Heffter arrays from finite fields

Marco Buratti *

Dedicated to Doug Stinson on the occasion of his 66th birthday

Abstract

After extending in the obvious way the classic notion of a Heffter array $H(n, k)$ to any group of order $2nk + 1$, we give direct constructions for elementary abelian Heffter arrays, hence in particular for prime Heffter arrays (whose existence was already known). If $q = 2nk + 1$ is a prime power, we say that an elementary abelian $H(n, k)$ is “over $\mathbb{F}_q$” since, for its construction, we exploit both the additive and multiplicative structure of the field of order $q$.

We show that in many cases a direct construction of a $H(n, k)$ over $\mathbb{F}_q$, say $A$, can be obtained very easily by imposing that $A$ has rank 1 and, possibly, a rich group of multipliers, that are elements $m$ of $\mathbb{F}_q$ such that $mA = A$ up to a permutation of rows and columns. A $H(n, k)$ over $\mathbb{F}_q$ will be said optimal if the order of its group of multipliers is the least common multiple of the odd parts of $n$ and $k$, since this is the maximum possible order for it.

We give an explicit direct construction of a rank-one $H(n, k)$ – reaching almost always the optimality – for all admissible pairs $(n, k)$ except for the demanding ones, i.e., those where $n$ or $k$ is a power of 2, or $nk$ has only one odd prime divisor. A less explicit construction makes reasonable to believe that an optimal rank-one $H(n, k)$ exists for any admissible pair $(n, k)$.

Keywords: Heffter array; multiplier; cyclotomy.

1 Introduction

Heffter arrays are interesting combinatorial designs introduced by Archdeacon [1] in 2015. For a rich survey on the many variations and the related results we refer to [8]. In this note we consider Heffter arrays in the original meaning of “tight” Heffter arrays extending the definition to any group of odd order as proposed in [7].

A half-set of an additive group $G$ of odd order $2\ell + 1$ is a $\ell$-subset $L$ of $G$ such that $L \cup -L = G \setminus \{0\}$, i.e., a complete set of representatives for the so-called patterned starter of $G$. A subset or multisubset $S$ of an additive abelian group $G$ will be said zero-sum if the sum of all elements of $S$ is zero. This can be extended to non-abelian groups saying that an ordered subset or multisubset $S = \{s_1, \ldots, s_n\}$ of $G$ is zero-sum if $s_1 + \ldots + s_n = 0$.

*Dipartimento di Scienze di Base e Applicate per l’Ingegneria (S.B.A.I.), Università Sapienza di Roma, Italy. Email: marco.buratti@uniroma1.it
Definition 1.1. A Heffter array $H(n, k)$ over an additive group $G$ of order $2nk + 1$ is a $n \times k$ matrix whose entries form a half-set of $G$ and whose rows and columns are all zero-sum.

A Heffter array is cyclic or elementary abelian if it is over a cyclic or elementary abelian group, respectively. If a $H(n, k)$ is elementary abelian, then $q = 2nk + 1$ is obviously a prime power and we say that the array is over $\mathbb{F}_q$, that is the field of order $q$.

The existence problem for a cyclic $H(n, k)$ has been completely solved [2]. On the other hand the solution has been obtained via recursive methods and, as far as we are aware, just a few direct constructions are known. In this note we will give direct constructions for infinitely many elementary abelian $H(n, k)$.

Thus, in particular, for infinitely many prime $H(n, k)$.

We get our constructions by imposing, first of all, that the arrays are rank-one, i.e., of rank equal to 1 in the usual sense of linear algebra. Thus, a Heffter array $H(n, k)$ over $\mathbb{F}_q$ is rank-one if its rows are all multiples of a non-zero vector of $\mathbb{F}_q^k$ (and consequently its columns are all multiples of a non-zero vector of $\mathbb{F}_q^n$).

Example 1.2. It is readily seen that the following is a rank-one $H(3, 3)$ over $\mathbb{Z}_{19}$.

$$A = \begin{pmatrix} 1 & 3 & -4 \\ 7 & 2 & -9 \\ -8 & -5 & -6 \end{pmatrix}$$

Example 1.3. Let $g$ be a root of the primitive polynomial $x^2 + x + 2$ over $\mathbb{F}_5$. Then the following is a rank-one $H(3, 4)$ over $\mathbb{F}_{25}$.

$$A = \begin{pmatrix} 1 & g & g + 4 & 3g \\ 3g + 1 & 3g + 4 & 3 & 4g + 2 \\ 2g + 3 & g + 1 & 4g + 3 & 3g + 3 \end{pmatrix}$$

In [6] Cavenagh et al. propose a definition of equivalent Heffter arrays. On the other hand, as far as we are aware, there is no “official” definition of isomorphic Heffter arrays. From the perspective of the classic design theory, we think it is natural to give the following.

Definition 1.4. An isomorphism between a Heffter array $A$ over a group $G$ and a Heffter array $A'$ over a group $G'$ is a group isomorphism $\phi$ between $G$ and $G'$ such that $\phi(A)$ or its transposal can be obtained from $A'$ by suitable permutations of its rows and columns.

Thus, in particular, an automorphism of a Heffter array $A$ over a group $G$ is an automorphism of the group $G$ mapping $A$ or $A^T$ into a matrix obtainable from $A$ itself by permuting its rows and columns.

Two Heffter arrays are isomorphic if there exists an isomorphism between them.

By saying that a Heffter array $A$ is over a ring $R$ we will mean that it is over the additive group of $R$. If $R$ is with identity and $u$ is a unit of $R$, it is clear that $A$ and $uA$ are isomorphic since the map $\tilde{u} : x \in R \rightarrow ux \in R$ is an isomorphism between them. On the other hand it is not said that $\tilde{u}$ is an automorphism of $A$. In the event this happens we will say that $u$ is a multiplier of $A$. 

2
Definition 1.5. Let $A$ be a Heffter array over a ring $R$ with identity. A multiplier of $A$ is any unit $u$ of $R$ such that $uA$ or $uA^T$ can be obtained from $A$ by suitable permutations of its rows and columns.

It is evident that if $u$ is a multiplier of a Heffter array $A$, then the set of entries of $A$ and $uA$ coincide. Thus $-1$ is never a multiplier since, by the definition of a half-set, the set of entries of $-A$ is exactly the complement of the set of entries of $A$. Note, however, that $A$ and $-A$ are equivalent in the sense of Cavenagh et al. [6].

The set $M$ of all multipliers of a Heffter array over a ring $R$ with identity clearly form a subgroup of the group $U(R)$ of units of $R$. For instance, it is easy to see that the group of multipliers of the $H(3,3)$ of Example 1.2 is $\{1, 7, 11\}$ and that the group of multipliers of the $H(3,4)$ of Example 1.3 is $\{1, 3g + 1, 2g + 3\}$.

Starting from the fundamental paper by R.M. Wilson [9] – or even from the earlier paper by R.C. Bose [3] – arriving to very recent work by the present author et al. [4] the search for difference families and all their variants (a well-know topic of design theory) has been made easier by imposing “many” multipliers. The same can be applied to rank-one Heffter arrays. Indeed most of the rank-one Heffter arrays constructed in this paper have a non-trivial group of multipliers.

Throughout the paper, saying that a pair $(n,k)$ is admissible we mean that $2nk + 1$ is a prime power and that both $n$ and $k$ are greater than 2. Also, speaking of “a rank-one Heffter array $H(n,k)$” it will be understood that $(n,k)$ is admissible and that the array is over $F_{2nk+1}$.

We will need to distinguish admissible pairs of two types that we define “agreeable” and “demanding”.

We say that an admissible pair $(n,k)$ is agreeable if there exist two distinct odd primes $p$ and $p'$ dividing $n$ and $k$, respectively. We say that it is demanding in the opposite case. Equivalently, $(n,k)$ is demanding when $n$ or $k$ (possibly both) is a power of 2 or $nk$ has only one odd prime factor.

The reason of the above terminology lies in the fact that we are able to give an explicit construction of a rank-one $H(n,k)$ for any agreeable pair $(n,k)$. The construction requires some computer work if $(n,k)$ is demanding.

The paper will be organized as follows.

In the next section we will give some very elementary prerequisites that are necessary to understand the paper.

In Section 3 it is proved that the existence of a rank-one $H(n,k)$ is completely equivalent to a factorization of a half-set of $F_{2nk+1}$ into the product $X \cdot Y$ of a zero-sum $n$-set $X$ by a zero-sum $k$-set $Y$. As a corollary we get the easiest and nicest construction of a rank-one $H(n,k)$: if $(n,k)$ is admissible with $n$, $k$ odd and coprime, then the $n \times k$ array $[r^{2ki+2nj}]$ where $r$ is a primitive element of $F_{2nk+1}$, is a rank-one $H(n,k)$ whose multipliers are the non-zero squares of $F_{2nk+1}$.

In Section 4 we prove that the order $\mu$ of the group of multipliers of a rank-one $H(n,k)$ is at most equal to the least common multiple of the odd parts of $n$ and $k$. So we say that a rank-one $H(n,k)$ is optimal when $\mu$ reaches this value. In particular, we say that it is perfect when $\mu = nk$. The perfect rank-one Heffter arrays are precisely the “easiest and nicest” obtained in Section 2.

In Section 5, using cyclotomy, we give an explicit construction of a rank-one $H(n,k)$ for every admissible agreeable pair $(n,k)$. We also prove that this
construction reaches optimality unless \( n \) and \( k \) have the same radical \( r \) and either \( \frac{n}{r} \) or \( \frac{k}{r} \) is an integer.

In Section 6 we provide another construction method which is less explicit but gives a very strong indication on the existence of a rank-one \( H(n, k) \) also for \((n, k)\) demanding.

In Section 7, we are able to give an explicit construction of a rank-one \( H(n, k) \) for all the (known) demanding pairs of the form \((2^\alpha, 2^\beta)\).

In the last section we strongly conjecture that a rank-one \( H(n, k) \) exists for all the admissible pairs \((n, k)\) and we are able to prove that it is true whenever \( 2nk + 1 < 10^6 \).

2 Preliminaries

We will need some elementary facts about cyclotomy and the related standard notation/terminology. Given a prime power \( q = de + 1 \), the multiplicative group of \( \mathbb{F}_q \) will be denoted by \( \mathbb{F}_q^* \) and the subgroup of \( \mathbb{F}_q^* \) of index \( e \) or, equivalently, the subgroup of \( \mathbb{F}_q^* \) of order \( d \) will be denoted by \( C_e \). If \( r \) is a primitive element of \( \mathbb{F}_q^* \), then the set of cosets of \( C_e \) in \( \mathbb{F}_q^* \) (the so-called cyclotomic classes of index \( e \)) is \( \{r^iC_e \mid 0 \leq i \leq e-1\} \). It will be always understood that \( r \) is fixed and, as it is standard, the coset \( r^iC_e \) will be denoted by \( C_e^i \) whichever is \( i \).

Note that we have \( C_e^i = C_e^j \) if and only if \( i \equiv j \pmod{e} \) and that \( C_e^i \cdot C_e^j = C_e^{i+j} \). Anyone who has a little bit of familiarity with finite fields should know the elementary facts below that we recall for convenience.

**Lemma 2.1.** Let \( q \) be a prime power. Then we have:

(i) Every union of cosets of a non-trivial subgroup of \( \mathbb{F}_q^* \) is zero-sum.

(ii) If \( q = 2d + 1 \) with \( d \) odd, then \( -1 \in C_2^e \) so that \( C_2^e \cup C_2^{2e} \cup \ldots \cup C_2^{(e-1)e} \) is a half-set of \( \mathbb{F}_q^* \).

In particular, if \( q = 2d + 1 \) with \( d \) odd, then \( -1 \in C_2^e \) and \( C_2^e \) is a half-set of \( \mathbb{F}_q^* \).

(iii) the product of two subgroups of \( \mathbb{F}_q^* \) of orders \( s \) and \( t \), is the subgroup of \( \mathbb{F}_q^* \) of order \( \text{lcm}(s, t) \).

We also need the following.

**Proposition 2.2.** Let \( q = de + 1 \) be a prime power and let \( X \) be a subset of \( \mathbb{F}_q^* \). Then the stabilizer of \( X \) under the natural action of \( \mathbb{F}_q^* \) is divisible by \( d \) if and only if \( X \) is a union of cosets of \( C_e \).

**Proof.** The “if part” is obvious. Let us prove the “only if” part. Let \( S \) be the \( \mathbb{F}_q^* \)-stabilizer of \( X \) and assume that its order is divisible by \( d \). Then \( S \) contains the subgroup of \( \mathbb{F}_q^* \) of order \( d \), that is \( C_e \). Thus it makes sense to consider the action of \( C_e \) on \( X \). The orbits of this action partition \( X \) and each of them is of the form \( xC_e \) for some \( x \in X \), that is a coset of \( C_e \) in \( \mathbb{F}_q^* \). The assertion follows. \( \square \)
3 Characterization

One says that a subset $S$ of an additive (resp. multiplicative) group $G$, can be factorized into the product $X \cdot Y$ (resp. sum $X + Y$) of two subsets $X, Y$ of $S$ if every element of $S$ can be written in exactly one way as $x + y$ (resp. $x \cdot y$) with $x \in X$ and $y \in Y$. One also says that $X + Y$ (resp. $X \cdot Y$) is a factorization of $S$. By saying that $X$ is a factor of $S$ one means that $X$ is a subset of $S$ for which there exists another subset $Y$ of $S$ such that $S = X + Y$ (resp. $S = X \cdot Y$). In other words, $X$ is a factor of $S$ if it is possible to "tile" $S$ with suitable translates of $X$.

The group $G$ could be also infinite. For instance, if $G = (\mathbb{Z}, +)$ and $S = \{s \in \mathbb{Z} : 0 \leq s \leq 15\}$, then one can check that the factors of $S$ of size four are

$$X_1 = \{0, 1, 2, 3\}, \quad X_2 = \{0, 1, 4, 5\}, \quad X_3 = \{0, 1, 8, 9\},$$

$$X_4 = \{0, 2, 4, 6\}, \quad X_5 = \{0, 2, 8, 10\}, \quad X_6 = \{0, 4, 8, 12\}$$

and that we have $S = X_i + X_{7-i}$ for $1 \leq i \leq 6$.

We are going to show that the rank-one Heffter arrays can be characterized in terms of factorizations of a half-set of a finite field.

**Proposition 3.1.** Let $q = 2nk + 1$ be a prime power. There exists a rank-one $H(n,k)$ if and only if there is a suitable half-set of $\mathbb{F}_q$ admitting a factorization into the product of two zero-sum subsets of $\mathbb{F}_q^*$ of sizes $n$ and $k$.

**Proof.** ($\Rightarrow$). If $A$ is a rank-one $H(n,k)$ over $\mathbb{F}_q$, then all columns of $A$ are multiples of a vector $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$. Thus, if $A^j$ is the $j$-th column of $A$, there is a suitable $y_j \in \mathbb{F}_q$ such that $A^j = (x_1, \ldots, x_n) \cdot y_j$ for $1 \leq j \leq n$. It follows that $a_{i,j} = x_i y_j$. Hence the set of all entries of $A$, which is a half-set of $(\mathbb{F}_q, +)$ by definition of a Heffter array, coincides with the product of the two sets $X = \{x_1, \ldots, x_n\}$ and $Y = \{y_1, \ldots, y_k\}$.

($\Leftarrow$). Let $V$ be a half-set of $\mathbb{F}_q$ and assume that $V = X \cdot Y$ where $X = \{x_1, \ldots, x_n\}$ and $Y = \{y_1, \ldots, y_k\}$ are zero-sum subsets of $\mathbb{F}_q^*$ of sizes $n$ and $k$, respectively. Consider the $n \times k$ array $A$ over $\mathbb{F}_q$ defined by $a_{i,j} = x_i y_j$ for $1 \leq i \leq n$ and $1 \leq j \leq k$. It is obvious that the entries of $A$ are precisely the elements of $V$, hence they form a half-set of $(\mathbb{F}_q, +)$. Note that the $i$-th row of $A$ is $(x_1 \cdot y_i, \ldots, x_n \cdot y_i)$ and that the $j$-th column of $A$ is $(x_1 \cdot y_j, \ldots, x_n \cdot y_j)$. Thus, given that both $X$ and $Y$ are zero-sum, we infer that all rows and columns of $A$ are also zero-sum. We conclude that $A$ is a rank-one $H(n,k)$.

We will briefly refer to the sets $X$ and $Y$ in the above proof as the factors of the Heffter array $A$.

The next result is just a special case of the more general Theorem 5.1 that we will see later. On the other hand we think it is appropriate to give its statement now and separately, since it is an almost immediate consequence of Proposition 3.1. Actually, this is the easiest and nicest construction of a rank-one Heffter array.

**Corollary 3.2.** If $(n, k)$ is an admissible pair with $n, k$ odd and coprime, then $C^{2k}$ and $C^{2n}$ are the factors of a rank-one $H(n,k)$.

**Proof.** By assumption, $q = 2nk + 1$ is a prime power. The set $X = C^{2k}$ and $Y = C^{2n}$ are the subgroups of $\mathbb{F}_q^*$ of orders $n$ and $k$, respectively. They are
zero-sum by Lemma 2.1(i). Also, their product is the subgroup of \(F_q^\ast\) of order \(nk\) by Lemma 2.1(iii), i.e., the group \(C^2\) of non-zero squares of \(F_q\) which is a half-set by Lemma 2.1(ii). The assertion then follows from Proposition 3.1. □

The above gives, in particular, infinitely many Heffter arrays which are elementary abelian but not prime. For instance, we have \(7^3 = 2 \cdot 9 \cdot 19 + 1\) and hence, applying Corollary 3.2 with \(n = 9\) and \(k = 19\), we get a H(9, 19) over \(F_7\).

We will see that the group of multipliers of a H(n, k) obtainable via Corollary 3.2 is \(C^2\), i.e., the group of non-zero squares of \(F_{2nk+1}\).

**Example 3.3.** Let us construct a rank-one H(3, 5). The request makes sense since \(q = 2 \cdot 3 \cdot 5 + 1 = 31\) is a prime. Note that \(x = 5\) is a cubic root of unity (mod 31) and that \(y = 2\) is a 5th root of unity (mod 31). Thus \(X = \{x\} = \{1, 5, 25\}\) is the subgroup of \(F^\ast_{31}\) of order 3 and \(Y = \{y\} = \{1, 2, 4, 8, 16\}\) is the subgroup of \(F^\ast_{31}\) of order 5. The desired rank-one H(3, 5) is therefore

\[
A = \begin{pmatrix} 1 & 2 & 4 & 8 & 16 \\ 5 & 10 & 20 & 9 & 18 \\ 25 & 19 & 7 & 14 & 28 \end{pmatrix}
\]

Note that multiplying \(A\) by 9 (which is a generator of the squares of \(F_{31}\)) corresponds to permuting its rows cyclically \(R_i \to R_{i+1} \mod 3\) and then to permute the columns cyclically \(C_j \to C_{j+3} \mod 5\). This implies that the non-zero squares of \(F_{31}\) form a group of multipliers of the above array.

4 Multipliers of a rank-one Heffter array

From now on, given any integer \(n\) we denote by \(n_o\) the odd part of \(n\), that is the greatest odd divisor of \(n\).

**Proposition 4.1.** Let \(A\) be a rank-one H(n, k) over \(F_q\) with factors X and Y. Then the group of multipliers of \(A\) is the product of the \(F^\ast_q\)-stabilizers of \(X\) and \(Y\). Also, its order is at most equal to lcm\((n_o, k_o)\).

**Proof.** Set \(X = \{x_1, \ldots, x_n\}\) and \(Y = \{y_1, \ldots, y_k\}\) so that we have \(a_{i,j} = x_i y_j\) for \(1 \leq i \leq n, 1 \leq j \leq k\). We have to prove that the group \(M\) of multipliers of \(A\) is the product \(S \cdot T\) where \(S\) and \(T\) are the \(F^\ast_q\)-stabilizers of \(X\) and \(Y\), respectively. In the following, \(A_i\) and \(A_j\) will denote the \(i\)-th row of \(A\) and the set of its elements, respectively. Analogously, \(A^j\) and \(A^j\) will denote the \(j\)-th column of \(A\) and the set of its elements, respectively.

If \(s \in S\), then \(s(x_1, \ldots, x_n) = (x_{\pi(1)}, \ldots, x_{\pi(n)})\) for a suitable permutation \(\pi\) on the set \(\{1, \ldots, n\}\). It easily follows that \(sA\) is the matrix whose \(j\)-th column is \(A_{\pi(j)}\) for \(1 \leq j \leq n\), hence a matrix obtainable from \(A\) by permuting its columns. Thus, by definition, \(s\) is a multiplier of \(A\).

Analogously, if \(t \in T\), then \(t(y_1, \ldots, y_k) = (y_{\psi(1)}, \ldots, y_{\psi(k)})\) for a suitable permutation \(\psi\) on the set \(\{1, \ldots, k\}\). It follows that \(tA\) is the matrix whose \(i\)-th row is \(A_{\psi(i)}\) for \(1 \leq i \leq k\), hence a matrix obtainable from \(A\) by permuting its rows and then \(t\) is a multiplier of \(A\).

Thus \(M\) contains both \(S\) and \(T\), hence it contains their product \(S \cdot T\).
Now we prove the inverse inclusion. Let \( m \in M \). By definition of a multiplier, there is a suitable pair \((i, j)\) such that either

1. \( mA_1 \) is a permutation of \( A_i \) and \( mA^1 \) is a permutation of \( A^j \);

or

2. \( mA_1 \) is a permutation of \( A^j \) and \( mA^1 \) is a permutation of \( A_i \).

Of course (2) may happen only in the case \( n = k \).

Assume that (1) holds. It follows, in particular, that \( ma_{1,1} = mx_1y_1 \) must be the common element of \( A_i \) and \( A_j \), that is \( a_{i,j} = x_1y_j \). Thus we have

\[
m = x_iy_jx_1^{-1}y_1^{-1} \quad (4.1)
\]

For \( 1 \leq i \leq n \), we have \( A_i = (x_1y_1, x_2y_1, \ldots, x_1y_k) \), hence \( \overline{A_i} = x_iY \). Analogously, for \( 1 \leq j \leq k \), we have \( A^j = (x_1y_j, x_2y_j, \ldots, x_ny_j) \), hence \( \overline{A^j} = XY_j \). In particular, we have \( \overline{A_1} = x_1Y \) and \( \overline{A^1} = Xy_1 \).

The fact that \( mA_1 \) is a permutation of \( A_i \) implies that \( m \overline{A_1} = \overline{A_i} \), i.e., \( mx_iY = x_iY \). Analogously, the fact that \( mA^1 \) is a permutation of \( A^j \) implies that \( m \overline{A^1} = \overline{A^j} \), i.e., \( mx_1Y = x_1Y \). Thus, using (4.1), we get \( y_jy_1^{-1}Y = Y \) and \( x_iy_1^{-1}X = X \). This means that \( y_jy_1^{-1} \) stabilizes \( Y \) and \( x_iy_1^{-1} \) stabilizes \( X \), i.e., \( y_jy_1^{-1} \in T \) and \( x_iy_1^{-1} \in S \). The conclusion is that \( m = (x_iy_1^{-1})(y_jy_1^{-1}) \in S \cdot T \).

If \( n = k \) and (2) holds, reasoning in a very similar way one finds that \( m \in S \cap T \), hence \( m \) is the unity.

By Proposition 2.2, the order of \( S \) is a divisor of \( |X| = n \). Remember, however, that \(-1\) cannot be a multiplier so that \(-1 \not\in S \) which means that \( S \) has odd order. Hence \( |S| \) is a divisor of \( n_o \) and then \( S \) is a subgroup of the group \( N_o \) of the \( n_o \)-th roots of unity. Reasoning exactly in the same way, one can see that \( T \) is a subgroup of the group \( K_o \) of the \( k_o \)-th roots of unity. Thus \( M = S \cdot T \) is a subgroup of \( N_o \cdot K_o \). We get the assertion observing that the order of \( N_o \cdot K_o \) is \( \text{lcm}(n_o, k_o) \) (see Lemma 2.1(iii)).

The above suggests the following definition.

**Definition 4.2.** A rank-one \( H(n, k) \) is optimal if the order of its group of multipliers is the least common multiple of the odd parts of \( n \) and \( k \). It is perfect if it has order \( nk \), i.e., it is the group \( C^2 \) of non-zero squares of \( \mathbb{F}_{2nk+1} \).

The perfect rank-one \( H(n, k) \) can be completely characterized in view of Corollary 3.2.

**Proposition 4.3.** There exists a perfect rank-one \( H(n, k) \) if and only if \((n, k)\) is an admissible pair with \( n, k \) odd and coprime.

**Proof.** Let \( A \) be a perfect rank-one \( H(n, k) \) and let \( M \) be its group of multipliers. By definition, we have \( |M| = nk \) but we also have \( |M| \leq \text{lcm}(n_o, k_o) \) by Proposition 4.1. Thus, considering that \( \text{lcm}(n_o, k_o) \) is a divisor of \( nk \), we necessarily have \( \text{lcm}(n_o, k_o) = nk \). Clearly, this is possible only if \( n \) and \( k \) are odd and coprime.

Now let \((n, k)\) be an admissible pair with \( n, k \) odd and coprime. By Corollary 3.2 there exists a rank-one \( H(n, k) \) whose factors are the group \( X \) of \( n \)-th roots of unity and the group \( Y \) of \( k \)-th roots of unity. Their \( \mathbb{F}_q^* \)-stabilizers are \( X \) and \( Y \), respectively (see Proposition 2.2). So the group of multipliers is \( X \cdot Y \) whose order is \( nk \) by Lemma 2.1(iii).

\footnote{If \( m \) fixes both \( X \) and \( Y \) then we have \( mx_1 = x_1 \) and \( my_j = y_j \) for a suitable pair \((i, j)\). It follows that \( m(x_1y_1 = x_1y_1 = x_1y_j \) which implies \( i = j = 1 \), hence \( m = 1 \).}
5 Rank-one Heffter arrays with \((n, k)\) agreeable

In this section we first give an explicit construction of a rank-one \(H(n, k)\) for any admissible agreeable pair \((n, k)\). Then we discuss its possible optimality.

**Theorem 5.1.** If \(q = 2nk + 1\) is a prime power with \((n, k)\) agreeable, then there exists a rank-one \(H(n, k)\) over \(\mathbb{F}_q\).

**Proof.** Take any pair \((n_1, k_1)\) of odd coprime integers greater than 1 with \(n_1\) dividing \(n_o\) and \(k_1\) dividing \(k_o\). Such a pair certainly exists by definition of an agreeable pair; in the worst of the cases \(n_1\) and \(k_1\) may be suitable odd primes.

Set \(n = n_1n_2\), \(k = k_1k_2\) and consider the following subsets of \(\mathbb{F}_q^*\):

\[
X = \bigcup_{i=0}^{n_2-1} C_{i+1}^{2n_2k_2} \quad \text{and} \quad Y = \bigcup_{j=0}^{k_2-1} C_{j+1}^{2nk_2}.
\]

We have \(2n_2k = \frac{q-1}{n_1}\), hence \(C_{i+1}^{2n_2k_2}\) is a subgroup of \(\mathbb{F}_q^*\) of order \(n_1\). So we see that \(X\) is a union of \(n_2\) cosets of this subgroup, hence a \(n\)-subset of \(\mathbb{F}_q^*\) which is zero-sum by Lemma 2.1(i). Analogously, we have \(2nk_2 = \frac{q-1}{k_1}\), hence \(C_{j+1}^{2n_2k_2}\) is the subgroup of \(\mathbb{F}_q^*\) of order \(k_1\). Thus \(Y\) is a union of \(k_2\) cosets of this subgroup, hence a \(k\)-subset of \(\mathbb{F}_q^*\) which is zero-sum by Lemma 2.1(i).

Given that \(\gcd(n_1, k_1) = 1\), by Lemma 2.1(iii) the product of the subgroups of \(\mathbb{F}_q^*\) of orders \(n_1\) and \(k_1\) is the subgroup of \(\mathbb{F}_q^*\) of order \(n_1k_1\):  

\[
C_{i+1}^{2n_2k_2} \cdot C_{j+1}^{2nk_2} = C_{i+j}^{2nk_2}.
\]

It follows that

\[
C_{i+1}^{2n_2k_2} \cdot C_{j+1}^{2nk_2} = C_{i+j}^{2nk_2}
\]

and then we can write:

\[
X \cdot Y = \bigcup_{(i, j) \in I \times J} C_{i+j}^{2nk_2}
\]

with \(I = \{0, 1, \ldots, n_2 - 1\}\) and \(J = \{0, n_2, 2n_2, \ldots, (k_2 - 1)n_2\}\). Now note that \(I + J\) is a factorization of the whole interval \([0, n_2k_2 - 1]\). Thus, setting \(e = n_2k_2\), we can write

\[
X \cdot Y = C_0^{2e} \cup C_1^{2e} \cup \ldots \cup C_{e-1}^{2e}.
\]

It follows, by Lemma 2.1(ii), that \(X \cdot Y\) is a half-set of \(\mathbb{F}_q\). Using the “if part” of Proposition 5.1 we can finally say that the \(n \times k\) array \([x_i, y_j]\) is a rank-one \(H(n, k)\).

**Example 5.2.** Let us construct a rank-one \(H(6, 15)\). The pair \((6, 15)\) is agreeable. Indeed \(q = 2 \cdot 6 \cdot 15 + 1 = 181\) is a prime and \(n_1 = 3, k_1 = 5\) are distinct primes dividing \(n_o\) and \(k_o\), respectively. Using \(r = 2\) as primitive element of \(\mathbb{F}_{97}\) and following the instructions of Theorem 5.1 we find that the factors of a rank-one \(H(6, 15)\) are

\[
X = C_0^{60} \cup C_1^{60} = \{1, 48, 132, 2, 96, 83\} \quad \text{and}
\]

\[
Y = C_0^{36} \cup C_2^{36} \cup C_4^{36} = \{1, 59, 42, 125, 135, 4, 55, 168, 138, 178, 16, 39, 129, 9, 169\}.
\]
Therefore the desired $H(6, 15)$ is the following

\[
\begin{pmatrix}
1 & 59 & 42 & 125 & 135 & 4 & 55 & 168 & 138 & 178 & 16 & 39 & 129 & 9 & 169 \\
48 & 117 & 25 & 27 & 145 & 11 & 106 & 100 & 108 & 37 & 44 & 62 & 38 & 70 & 148 \\
132 & 5 & 114 & 29 & 82 & 166 & 20 & 94 & 116 & 147 & 121 & 80 & 14 & 102 & 45 \\
2 & 118 & 84 & 69 & 89 & 8 & 110 & 155 & 95 & 175 & 32 & 78 & 77 & 18 & 157 \\
96 & 53 & 50 & 54 & 109 & 22 & 31 & 19 & 35 & 74 & 88 & 124 & 76 & 140 & 115 \\
83 & 10 & 47 & 58 & 164 & 151 & 40 & 7 & 51 & 113 & 61 & 160 & 28 & 23 & 90
\end{pmatrix}
\]

We recall that the radical of an integer $n$, denoted by $rad(n)$, is the product of the individual prime factors of $n$ if $n > 1$, and it is equal to 1 if $n = 1$. We give the following definition.

**Definition 5.3.** A pair $(n, k)$ is optimal if it is agreeable and neither $n_o \cdot rad(n_o)$ divides $k_o$ nor $k_o \cdot rad(k_o)$ divides $n_o$.

We want to exploit the proof of Theorem 4.1 in the best possible way in order to establish whether it may leads to an optimal rank-one Heffter array.

**Theorem 5.4.** If an admissible pair $(n, k)$ is optimal, then there exists an optimal rank-one $H(n, k)$.

**Proof.** Let $A$ be the rank-one $H(n, k)$ constructed in Theorem 5.1 let $X, Y$ be its factors and let $S, T$ be their respective $P_q$-stabilizers. Recall that $X$ is a union of cosets of the $n_1$-th roots of unity and that $Y$ is a union of cosets of the $k_1$-th roots of unity. Then, by Proposition 2.2 the orders of $S$ and $T$ are divisible by $n_1$ and $k_1$, respectively. Recalling that the group of multipliers of $A$ is $S \cdot T$ by Proposition 4.1, we deduce that its order is at least equal to $n_1k_1$.

Thus, to prove the assertion it is enough to show that $lcm(n_o, k_o)$ can be written as a product $n_1k_1$ with $n_1 > 1$ a divisor of $n_o$, $k_1 > 1$ a divisor of $k_o$, and $gcd(n_1, k_1) = 1$.

Consider first the case $n_o = k_o$. Here, to say that $(n, k)$ is optimal simply means that $n_o$ has at least two distinct prime factors. Let $p$ be one of them and let $p^a$ be the largest power of $p$ dividing $n_o$. Then $n_1 = p^a$ and $k_1 = \frac{n_o}{p^a}$ satisfy the requirement.

Now assume that $n_o < k_o$. Let $\{p_1, \ldots, p_t\}$ be the set of prime divisors of $n_o k_o$, let $p_i^{\alpha_i}$ be the largest power of $p_i$ dividing $n_o$, and let $p_j^{\beta_j}$ be the largest power of $p_j$ dividing $k_o$. Now let $I$ be the set of $i$’s such that $\alpha_i \geq \beta_j$ and let $J$ be the complement of $I$ in $\{1, \ldots, t\}$, i.e., the set of $j$’s such that $\alpha_j < \beta_j$. It is obvious that $lcm(n_o, k_o) = \prod_{i=1}^{t} p_i^{\max(\alpha_i, \beta_j)}$, hence we can write $lcm(n_o, k_o)$ as a product of a divisor $n_1$ of $n_o$ and a divisor $k_1$ of $k_o$ as follows

\[
lcm(n, k) = n_1k_1 \text{ with } n_1 = \prod_{i \in I} p_i^{\alpha_i} \text{ and } k_1 = \prod_{j \in J} p_j^{\beta_j}.
\]

It is also obvious that $n_1$ and $k_1$ are coprime. It remains to show that $n_1$ and $k_1$ are both greater than 1. Indeed, if $n_1 = 1$, then $I$ would be empty which means that, for every $h$, the exponent of $p_h$ in the prime factorization of $n_o$ is strictly less than the exponent of $p_h$ in the prime factorization of $k_o$. This clearly implies that $n_o \cdot rad(n_o)$ is a divisor of $k_o$, contradicting that $(n, k)$ is optimal. Also, if $k_1 = 1$ then $J$ would be empty which means that, for every $h$, the exponent of $p_h$ in the prime factorization of $n_o$ is greater than or equal to the exponent of $p_h$ in the prime factorization of $k_o$. This would imply that $n_o \geq k_o$ against the assumption. We conclude that $n_1$, $k_1$ satisfy the requirement.

The remaining case $n_o > k_o$ can be proved exactly in the same way by inverting the roles of $n_o$ and $k_o$. \qed
Note that the agreeable pairs which are not optimal are, up to the order, of the form \((2^\alpha \nu \rho, 2^\beta \nu)\) where \(\nu, \rho\) are odd integers such that \(\nu\) has at least two distinct prime divisors and \(\text{rad}(\rho) = \text{rad}(\nu)\). The least admissible pair which is agreeable but not optimal is \((21^2, 21)\). Indeed the pair \((15^2, 15)\) is not admissible since we have \(2 \cdot 15^3 + 1 = 43 \cdot 157\).

6 Rank-one Heffter arrays with \((n, k)\) demanding

Obviously, if a pair \((n, k)\) is admissible, then \((k, n)\) is admissible as well. So, from now on, speaking of an admissible pair \((n, k)\) we can assume without loss of generality that \(n_o \geq k_o\). With this agreement a demanding pair has one the following forms:

1. \((2^\alpha, 2^\beta)\);
2. \((2^\alpha d, 2^\beta)\) with \(d > 1\) odd;
3. \((2^\alpha p^a, 2^\beta p^b)\) with \(p\) an odd prime and \(a \geq b > 0\).

The demanding pairs of form (1) will be said Fermat pairs since their related \(q = 2^{\alpha+\beta+1} + 1\) is necessarily a Fermat prime, i.e., a prime of the form \(F_i := 2^{2^i} + 1\). The pairs of form (2) or (3) will be said non-Fermat demanding pairs.

Note that we have \(\text{lcm}(n_o, k_o) = n_o\) for any admissible pair \((n, k)\) which is either demanding or agreeable but not optimal.

From now on, given a prime power \(q = 2nk + 1\), speaking of a half-set of \(C_k\) we will mean a complete system of representatives for the cosets of \(\{1, -1\}\) in \(C_k\), hence a subset \(X\) of \(\mathbb{F}_q^*\) such that \(\{1, -1\} \cdot X = C_k^*\). The following construction can be applied for both agreeable and demanding pairs \((n, k)\). On the other hand, we will need it only for demanding pairs in view of Theorem 5.1.

**Lemma 6.1.** Let \(q = 2nk + 1\) be a prime power such that there exist a zero-sum half-set \(X\) of \(C_k^*\), and a zero-sum complete system of representatives \(Y\) for the cosets of \(C_k^*\) in \(\mathbb{F}_q^*\). Then there exists a rank-one \(H(n, k)\).

**Proof.** Note that \(X\) is a zero-sum \(n\)-subset of \(\mathbb{F}_q^*\) such that \(\{1, -1\} \cdot X = C_k^*\) and that \(Y\) is a \(k\)-subset of \(\mathbb{F}_q^*\) such that \(C_k^* \cdot Y = \mathbb{F}_q^*\). Thus we have

\[
\{1, -1\} \cdot (X \cdot Y) = (\{1, -1\} \cdot X) \cdot Y = C_k^* \cdot Y = \mathbb{F}_q^*
\]

which means that \(X \cdot Y\) is a half-set of \(\mathbb{F}_q\). The assertion then follows from Proposition 3.1. \(\square\)

**Example 6.2.** Let us construct an optimal rank-one \(H(16, 3)\) over \(\mathbb{F}_{97}\). One can check that

\[X = \{1, 28, 8, 30, 64, 46, 27, 77, 22, 34, 18, 78, 50, 42, 12, 45\}\]

is a zero-sum half-set of \(C_3^*\) and that the group of cubic roots of unity, that is \(Y = \{1, 35, 61\}\), is a complete system of representatives for the cosets of \(C_3^*\) in \(\mathbb{F}_{97}^*\).
We note that it is optimal since the stabilizer of $Y$ is $Y$ itself.

For each demanding pair $(n, k)$ whose related $q$ does not exceed 101, we report the factors of an optimal rank-one $H(n, k)$ that we have found by computer using Lemma 6.1. The table below records the cases where $q$ is a prime (for $(n, k) = (3, 3)$ where $q = 19$ see Example 1.2) for $(n, k) = (3, 16)$ where $q = 97$ see Example 6.2. The multipliers are reported in boldface.

| $n$ | $k$ | $q$ | $X$          | $Y$          |
|-----|-----|-----|--------------|--------------|
| 3   | 6   | 37  | $\{1, 10, 26\}$ | $\{1, 2, 4, 12, 23, 32\}$ |
| 5   | 4   | 41  | $\{1, 10, 18, 16, 37\}$ | $\{1, 27, 2, 11\}$ |
| 3   | 12  | 73  | $\{1, 8, 64\}$ | $\{1, 5, 25, 52, 41, 59, 3, 15, 2, 10, 50, 29\}$ |
| 9   | 4   | 73  | $\{1, 2, 4, 8, 16, 32, 64, 55, 37\}$ | $\{1, 5, 25, 42\}$ |
| 6   | 6   | 73  | $\{1, 8, 64, 3, 24, 46\}$ | $\{1, 5, 25, 52, 50, 13\}$ |
| 11  | 4   | 89  | $\{1, 64, 2, 39, 4, 78, 8, 67, 16, 45, 32\}$ | $\{1, 3, 9, 76\}$ |
| 12  | 4   | 97  | $\{1, 35, 61, 43, 50, 4, 6, 16, 75, 64, 9, 24\}$ | $\{1, 56, 12, 28\}$ |
| 6   | 8   | 97  | $\{1, 35, 61, 6, 16, 75\}$ | $\{1, 5, 25, 28, 43, 21, 86, 82\}$ |
| 5   | 10  | 101 | $\{1, 95, 36, 87, 84\}$ | $\{1, 89, 43, 53, 16, 32, 64, 27, 54, 7\}$ |

Now let us show the computer results obtained for demanding pairs $(n, k)$ with $2nk + 1 \leq 101$ a perfect power (for the case $(n, k) = (3, 4)$ over $\mathbb{F}_{25}$ see Example 1.3). We have to consider the cases $(n, k) \in \{(6, 4), (3, 8)\}$ over $\mathbb{F}_{49}$ and the cases $(n, k) \in \{(10, 4), (5, 8)\}$ over $\mathbb{F}_{81}$.

Let $q$ be a root of the primitive polynomial $z^4 + z + 3$ over $\mathbb{F}_7$. Then the factors of an optimal rank-one $H(6, 4)$ over $\mathbb{F}_{49}$ are the following:

$$X = \{1, 2, 4, g + 4, 2g + 1, 4g + 2\}; \quad Y = \{1, g, 5g, 2 + g\}.$$

Also, the factors of an optimal rank-one $H(3, 8)$ over $\mathbb{F}_{49}$ are the following:

$$X = \{1, 2, 4\}; \quad Y = \{1, 2g, 1 + 5g, 5 + 6g, 5 + 3g, 6 + g, 4 + 5g, 6 + 6g\}.$$

Now let $g$ be a root of the primitive polynomial $z^4 + z + 2$ over $\mathbb{F}_3$ and, to save space, let us write each element $a + bg + cg^2 + dg^3$ of $\mathbb{F}_{81}$ in the form $abcd$. Then the factors of an optimal rank-one $H(5, 8)$ over $\mathbb{F}_{81}$ are the following:

$$X = \{1000, 2102, 2021, 2220, 2020\};$$

$$Y = \{1000, 1102, 2012, 0212, 1200, 0120, 0012, 2101\}.$$
Also, the factors of an optimal rank-one $H(10,4)$ over $\mathbb{F}_8$ are the following:

$$X = \{1000, 2102, 2021, 2220, 2020, 1200, 1002, 0122, 1212, 1222\};$$

$$Y = \{1000, 2112, 0220, 0001\}.$$

Let us investigate if there are conditions assuring the existence of the first ingredient $X$ requested by Lemma 6.1.

**Lemma 6.3.** Let $q = 2nk + 1$ be a prime power and let $e$ be a divisor of $n$. If there exists a zero-sum half-set of $C^{ek}$, then there exists a zero-sum half-set of $C^k$.

**Proof.** Let $S$ be a zero-sum half-set of $C^{ek}$ so that we have $\{1, -1\} \cdot S = C^{ek}$. Take any complete system $T$ of representatives for the cosets of $C^{ek}$ in $C^k$ so that $C^{ek} \cdot T = C^k$. We claim that $X = S \cdot T$ is a zero-sum half-set of $C^k$. Indeed we have

$$\{1, -1\} \cdot X = (\{1, -1\} \cdot S) \cdot T = C^{ek} \cdot T = C^k$$

which means that $X$ is a half-set of $C^k$. Also, we have

$$\sum_{x \in X} x = \sum_{t \in T} (t \cdot \sum_{s \in S} s) = 0$$

because $\sum_{s \in S} s = 0$ by assumption on $S$. \qed

The above lemma allows to see that the first ingredient $X$ requested by Lemma 6.1 is certainly available when $n_o \neq 1$, i.e., $n$ is not a power of 2.

**Corollary 6.4.** Let $(n, k)$ be admissible with $n_o \neq 1$ and let $q = 2nk + 1$. Then there exists a zero-sum half-set of $C^k$ whose $\mathbb{F}_q^*$-stabilizer has order divisible by $n_o$.

**Proof.** Set $n = n_o e$ and consider the group $C^{2ek}$ of $n_o$-th roots of unity. Note that $\{1, -1\} \cdot C^{2ek}$ has order $2n_o$ by Lemma 2.1(iii), i.e., we have $\{1, -1\} \cdot C^{2ek} = C^{ek}$. This means that $S = C^{2ek}$ is a half-set of $C^{ek}$. Also, $C^{2ek}$ is zero-sum by Lemma 2.1(i). Then, following the proof of Lemma 6.3 we find a zero-sum half-set $X$ of $C^k$ of the form $C^{2ek} \cdot T$ with $T$ a complete system of representatives for the cosets of $C^{ek}$ in $C^k$. Such a half-set $X$ is clearly stabilized by $C^{2ek}$ and the assertion follows. \qed

It is easy to see that the second ingredient $Y$ requested by Lemma 6.1 is available if there is an odd prime divisor $p$ of $k$ which does not divide $2n$. On the other hand, we are now focused only on demanding pairs $(n, k)$ of the forms (1), (2), (3) listed at the beginning of this section. For these pairs, a prime $p$ as above does not exist.

By the way, the second ingredient $Y$ requested by Lemma 6.1 is certainly available for $k \leq \sqrt{2n}$. To prove this, we need an application of the theorem of Weil on multiplicative character sums, that is Theorem 2.2 in [5]. The reader can easily see that specializing that theorem to the case where $t$ (one of the parameters in the statement) is equal to 2, then one gets the following.

**Lemma 6.5.** Let $q \equiv 1 \pmod{e}$ be a prime power with $q > e^4$, let $i$ be any integer in the interval $[0, e - 1]$, and let $s$ be any non-zero element of $\mathbb{F}_q$. Then the set $Z = \{z \in C_0^i : z + s \in C_1^i\}$ is not empty.
This lemma allows to get the following.

**Lemma 6.6.** Let \( q = 2nk + 1 \) be a prime power with \( 2 < k \leq \sqrt{2n} \). Then there exists a zero-sum complete system of representatives for the cosets of \( C^k \) in \( \mathbb{F}_q^* \).

**Proof.** Let \( r \) be a primitive element of \( \mathbb{F}_q \) and set \( s = r^2 + r^3 + \cdots + r^{k-2} \). Note that we have \( (r - 1)s = r^2(r^{k-2} - 1) \), hence \( s \neq 0 \) otherwise we would have \( r^{k-2} = 1 \) contradicting that \( r \) has order \( 2nk \) in \( \mathbb{F}_q^* \). The assumption \( k \leq \sqrt{2n} \) implies that \( q > k^4 \), hence applying Lemma 6.5 with \( e = k \) we can find an element \( z \in C_0^k \) such that \( z + s \in C_1^k \). Consider the \( k \)-tuple \((x_0, x_1, \ldots, x_{k-1})\) defined by

\[
x_0 = z; \quad x_1 = -z - s; \quad x_i = r^i \quad \text{for} \quad 2 \leq i \leq k - 1.
\]

It is readily seen that this \( k \)-tuple is zero-sum. Also, we have \( x_i \in C^k_i \) for \( 0 \leq i \leq k - 1 \). This is evident for \( i \neq 1 \). For \( i = 1 \), it enough to note that \( x_1 = (-1)(z + s) \in C_0^k \cdot C_1^k = C_1^k \).

Putting together Lemma 6.1, Corollary 6.4 and Lemma 6.6 we can state the following.

**Theorem 6.7.** If \((n, k)\) is a non-Fermat demanding pair with \( k \leq \sqrt{2n} \), then there exists an optimal rank-one \( H(n, k) \).

As a matter of fact this theorem is not very satisfactory. Indeed, as we will point out in the last section, we are convinced that the same result would be true without making any assumption on \( k \).

7 Rank-one Fermat Heffter arrays

Here we consider the demanding pairs of form (1), i.e., the admissible Fermat pairs. A \( H(2^\alpha, 2^\beta) \) will be said a Fermat Heffter array.

Someone believes that the only Fermat primes are the \( F_i \)'s with \( 0 \leq i \leq 4 \), i.e., 3, 5, 17, 257 and 65537. If this was true, there are only eight Fermat pairs, that are \((32, 4), (16, 8),\) and \((2^{13-\beta}, 2^\beta)\) for \( 2 \leq \beta \leq 7 \).

Note that the group of multipliers of a rank-one Fermat Heffter array is necessarily trivial by Proposition 4.1.

We construct a rank-one \( H(2^\alpha, 2^\beta) \) for all the eight known Fermat pairs.

**Proposition 7.1.** There exists a rank-one \( H(2^\alpha, 2^\beta) \) for every known Fermat pair \((2^\alpha, 2^\beta)\).

**Proof.** Consider first the two pairs \((32, 4)\) and \((16, 8)\). Here we are in \( \mathbb{F}_{257} \) and we take \( r \) as primitive element of this field.

By computer, we have found that a zero-sum half-set of \( C^{2^3} \) is given by

\[
X = \{ r^{8i} \mid i \in I \setminus \{10, 13\} \} \cup \{-r^{8\cdot 10}, -r^{8\cdot 13}\}
\]

where \( I = \{0, 1, 2, \ldots, 31\} \). The existence of this set \( X \) implies also the existence of a zero-sum half-set of \( C^{2^3} \) by Lemma 6.3.

For \( \beta = 2, 3 \) we have also found a zero-sum complete system of representatives \( Y_\beta \) for the cosets of \( C^{2^\beta} \) in \( \mathbb{F}_{257} \) as follows:

\[
Y_2 = \{ r^0, r^{4+1}, r^{4\cdot 2+2}, r^{4\cdot 2+3} \};
\]
manding pairs \((n,k)\). There exists an optimal \(H(32,4)\) and a rank-one \(H(16,8)\) in view of Lemma 6.1.

Now let us consider the six pairs \((2^{15-\beta},2^\beta)\) with \(2 \leq \beta \leq 7\). Here we are in \(\mathbb{F}_{65537}\) and we can take again \(r = 3\) as primitive element of this field.

By computer, we have found that a zero-sum half-set of \(C^{2^\beta}\) is given by

\[ X = \{r^{128i} \mid i \in I \setminus J\} \cup \{-r^{128i} \mid i \in J\} \]

where \(I = \{0,1,2,\ldots,127\}\) and \(J = \{2,4,5,9,10,11\}\). By Lemma 6.3 the existence of this set \(X\) implies also the existence of a zero-sum half-set of \(C^{2^\beta}\) for \(2 \leq \beta \leq 7\).

For \(2 \leq \beta \leq 7\), we have also found a zero-sum complete system of representatives \(Y_\beta\) for the cosets of \(C^{2^\beta}\) in \(\mathbb{F}_{65537}\) as follows:

\[ Y_2 = \{r^0, r^{4\cdot1+1}, r^{4\cdot32+2}, r^{4\cdot38+3}\} \]
\[ Y_3 = \{r^0, r^{8\cdot17+1}, r^{8\cdot28+2}, r^3, r^4, r^5, r^6, r^7\} \]
\[ Y_4 = \{r^0, r^{16\cdot14+1}, r^{16\cdot17+2}, r^{16\cdot22+3}\} \cup \{r^i \mid 4 \leq i \leq 15\} \]
\[ Y_5 = \{r^0, r^{32\cdot12+1}, r^{32\cdot21+2}, r^{32\cdot21+3}\} \cup \{r^i \mid 4 \leq i \leq 31\} \]
\[ Y_6 = \{r^0, r^{64\cdot20+1}, r^{64\cdot72+2}, r^{64\cdot8+3}\} \cup \{r^i \mid 4 \leq i \leq 63\} \]
\[ Y_7 = \{r^0, r^{128\cdot1+1}, r^{128\cdot28+2}, r^{128\cdot80+3}\} \cup \{r^i \mid 4 \leq i \leq 127\} \]

Then we have a zero-sum half-set of \(C^{2^\beta}\) and a zero-sum complete system of representatives for the cosets of \(C^{2^\beta}\) in \(\mathbb{F}_{65537}\) for \(2 \leq \beta \leq 7\). This implies the existence of a rank-one \(H(2^{15-\beta},2^\beta)\) in view of Lemma 6.1.

### 8 Conclusion

We are convinced that the condition \(k \leq \sqrt{2n}\) of Lemma 6.6 is not necessary at all. Indeed we strongly conjecture that the second ingredient \(Y\) requested by Lemma 6.1 is always available.

**Conjecture 8.1.** Let \((n,k)\) be admissible and let \(q = 2nk + 1\). Then there exists a zero-sum complete system of representatives for the cosets of \(C^{k}\) in \(\mathbb{F}_q^*\).

In other words, we are conjecturing that at least one among the \((2n)^k\) ordered \(k\)-tuples of \(C^{n}_q \times C^{n}_q \times \cdots \times C^{n}_q\) is zero-sum. This is very reasonable considering that \((2n)^k\) is extremely greater than \(q\).

If one proved Conjecture 8.1 and we assume that there is no Fermat prime greater than \(F_4\), then we would have an optimal rank-one \(H(n,k)\) for any admissible pair \((n,k)\). It is enough to apply Lemma 6.1 and Corollary 6.1.

We have checked by computer that the conjecture is true for all the demanding pairs \((n,k)\) whose related \(q\) is less than \(10^6\). Thus, also considering the results obtained in the previous section, we can state the following.

**Proposition 8.2.** There exists an optimal \(H(n,k)\) for all the admissible pairs \((n,k)\) such that \(2nk + 1 < 10^6\).
References

[1] D.S. Archdeacon, *Heffter arrays and biembedding graphs on surfaces*, Electron. J. Combin. 22, P1.74 (2015).

[2] D.S. Archdeacon, T. Boothby, J.H. Dinitz, *Tight Heffter arrays exist for all possible values*, J. Combin. Des. 25 (2017), 5–35.

[3] R. C. Bose, *On the construction of balanced incomplete block designs*, Ann. Eugenics 9 (1939), 353–399.

[4] S. Bonvicini, M. Buratti, M. Garonzi, G. Rinaldi, T. Traetta, *The first families of highly symmetric Kirkman Triple Systems whose orders fill a congruence class*, Des. Codes Cryptogr. 89 (2021), 2725–2757.

[5] M. Buratti, A. Pasotti, *Combinatorial designs and the theorem of Weil on multiplicative character sums*, Finite Fields Appl. 15 (2009), 332–344.

[6] N.J. Cavenagh, D.M. Donovan, E.S. Yazici, *Biembeddings of cycle systems using integer Heffter arrays*, J. Combin. Designs 29 (2021), 750–764.

[7] S. Costa, A. Pasotti, M. Pellegrini, *Relative Heffter arrays and biembeddings*, Ars Math. Contemp. 18 (2020), 241–271.

[8] A. Pasotti, J.H. Dinitz, *A survey of Heffter arrays*, arXiv:2209.13879

[9] R.M. Wilson, *Cyclotomy and difference families in elementary abelian groups*, J. Number Theory 4 (1972), 17–47.