I \) as in Theorem 3.1, we have that

\[
\mathcal{F} := \left\{ A_h \omega^{j+i} \mid 1 \leq h \leq t, i \in I, 0 \leq j < \frac{n_h}{n} \right\}
\]

is a \((q, k, \lambda)\)-DF.

**Proof.** By Theorem 3.1 we have \( \text{ind} S_h + I = Z_n \pmod{n} \) for each \( h = 1, \ldots, \lambda \). This implies that \( \text{ind} L + I = \lambda Z_n \pmod{n} \) and hence that the identity \((X_1 + I_1) \cup (X_2 + I_2) \cup \cdots \cup (X_t + I_t) = \lambda Z_n \pmod{n} \) holds with \( I_h = I \) for each \( h \). Then the assertion follows from Theorem 2.1. \( \square \)

The most simple way of exploiting the previous theorem is to try with a chain of type \((1, 1, m, n)\). Such an attempt is described in the following theorem.

**Theorem 3.3.** With the same notation as in Theorem 2.1 suppose that the list \( L := L_1 \cup L_2 \cup \cdots \cup L_t \) is evenly distributed over the \( m \)-th power cosets of \( \text{GF}(q) \) for a suitable divisor \( m \) of \( n \); say \( \text{ind} L = \lambda Z_m \pmod{m} \). Then the family

\[
\mathcal{F} := \left\{ A_h \omega^{i+j} \mid 1 \leq h \leq t, 0 \leq i < \frac{n}{m}, 0 \leq j < \frac{n_h}{n} \right\}
\]

is a \((q, k, \lambda)\)-DF.

**Proof.** By assumption \( L \) has exactly \( \lambda \) elements in each coset of \( H^m \) in \( H \). This is equivalent to say that \( L \) is partitionable into \( \lambda \) systems \( S_1, \ldots, S_\lambda \) of representatives for the cosets of \( H^m \) in \( H \). So, for each pair of distinct elements \( x, y \) in \( S_h \) we have that \( \text{ind} x - \text{ind} y \) is not divisible by \( m \). It follows that the condition of Theorem 3.2 is satisfied with respect to the chain of divisors \((d_0 = 1, d_1 = 1, d_2 = m, d_3 = n)\). So, applying that theorem the assertion follows. \( \square \)

The case where Theorem 3.3 fails but Theorem 3.2 succeeds in finding a difference family of prescribed parameters, seems to be a quite rare occurrence. An example of such an exceptional case is the \((577,9,1)\)-DF mentioned in the introduction and found in [14]. Now, we show an example with \( \lambda > 1 \).
Example 3.4. Let \( q = 433 \). We can take \( \omega = 5 \) as a primitive root of unity (mod \( q \)). Then \( \omega^{(q-1)/27} = 5^{16} \) is a primitive 27th root of unity (mod \( q \)). Consider the set \( A = \langle \omega \rangle \cup \{0\} \). By Lemma 1.2 we have \( A^i = H^iL \) where

\[
L = \{1\} \cup (\omega^i - 1 \mid 1 \leq i \leq 13)
\]

\]

Since \( m = |L|/7 = 2 \), we can try to find a \((433, 28, 7)\)-DF with initial base block \( A \) (hence a radical DF). In order that Theorem 3.3 works for our purpose we should have \( \text{ind} L = 7Z_2 \) (mod 2) while an easy calculation shows that \( \text{ind} L = 6Z_2 \cup (0, 0) \) (mod 2). On the other hand we can partition \( L \) in seven pairs \((a_1, b_1), \ldots, (a_7, b_7)\) in such a way that \( \text{ind} a_i - \text{ind} b_i \equiv 2 \) (mod 4) for each pair \((a_i, b_i)\) so that Theorem 3.2 succeeds using the chain \((1, 2, 4, 8)\). One can check that a working partition is the following:

\[
L = (16, 288) \cup (416, 384) \cup (197, 49) \cup (1, 334) \cup (138, 149) \cup (255, 160) \cup (21, 65).
\]

As a corollary of Theorem 3.3 we get:

Corollary 3.5. Let \( k_1, \ldots, k_t, \lambda \) be positive integers such that \( \lambda(q - 1) \equiv 0 \) (mod \( m \)) where \( m := (1/2\lambda) \sum_{h=0}^t k_h(k_h - 1) \) is also an integer. Let \( q \equiv 1 \) (mod \( m \)) be an odd prime power and let \( A_h := \{a_{h,1}, a_{h,2}, \ldots, a_{h,k_h}\} \) be a \( k_h \)-subset of \( GF(q) \). Then, if the list \( L := (a_{h,r} - a_{h,s} \mid 1 \leq h \leq t, 1 \leq r < s \leq k_h) \) is evenly distributed over the \( m \)th power cosets of \( GF(q) \), we have that

\[
\mathcal{F} := \left( A_h\omega^{mi} \mid 1 \leq h \leq t, 0 \leq i < \frac{q - 1}{2m} \right)
\]

is a \((q, K, \lambda)\)-DF where \( K = \{k_1, \ldots, k_t\} \).

Proof. We have \( \Delta A_h = \{1, -1\}L_h \) where \( L_h = (a_{h,r} - a_{h,s} \mid 1 \leq r < s \leq k_h) \), i.e. \( \Delta A_h = H^iL_h \) with \( n_h = (q - 1)/2 \), \( h = 1, \ldots, t \). Since \( L \), i.e. the strong union of the \( L_h \)'s, has \( \frac{1}{2} \sum_{h=0}^t k_h(k_h - 1) \) elements and is evenly distributed over the \( m \)th power cosets of \( GF(q) \), we have \( \text{ind} L = \lambda Z_m \) (mod \( m \)). Then, applying Theorem 3.3, we get the assertion.

Note that when \( t = 1 \) the previous corollary coincides with Wilson's lemma on evenly distributed differences [25], just the first step leading to the asymptotic existence theorem mentioned in the introduction.

We say that a \((q, K, \lambda)\)-DF is balanced when the number of base blocks of size \( k \) is constant for \( k \in K \). For instance, the difference families obtainable by Corollary 3.5 are balanced in the hypothesis that the \( k_h \)'s are pairwise distinct. Now, we give a cyclotomic condition leading to balanced \((q, \{3, 4\}, 1)\) radical DFs.
Theorem 3.6. Let \( q = 18u + 1 \) be a prime power and let \( 3^e \) be the highest power of 3 dividing \( u \). Then, if 3 is not a 3\(^{e+1}\)th power in GF(q), there exists a balanced \((q,\{3,4\},1)\) radical DF.

Proof. Let \( \varepsilon \) be a primitive 3rd root of unity in GF(q) and consider the sets \( A_1 := \langle \varepsilon \rangle \cup \{0\} \), \( A_2 := (\varepsilon - 1)/(\varepsilon) \). By Lemma 1.2 we have \( \Delta A_1 = H^3L_1 \) and \( \Delta A_2 = H^3L_2 \) where \( L_1 = (1, \varepsilon - 1) \) and \( L_2 = ((\varepsilon - 1)^2) \).

Since 3 is not a 3\(^{e+1}\)th power in GF(q), there is a suitable \( f \leq \varepsilon \) such that 3 is a 3\(^{f}\)th power but not a 3\(^{f+1}\)th power in GF(q). As a consequence we have that:

\[ \text{ind } 3 \equiv 3^f \text{ or } 3^{f/2} \pmod{3^{f+1}} \]

Since \( \varepsilon \) is a primitive 3rd root of unity in GF(q) we have \( \varepsilon^2 + \varepsilon + 1 = 0 \) and hence \( (\varepsilon - 1)^2 = -3\varepsilon \). Then, since \( \text{ind}(-1) = 9u \) and \( \text{ind}(\varepsilon) = 6u \) or \( 12u \), we have:

\[ \text{ind}(\varepsilon - 1)^2 = 2 \text{ind}(\varepsilon - 1) = \text{ind}(-3\varepsilon) \equiv 3^f \text{ or } 3^{f/2} \pmod{3^{f+1}}. \]

It easily follows that:

\[ \text{ind}(L_1 \cup L_2) = \text{ind}(1, \varepsilon - 1, (\varepsilon - 1)^2) = (0, 3^f, 3^{f/2}) \pmod{3^{f+1}}. \]

This means that conditions (i), (ii) of Theorem 3.2 are satisfied with \( \lambda = 1 \) with respect to the chain \((1, 3^f, 3^{f+1}, 3u)\). So, applying that theorem we have that

\[ \mathcal{F} := \left\{ \{A_i \varepsilon^{3^{f+1}i+j} : h = 1, 2; \ 0 \leq i < \frac{u}{3^f}; \ 0 \leq j < 3^f \} \right\} \]

is a \((q,\{3,4\},1)\)-DF.

Finally, note that the above family has \( u \) base blocks of size 3 and \( u \) base blocks of size 4. \hfill \Box

Table 1

Some \((q,\mathcal{K},1)\) radical DFs with \(|\mathcal{K}| = 2 \text{ or } 3\)

<table>
<thead>
<tr>
<th>( q )</th>
<th>( \omega )</th>
<th>( \mathcal{K} )</th>
<th>( n )</th>
<th>( m )</th>
<th>Initial base blocks</th>
</tr>
</thead>
<tbody>
<tr>
<td>241</td>
<td>7</td>
<td>{4,5}</td>
<td>8</td>
<td>4</td>
<td>( R_3 \cup {0}, \omega R_9 )</td>
</tr>
<tr>
<td>151</td>
<td>6</td>
<td>{4,6}</td>
<td>5</td>
<td>5</td>
<td>( R_3 \cup {0}, \alpha^2 R_5 \cup {0} )</td>
</tr>
<tr>
<td>631</td>
<td>3</td>
<td>{4,7}</td>
<td>15</td>
<td>5</td>
<td>( R_2 \cup {0}, R_7 )</td>
</tr>
<tr>
<td>1009</td>
<td>11</td>
<td>{4,8}</td>
<td>24</td>
<td>6</td>
<td>( R_1 \cup {0}, \omega R_2 \cup {0} )</td>
</tr>
<tr>
<td>2143</td>
<td>3</td>
<td>{4,10}</td>
<td>119</td>
<td>7</td>
<td>( R_5 \cup {0}, \omega R_2 \cup {0} )</td>
</tr>
<tr>
<td>1051</td>
<td>2</td>
<td>{5,6}</td>
<td>10</td>
<td>5</td>
<td>( R_5, \omega R_5 \cup {0} )</td>
</tr>
<tr>
<td>1051</td>
<td>7</td>
<td>{5,7}</td>
<td>15</td>
<td>5</td>
<td>( R_5, \omega R_7 )</td>
</tr>
<tr>
<td>421</td>
<td>2</td>
<td>{5,8}</td>
<td>6</td>
<td>6</td>
<td>( R_5, \omega^2 R_7 \cup {0} )</td>
</tr>
<tr>
<td>9721</td>
<td>7</td>
<td>{5,9}</td>
<td>108</td>
<td>7</td>
<td>( R_5, \omega^3 R_9 )</td>
</tr>
<tr>
<td>6301</td>
<td>10</td>
<td>{5,10}</td>
<td>70</td>
<td>7</td>
<td>( R_5, \omega R_9 \cup {0} )</td>
</tr>
<tr>
<td>7351</td>
<td>6</td>
<td>{7,8}</td>
<td>525</td>
<td>7</td>
<td>( R_7, \omega R_7 \cup {0} )</td>
</tr>
<tr>
<td>211</td>
<td>2</td>
<td>{4,5,6}</td>
<td>70</td>
<td>7</td>
<td>( \omega R_7 \cup {0}, R_7, \omega^3 R_3 )</td>
</tr>
<tr>
<td>7351</td>
<td>6</td>
<td>{4,5,7}</td>
<td>35</td>
<td>7</td>
<td>( R_5 \cup {0}, \omega R_3 \cup {0} )</td>
</tr>
<tr>
<td>7561</td>
<td>13</td>
<td>{4,6,8}</td>
<td>36</td>
<td>9</td>
<td>( R_7 \cup {0}, \omega R_7 \cup {0} )</td>
</tr>
<tr>
<td>7561</td>
<td>13</td>
<td>{5,6,8}</td>
<td>108</td>
<td>9</td>
<td>( R_5, \omega^2 R_7 \cup {0}, \omega^2 R_7 \cup {0} )</td>
</tr>
<tr>
<td>631</td>
<td>3</td>
<td>{5,7,8}</td>
<td>9</td>
<td>9</td>
<td>( R_5, \omega R_7, \omega R_7 \cup {0} )</td>
</tr>
</tbody>
</table>
Table 2
Some \((q,K,1)\)-DFs with \(q < 1000\) and \(|K| = 2\) or 3

<table>
<thead>
<tr>
<th>(q)</th>
<th>(\omega)</th>
<th>(K)</th>
<th>(n)</th>
<th>(m)</th>
<th>Initial base blocks</th>
</tr>
</thead>
<tbody>
<tr>
<td>337</td>
<td>10</td>
<td>{4,6}</td>
<td>56</td>
<td>7</td>
<td>(\omega R_1 \cup {0}, {1,33}R_1)</td>
</tr>
<tr>
<td>601</td>
<td>7</td>
<td>{4,6}</td>
<td>20</td>
<td>10</td>
<td>(\omega^2 R_5 \cup {0}, \omega^2 R_2 \cup {0}, {1,16}R_3)</td>
</tr>
<tr>
<td>163</td>
<td>2</td>
<td>{4,7}</td>
<td>27</td>
<td>9</td>
<td>(\omega^2 R_5 \cup {0}, {1,67}R_3 \cup {0})</td>
</tr>
<tr>
<td>991</td>
<td>6</td>
<td>{4,10}</td>
<td>33</td>
<td>11</td>
<td>(\omega^2 R_3 \cup {0}, {1,29}R_3 \cup {0})</td>
</tr>
<tr>
<td>631</td>
<td>3</td>
<td>{5,6}</td>
<td>21</td>
<td>7</td>
<td>(\omega^2 R_5, {1,262}R_3)</td>
</tr>
<tr>
<td>811</td>
<td>3</td>
<td>{5,7}</td>
<td>27</td>
<td>9</td>
<td>(\omega^2 R_3, {1,28}R_3 \cup {0})</td>
</tr>
<tr>
<td>991</td>
<td>6</td>
<td>{5,10}</td>
<td>99</td>
<td>11</td>
<td>(\omega^2 R_5, {1,128}R_3)</td>
</tr>
<tr>
<td>337</td>
<td>10</td>
<td>{6,7}</td>
<td>8</td>
<td>8</td>
<td>{1,17}R_3, \omega R_7)</td>
</tr>
<tr>
<td>433</td>
<td>5</td>
<td>{6,7}</td>
<td>72</td>
<td>12</td>
<td>(\omega^2 {1,58}R_3, {1,62}R_3 \cup {0})</td>
</tr>
<tr>
<td>541</td>
<td>2</td>
<td>{4,5,6}</td>
<td>18</td>
<td>9</td>
<td>(\omega^2 R_3 \cup {0}, \omega^2 R_2, {1,2}R_3)</td>
</tr>
<tr>
<td>331</td>
<td>3</td>
<td>{4,5,7}</td>
<td>11</td>
<td>11</td>
<td>(\omega^2 R_5 \cup {0}, \omega^2 R_5, {1,73}R_3 \cup {0} )</td>
</tr>
<tr>
<td>337</td>
<td>10</td>
<td>{4,6,7}</td>
<td>56</td>
<td>14</td>
<td>(\omega^2 R_3 \cup {0}, \omega^2 {1,7}R_3, {1,9}R_3 \cup {0})</td>
</tr>
<tr>
<td>421</td>
<td>2</td>
<td>{4,6,7}</td>
<td>10</td>
<td>10</td>
<td>(\omega^2 R_3 \cup {0}, \omega^2 R_5 \cup {0}, {1,16}R_3)</td>
</tr>
<tr>
<td>199</td>
<td>3</td>
<td>{4,6,9}</td>
<td>11</td>
<td>11</td>
<td>(\omega^2 0R_3 \cup {0}, {1,18}R_3, \omega^2 R_9)</td>
</tr>
<tr>
<td>433</td>
<td>5</td>
<td>{4,6,10}</td>
<td>24</td>
<td>12</td>
<td>(\omega^2 R_3 \cup {0}, {1,2}R_3, \omega^2 R_9 \cup {0})</td>
</tr>
</tbody>
</table>

The values of \(q < 1,000\) for which the above construction succeeds are 19, 37, 109, 127, 163, 181, 199, 361, 379, 397, 433, 487, 541, 631, 739, 757, 811, 829, 883, 919, 937.

Now, with the only aim of giving more examples, we present two tables (Tables 1 and 2) of simple DFs obtainable using Theorem 3.3. In Table 1 the DFs are also radical. In both the tables, we give the variables \(\omega, m, n\) and the initial base blocks. Also, in order to simplify the notation, the group of \(e\)th roots of unity (mod \(q\)) will be denoted by \(R_e\), instead of \(H^{(q-1)/e}\).

4. Some constructions for balanced block designs

We finally examine which consequences the above constructions have for balanced block designs. First of all, applying Theorem 3.3 using only one initial base block we get the following theorems.

**Theorem 4.1.** Let \(e, f\) and \(\lambda\) be positive integers such that \(e\) is odd and \(m := f(e f - 1) / 2 \lambda\) is also an integer. Let \(q = 2em + 1\) be a prime power and let \(A = \langle e \rangle B\) where \(e\) is an \(e\)th primitive root of unity in \(GF(q)\) and where \(B = \{b_1, b_2, \ldots, b_f\}\) is an \(f\)-subset of \(GF(q)^*\). Then, if the list

\[ L := (b_j (e^i - 1)) | 1 \leq j \leq f; 1 \leq i \leq \frac{1}{2}(e - 1)) \cup (b_j - b_j e^h | 1 \leq j < f; 1 \leq h \leq e) \]

is evenly distributed over the \(m\)th power cosets of \(GF(q)\), we have that the family \(\mathcal{F} := (Ae^m | 1 \leq i \leq t)\) is a \((q,e,f,\lambda)-DF\).
Theorem 4.2. Let \( e, f \) and \( \lambda \) be positive integers such that \( e \) is odd and \( m := f(e + 1)/2 \lambda \) is also an integer. Let \( q = 2emt + 1 \) be a prime power and let \( A = \langle \varepsilon \rangle B \cup \{0\} \) where \( \varepsilon \) is an \( e \)th primitive root of unity in \( \text{GF}(q) \) and where \( B = \{b_1, b_2, \ldots, b_f\} \) is an \( f \)-subset of \( \text{GF}(q) \). Then, if the list
\[
L := (b_j(\varepsilon^j - 1) | 1 \leq j \leq f; \ 1 \leq i \leq \frac{1}{2}(e - 1)) \cup
(b_i - b_j \varepsilon^h | 1 \leq i < j \leq f; \ 1 \leq h \leq e) \cup B
\]
is evenly distributed over the \( m \)th power cosets of \( \text{GF}(q) \), we have that the family \( \mathcal{F} := (\langle \varepsilon \rangle \sigma^{|i-1} | 0 \leq i < t) \) is a \((q, ef + 1, \lambda)\)-DF.

We point out that applying the previous theorems in the case where \( \lambda = 1 \) we rediscover the constructions for simple DFs given by Greig. Instead, applying them using \( f = 1 \), we get the following constructions for uniform radical DFs.

Theorem 4.3. Let \( k \) be an odd integer and let \( \lambda \) be a divisor of \( \frac{1}{2}(k-1) \), say \( \frac{1}{2}(k-1) = 2m \). Now let \( q = [k(k-1)/\lambda]t + 1 \) be a prime power and let \( \varepsilon \) be a primitive \( k \)th root of unity in \( \text{GF}(q) \). Then, if the list \( L := (\varepsilon - 1, \varepsilon^2 - 1, \ldots, \varepsilon^{k-1} - 1) \) is evenly distributed over the \( m \)th power cosets of \( \text{GF}(q) \), we have that
\[
\mathcal{F} := (\langle \varepsilon \rangle \sigma^{|i-1} \cup \{0\} | 0 \leq i < t)
\]
is a \((q, k, \lambda)\) radical difference family.

Theorem 4.4. Let \( k \) be an even integer and let \( \lambda \) be a divisor of \( k/2 \), say \( k/2 = \lambda m \). Now let \( q = [k(k-1)/\lambda]t + 1 \) be a prime power and let \( \varepsilon \) be a primitive \((k-1)\)th root of unity in \( \text{GF}(q) \). Then, if the list \( L := (1, \varepsilon - 1, \varepsilon^2 - 1, \ldots, \varepsilon^{k-1} - 1) \) is evenly distributed over the \( m \)th power cosets of \( \text{GF}(q) \), we have that
\[
\mathcal{F} := (\langle \varepsilon \rangle \sigma^{|i-1} \cup \{0\} | 0 \leq i < t)
\]
is a \((q, k, \lambda)\) radical difference family.

In particular, applying Theorems 4.3 and 4.4 assuming that \( \lambda = \lfloor \frac{k}{2} \rfloor \) we get, as a corollary, the following well-known result by Wilson (see [25], Theorem 7).

Corollary 4.5. There exists a \((q, k, \lfloor \frac{k}{2} \rfloor)\)-DF for any admissible prime power \( q \).

Several examples of \((q, k, 1)\) radical DFs were given in previous articles (see [10,12,13,21,5]). We get \((q, k, \lambda)\) radical DFs using Theorems 4.3 and 4.4 for many values of \( q, k \), and \( \lambda \). Some of these values are listed in Table 3. Of course, we have not reported values for which a \((q, k, \lambda)\) radical DF is easily obtainable from already known smaller DFs.

Our \((113,8,2)\) and \((109,9,2)\) difference families are new. In fact, although Abel has given difference families with these parameters (see [7], Table 10.51 and Table 10.45), they are not radical. His \((113,8,2)\)-DF is a Wilson difference family while his \((109,9,2)\)-DF is generated by a single initial base block of order 3.
We recall that a quasimultiple projective plane of order \( n \) is a \( (n^2 + n + 1, n + 1, \lambda) \)-BIBD. Note that the \((241,16,4)\) and \((601,25,3)\) DFs given in Table 3 give rise to quasimultiple projective planes of orders 15 and 24 respectively. The smallest values of \( \lambda \) for which quasimultiple projective planes of these orders were previously known were 8 and 11, respectively (see [23]). As far as the author is aware, all the BIBDs associated with the radical DFs listed in Table 3 are new.

We note that not every \((q,k,\lambda)\) radical difference family can be obtained using Theorems 4.3 and 4.4. In fact these theorems are corollaries of Theorem 3.3 which, in general, requires a stronger condition than Theorem 3.2 does. This was already pointed out in Example 3.4 where we have found a \((433,28,7)\) radical difference family. Other exceptional \((q,k,\lambda)\) radical DFs that we get using Theorem 3.2 have the following parameters:

\[(1289,8,2), (1117,9,2), (6689,12,3), (937,13,3)\]

\[(5281,16,4), (2857,17,4), (2281,20,5), (2521,21,5)\].

Now, we want to show some examples of difference families obtainable using Theorems 4.1 and 4.2 with \( f \neq 1 \). Applying Theorem 4.1 with \( e = 5 \) and \( f = 2 \) we can get \((q,10,3)\)-DFs for all the admissible primes \( q < 1000 \) with the only exceptions of \( q = 31 \) and \( q = 61 \). In Table 4, we indicate how to take the set \( B \) in order that the condition of the theorem be satisfied.

Applying Theorem 4.2 with \( e = 7 \) and \( f = 2 \) we can get \((q,15,5)\)-DFs for all the admissible primes \( q < 1000 \) with the only exceptions of \( q = 43, 127, 379, 421 \). In Table 5 we indicate how to take the set \( B \) in order that the condition of the theorem be satisfied.

### Table 3
Some \((q,k,\lambda)\) radical difference families

<table>
<thead>
<tr>
<th>( q )</th>
<th>( k )</th>
<th>( \lambda )</th>
<th>( q )</th>
<th>( k )</th>
<th>( \lambda )</th>
<th>( q )</th>
<th>( k )</th>
<th>( \lambda )</th>
</tr>
</thead>
<tbody>
<tr>
<td>113</td>
<td>8</td>
<td>2</td>
<td>409</td>
<td>17</td>
<td>4</td>
<td>601</td>
<td>25</td>
<td>3</td>
</tr>
<tr>
<td>109</td>
<td>9</td>
<td>2</td>
<td>3469</td>
<td>18</td>
<td>3</td>
<td>5101</td>
<td>25</td>
<td>4</td>
</tr>
<tr>
<td>4357</td>
<td>12</td>
<td>2</td>
<td>1483</td>
<td>19</td>
<td>3</td>
<td>701</td>
<td>25</td>
<td>6</td>
</tr>
<tr>
<td>397</td>
<td>12</td>
<td>3</td>
<td>1901</td>
<td>20</td>
<td>5</td>
<td>349</td>
<td>29</td>
<td>7</td>
</tr>
<tr>
<td>859</td>
<td>13</td>
<td>2</td>
<td>1009</td>
<td>21</td>
<td>5</td>
<td>4651</td>
<td>31</td>
<td>5</td>
</tr>
<tr>
<td>1249</td>
<td>13</td>
<td>3</td>
<td>7177</td>
<td>24</td>
<td>3</td>
<td>1613</td>
<td>32</td>
<td>8</td>
</tr>
<tr>
<td>241</td>
<td>16</td>
<td>4</td>
<td>1289</td>
<td>24</td>
<td>6</td>
<td>4621</td>
<td>33</td>
<td>8</td>
</tr>
</tbody>
</table>

### Table 4
\((q,10,3)\)-DFs with \( q < 1000 \) and with a multiplier of order 5

<table>
<thead>
<tr>
<th>( q )</th>
<th>( B )</th>
<th>( q )</th>
<th>( B )</th>
<th>( q )</th>
<th>( B )</th>
<th>( q )</th>
<th>( B )</th>
</tr>
</thead>
<tbody>
<tr>
<td>151</td>
<td>{1,11}</td>
<td>271</td>
<td>{1,11}</td>
<td>571</td>
<td>{1,4}</td>
<td>691</td>
<td>{1,3}</td>
</tr>
<tr>
<td>181</td>
<td>{1,8}</td>
<td>331</td>
<td>{1,3}</td>
<td>601</td>
<td>{1,6}</td>
<td>751</td>
<td>{1,22}</td>
</tr>
<tr>
<td>211</td>
<td>{1,2}</td>
<td>421</td>
<td>{1,2}</td>
<td>631</td>
<td>{1,6}</td>
<td>811</td>
<td>{1,3}</td>
</tr>
<tr>
<td>241</td>
<td>{1,2}</td>
<td>541</td>
<td>{1,26}</td>
<td>661</td>
<td>{1,18}</td>
<td>991</td>
<td>{1,10}</td>
</tr>
</tbody>
</table>
Table 5
(q,15,5)-DFs with q < 1000 and with a multiplier of order 7

<table>
<thead>
<tr>
<th>q</th>
<th>B</th>
<th>q</th>
<th>B</th>
<th>q</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td>211</td>
<td>{1,14}</td>
<td>547</td>
<td>{1,16}</td>
<td>757</td>
<td>{1,15}</td>
</tr>
<tr>
<td>337</td>
<td>{1,18}</td>
<td>631</td>
<td>{1,5}</td>
<td>883</td>
<td>{1,27}</td>
</tr>
<tr>
<td>463</td>
<td>{1,10}</td>
<td>673</td>
<td>{1,17}</td>
<td>967</td>
<td>{1,7}</td>
</tr>
</tbody>
</table>

Table 6
(q,15,3)-DFs with q < 1000 and with a multiplier of order 5

<table>
<thead>
<tr>
<th>q</th>
<th>B</th>
<th>q</th>
<th>B</th>
<th>q</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td>421</td>
<td>{1,4,36}</td>
<td>631</td>
<td>{1,11,84}</td>
<td>701</td>
<td>{1,40,98}</td>
</tr>
</tbody>
</table>

Note that the (211,15,5)-DF indicated above, gives rise to a quasimultiple projective plane of order 14. The smallest value of \( \lambda \) for which a quasimultiple projective plane of this order was previously known was 6 (see [23]). In a future article [17] the author will give other small quasimultiple projective planes using Theorems 4.1 and 4.2.

Applying Theorem 4.2 with \( e = 7 \) and \( f = 2 \) we get \((491,15,3)\) and \((911,15,3)\) difference families. For obtaining them it suffices to take \( B = \{1,62\} \) in the first case and \( B = \{1,27\} \) in the second case. Of course, both these DFs have a multiplier of order 7. Instead, \((q,15,3)\)-DFs with a multiplier of order 5 can be obtained using Theorem 4.1 with \( e = 5 \) and \( f = 3 \). Three of them are given in Table 6.

Note that Theorems 4.1, 4.2 give DFs having a single initial base block \( A \). Now, we show some examples of uniform DFs constructed via Theorem 3.3 and admitting two initial base blocks.

**Example 4.6.** Let \( q = 631 \). We can take \( \omega = 3 \) as a primitive root \((\text{mod } q)\). Then \( \varepsilon := \omega^{(q-1)/5} = 3^{126} \) and \( \phi := \omega^{(q-1)/9} = 3^{70} \) are primitive 5th and 9th roots of unity \((\text{mod } q)\) respectively. Consider the sets \( A_1 = \langle \varepsilon \rangle \{1, 56\} \) and \( A_2 = 17 \langle \phi \rangle \cup \{0\} \). By Lemma 1.2 we have \( \Delta A_1 = H^{63}L_1 \) and \( \Delta A_2 = H^{35}L_2 \) where

\[
L_1 = (\varepsilon - 1, \varepsilon^2 - 1, 56(\varepsilon - 1), 56, 56 - \varepsilon, 56 - \varepsilon^2, 56 - \varepsilon^3, 56 - \varepsilon^4)
\]

\[
L_2 = (17, 17(\phi - 1), 17(\phi^2 - 1), 17(\phi^3 - 1), 17(\phi^4 - 1)).
\]

Here \( n = \gcd(63, 35) = 7 \). We have:

\[
\ind(L_1 \cup L_2) = \ind(241, 511, 245, 221, 55, 445, 175, 459, 408, 98, 25, 161, 497, 28) = (551, 556, 484, 489, 275, 286, 161, 301, 593, 6, 522, 625, 561, 465)
\]

\[= 2Z_7 \pmod{n} \]

So, applying Theorem 3.3 we have that the family

\[
\mathcal{F} := \langle A_1 \omega^{7j} \mid 0 \leqslant j < 9 \rangle \cup \langle A_2 \omega^{7j} \mid 0 \leqslant j < 5 \rangle
\]

is a \((631,10,2)\)-DF.
Table 7

<table>
<thead>
<tr>
<th>(q)</th>
<th>(k)</th>
<th>(\lambda)</th>
<th>Initial base blocks</th>
</tr>
</thead>
<tbody>
<tr>
<td>661</td>
<td>11</td>
<td>8</td>
<td>(R_{11} \cup {0})</td>
</tr>
<tr>
<td>1321</td>
<td>11</td>
<td>4</td>
<td>(o^{3}R_{11} \cup {0})</td>
</tr>
<tr>
<td>1093</td>
<td>14</td>
<td>10</td>
<td>(R_{14} \cup {0})</td>
</tr>
<tr>
<td>6553</td>
<td>14</td>
<td>5</td>
<td>(o^{3}R_{14} \cup {0})</td>
</tr>
<tr>
<td>2731</td>
<td>14</td>
<td>4</td>
<td>(o^{2}R_{14} \cup {0})</td>
</tr>
<tr>
<td>421</td>
<td>15</td>
<td>11</td>
<td>(oR_{15} \cup {0})</td>
</tr>
<tr>
<td>2053</td>
<td>19</td>
<td>14</td>
<td>(oR_{19} \cup {0})</td>
</tr>
<tr>
<td>8209</td>
<td>19</td>
<td>7</td>
<td>(o^{2}R_{19} \cup {0})</td>
</tr>
</tbody>
</table>

Example 4.7. Let \(q = 881\). We can take \(\omega = 3\) as a primitive root \((\text{mod } q)\). Then \(\varepsilon := \omega^{(q-1)/5} = 3^{176}\) and \(\phi := \omega^{(q-1)/11} = 3^{80}\) are primitive 5th and 11th roots of unity \((\text{mod } q)\), respectively.

Consider the sets \(A_1 = \langle \varepsilon \rangle \cup \{0\}\) and \(A_2 = \langle \phi \rangle\). By Lemma 1.2 we have \(\Delta A_1 = H^{88}L_1\) and \(\Delta A_2 = H^{40}L_2\) where

\[
L_1 = (1, 69, \varepsilon - 1, \varepsilon^2 - 1, 69(\varepsilon - 1), 69(\varepsilon^2 - 1), 68, 69 - \varepsilon, 69 - \varepsilon^2, 69 - \varepsilon^3, 69 - \varepsilon^4),
\]

\[
L_2 = (9(\phi - 1), 9(\phi^2 - 1), 9(\phi^3 - 1), 9(\phi^4 - 1), 9(\phi^5 - 1)).
\]

Here \(n = \gcd(88, 40) = 8\). We have:

\[
\text{ind}(L_1 \cup L_2) = \text{ind}(1, 69, 285, 743, 283, 169, 68, 664, 206, 487, 682, 649, 622, 410, 279, 784)
\]

\[
= (0, 618, 141, 594, 759, 332, 715, 214, 567, 448, 873, 363, 533, 260, 865, 366)
\]

\[
= 2Z_n \pmod n.
\]

So, applying Theorem 3.3 we have that the family

\[
\mathcal{F} := \langle A_1 \omega^j \mid 0 \leq j < 11 \rangle \cup \langle A_2 \omega^j \mid 0 \leq j < 5 \rangle
\]

is a \((881, 11, 2)\)-DF.

As far as the author is aware, no \((v, 10, 2)\)-DF with \(91 < v < 1000\) and no \((v, 11, 2)\)-DF with \(v < 1000\) were previously known.

We conclude giving some other examples of small uniform difference families having two initial base blocks (Table 7).

Note added in proof

While this paper was in preparation, K. Chen and L. Zhu proved that for \(k \in \{4, 5, 6\}\) there exists a \((q, k, 1)\)-DF for any admissible prime power \(q\) with the only exception of a \((61, 6, 1)\)-DF. These results may be found in [18,19].
5. For further reading

The following references are also of interest to the reader: [6] and [9].

References

[22] M. Greig, Recursive constructions of balanced incomplete block designs with block size of 7, 8, or 9, Preprint.