Necessary Conditions for the Existence of Group-Invariant Butson Matrices and a New Family of Perfect Arrays

Tai Do Duc
Division of Mathematical Sciences
School of Physical & Mathematical Sciences
Nanyang Technological University
Singapore 637371
Republic of Singapore
March 19, 2019

Abstract

Let $G$ be a finite abelian group and let $\exp(G)$ denote the least common multiple of the orders of all elements of $G$. A BH($G, h$) matrix is a $G$-invariant $|G| \times |G|$ matrix $H$ whose entries are complex $h$th roots of unity such that $HH^* = |G|I_G$. By $\nu_p(x)$ we denote the $p$-adic valuation of the integer $x$. Using bilinear forms over abelian groups, we [12] constructed new classes of BH($G, h$) matrices under the following conditions

(i) $\nu_p(h) \geq [\nu_p(\exp(G))/2]$ for any prime divisor $p$ of $|G|$, and
(ii) $\nu_2(h) \geq 2$ if $\nu_2(|G|)$ is odd and $G$ has a direct factor $\mathbb{Z}_2$.

The purpose of this paper is to study further the relation between $G$ and $h$ so that a BH($G, h$) matrix exists. We will only focus on BH($\mathbb{Z}_n, h$) matrices and BH($G, 2p^b$) matrices, where $p$ is an odd prime. By our results, there are 2570 open cases left for the existence of BH($\mathbb{Z}_n, h$) matrices in which $1 \leq n, h \leq 100$. 

1
In the last section, we show that BH($\mathbb{Z}_n, h$) matrices can be used to construct a new family of perfect polyphase arrays.

1 Introduction

Let $n$ and $h$ be positive integers. An $n \times n$ matrix $H$ whose entries are complex $h$th roots of unity is called a Butson matrix if $HH^* = nI$, where $H^*$ is the complex conjugate transpose of $H$ and $I$ is the identity matrix of order $n$. We also say that $H$ is a BH$(n, h)$ matrix.

Let $(G, +)$ be a finite abelian group of order $n$. An $n \times n$ matrix $A = (a_{g,k})_{g,k \in G}$ is $G$-invariant if $a_{g+l,k+l} = a_{g,k}$ for all $g, k, l \in G$. A $G$-invariant BH$(n, h)$ matrix is also called a BH$(G, h)$ matrix. Note that in the case $G = \mathbb{Z}_n$, a cyclic group of order $n$, a BH$(\mathbb{Z}_n, h)$ matrix is a circulant matrix, i.e., a matrix each of whose rows (except the first) is obtained from the previous row by shifting one position to the right and moving the last entry to the front.

For any multiple $h'$ of $h$, a BH$(G, h)$ matrix is also a BH$(G, h')$ matrix, as each $h$th root of unity is automatically a $h'$th root of unity. Therefore, it is important to find the smallest positive integer $h$ such that a BH$(G, h)$ matrix exists. The topic of group invariant Butson matrices links to many other combinatorial objects like generalized Hadamard matrices, relative difference sets, generalized Bent functions, cyclic $n$-roots, see [25], and perfect polyphase arrays.

A sequence $\{a_0, \ldots, a_{n-1}\}$ is called a perfect $h$-phase sequence of length $n$ if each $a_i$ is a complex $h$th root of unity and

$$\sum_{i=0}^{n-1} a_i \overline{a_{i+j}} = 0$$

whenever $j \neq 0$, where the indices are taken modulo $n$. Such a sequence is equivalent to a BH$(\mathbb{Z}_n, h)$ matrix whose first row is $(a_0, \ldots, a_{n-1})$. More generally, a multi-dimensional array $A = (a_{i_1,\ldots,i_k})$ of size $n_1 \times \cdots \times n_k$ is called a perfect $h$-phase array if its entries are complex $h$th roots of unity.
and
\[ \sum_{0 \leq i_1 \leq n_1 - 1} a_{i_1, \ldots, i_k} \bar{a}_{i_1 + s_1, \ldots, i_k + s_k} = 0 \]
whenever \((s_1, \ldots, s_k) \neq (0, \ldots, 0)\), where the indices are taken modulo \(n_j\) for \(1 \leq j \leq k\). In Lemma 5.3, we show that this array is equivalent to a \(BH(\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}, h)\) matrix. Perfect sequences and perfect arrays have a wide range of applications in communication systems and radar systems, see [1], [2], [6], [14], [16] for example. In the last section of this paper, we use (circulant) \(BH(\mathbb{Z}_n, h)\) matrices to construct new families of perfect polyphase arrays. By [12, Corollary 2.5], we obtain \(BH(\mathbb{Z}_n, h)\) matrices whenever

\begin{enumerate}[i)]
  \item \(\nu_p(h) \geq \lceil \nu_p(n)/2 \rceil\) for every prime divisor \(p\) of \(n\), and
  \item \(\nu_2(h) \geq 2\) if \(n \equiv 2 \pmod{4}\),
\end{enumerate}

where \(\nu_p(x)\) denotes the \(p\)-adic valuation of the integer \(x\).

In this paper, we focus on studying necessary conditions for the existence of the following two types of Butson matrices:

\begin{itemize}
  \item \(BH(\mathbb{Z}_n, h)\) matrices and
  \item \(BH(G, 2^p h)\) matrices, where \(p\) is an odd prime.
\end{itemize}

The main tools used in this paper are group-ring equations combined with techniques from the field-descent method and a study on upper bounds on the norm of cyclotomic integers. We brief the approach as following.

Let \((a_g)_{g \in G}\) be the first row of a \(BH(G, h)\) matrix \(H\). Let \(D = \sum_{g \in G} a_g g\) be an element of the group ring \(\mathbb{Z}[\zeta_h][G]\). By Result 2.3, the equation \(HH^* = |G|I\) is equivalent to

\[ DD^{(-1)} = |G| . \]

(1)

Put \(n = |G|\) and \(m = \text{lcm}(\exp(G), h)\). Let \(\chi\) be a character of \(G\) and put \(X = \chi(D) \in \mathbb{Z}[\zeta_m]\). The equation (1) becomes

\[ |X|^2 = n, \ X \in \mathbb{Z}[\zeta_m] . \]

(2)

Using the field-descent method, see [26], [27], we have a divisor \(k\) of \(m\) such that \(X \zeta_m^j\) belongs to the subfield \(\mathbb{Q}(\zeta_k)\) of \(\mathbb{Q}(\zeta_m)\) for some \(j \in \mathbb{Z}\). Note that
$X\zeta_m^j$ is a sum of roots of unity in $\mathbb{Q}(\zeta_m)$. As $X\zeta_m^j$ belongs to the smaller subfield $\mathbb{Q}(\zeta_k)$, a lot of these roots of unity cancel each other. The norm of the remaining terms can be bounded using our bound on the norm of cyclotomic integers. Moreover by (2), this norm is equal to $\sqrt{n}$. We obtain a restriction between $n$ and $h$.

Before closing this section, we give a summary of known results in this direction

Result 1.1. The following Batson matrices do not exist

1. [19, Leung-Schmidt] $\text{BH}(\mathbb{Z}_{2p^2}, 2p)$ matrices with $p$ being an odd prime.
2. [22, Ma-Ng] $\text{BH}(\mathbb{Z}_{3pq}, 3)$ matrices with $p, q > 3$ being distinct primes.
3. [17, Hiranandani-Schlenker] $\text{BH}(p + q, pq)$ matrices with $p, q > 3$ being distinct primes.

Result 1.2. (Syllester conditions, see [17]) Suppose that a $\text{BH}(n,h)$ matrix exists, then we have the following

(i) If $h = 2$, then $4$ divides $n$ and $n/4$ is a square.

(ii) If $n = p + 2$ for some prime $p \geq 3$, then $h$ does not have the form $2p^b$ for some positive integer $b$.

(iii) If $n = 2q$ for some prime $q \geq 3$, then $h$ does not have the form $2^a p^b$ for some non-negative integers $a, b$ and prime $p > q$.

Result 1.3. [18, Lam-Leung] If a $\text{BH}(G, h)$ matrix exists and $h = \prod_{i=1}^{r} p_i^e_i$ is the prime factorization of $h$, then $|G| \in p_1 \mathbb{N} + \cdots + p_r \mathbb{N}$.

Result 1.4. [8, Brock] Let $n$ be an integer and let $m$ be the square-free part of $n$. Assume that $m$ is odd. If a $\text{BH}(n,h)$ matrix exists, then $m$ has no prime factor $p$ which satisfies

(a) $p$ does not divide $h$ and

(b) $p^j \equiv -1 \pmod{h}$ for some integer $j$.

Result 1.5. [12, Duc-Schmidt] Let $G$ be an abelian group and $h$ be a positive integer. Then a $\text{BH}(G, h)$ matrix exists if
\( (i) \ v_p(h) \geq \left\lceil v_p(\exp(G)/2) \right\rceil \) for every prime divisor \( p \) of \( |G| \), and

\( (ii) \ v_2(h) \geq 2 \) if \( v_2(|G|) \) is odd and \( G \) has a direct factor \( \mathbb{Z}_2 \).

Moreover, if \( G = \mathbb{Z}_{p^a} \) is a cyclic group of prime-power order, then \( (i) \) and \( (ii) \) become necessary conditions for the existence of \( \text{BH}(\mathbb{Z}_{p^a}, h) \) matrices.

Using Results \ref{1.1}, \ref{1.2}, \ref{1.3} and \ref{1.4}, we have 4550 open cases for the existence of a \( \text{BH}(\mathbb{Z}_n, h) \) matrix in which \( 1 \leq n, h \leq 100 \). We remark that the existence problem for \( \text{BH}(\mathbb{Z}_n, h) \) matrices is in general a difficult problem. For example, the existence of \( \text{BH}(\mathbb{Z}_n, 2) \) matrices is equivalent to the existence of circulant Hadamard matrices. Ryser \cite[p. 134]{24} conjectured that circulant Hadamard matrices exist only for orders \( n = 1 \) or \( n = 4 \). This conjecture remains open for more than 50 years.

Result \ref{1.5} confirms the existence/nonexistence of 1795 cases in the 4550 open cases above. There are 2755 cases left. In the sequel, we will illustrate the impact of our new results in reducing this number of open cases.

## 2 Preliminaries

In this section, we fix some notations, state definitions and known results which will be used later. First are some notations.

1. For a positive integer \( h \), let \( \zeta_h \) denote a primitive \( h \)th root of unity.

2. For a prime \( p \) and an integer \( n \), let \( v_p(n) \) denote the \( p \)-adic value of \( n \).

3. A positive integer is **square-free** if it is not divisible by any square of a prime. We call an integer \( l \) the square-free part of \( n \) if \( l \) is the product of all prime divisors \( p \) of \( n \) in which \( v_p(n) \) is odd.

4. For coprime integers \( m \) and \( n \), we denote the smallest positive integer \( j \) such that \( m^j \equiv 1 \pmod{n} \) by \( \text{ord}_n(m) \).

As it turns out, group-ring equation is pivotal in our study. Let \( G \) be a finite abelian group of order \( n \). Let \( R \) be a ring with identity 1 and let
$R[G]$ denote the group ring of $G$ over $R$. An element $X \in R[G]$ is uniquely expressed as $X = \sum_{g \in G} a_g g$, $a_g \in R$. Two elements $X = \sum_{g \in G} a_g g$ and $Y = \sum_{g \in G} b_g g$ are equal if and only if $a_g = b_g$ for all $g \in G$. We denote $1_G$ as the identity element of $G$. A subgroup $U$ of $G$ is identified with $\sum_{u \in U} u$ in $R[G]$.

The group of complex characters of $G$ is denoted by $\hat{G}$. It is well known that $\hat{G}$ is isomorphic to $G$. The trivial character of $G$, denoted by $\chi_0$, is defined by $\chi_0(g) = 1$ for all $g \in G$. For $D = \sum_{g \in G} a_g g \in R[G]$ and $\chi \in \hat{G}$, write $\chi(D) = \sum_{g \in G} a_g \chi(g)$. Let $U$ be a subgroup of $G$, denote

$$U^\perp = \{ \chi \in \hat{G} : \chi(g) = 1 \ \forall \ g \in U \}$$

Note that $U^\perp \cong \hat{G}/U$. The following result is from [15, Lemma 2.8].

**Result 2.1.** Let $G$ be a finite abelian group and let $U$ be a subgroup of $G$. Let $\mathbb{C}$ denote the set of complex numbers and put $D = \sum_{g \in G} a_g g \in \mathbb{C}[G]$. Then for any character $\chi \in \hat{G}$, we have

$$\sum_{\tau \in U^\perp} \chi_{\tau}(D) = |U^\perp| \chi \left( \sum_{g \in U} a_g g \right)$$

The next result is called Fourier inversion formula, a proof of which can be found in [4, Chapter VI, Lemma 3.5].

**Result 2.2.** Let $G$ be a finite abelian group and let $\hat{G}$ denote the group of characters of $G$. Let $D = \sum_{g \in G} a_g g \in \mathbb{C}[G]$. Then

$$a_g = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(D g^{-1}) \ \forall \ g \in G.$$ 

Consequently, if $D, E \in \mathbb{C}[G]$ and $\chi(D) = \chi(E)$ for all $\chi \in \hat{G}$, then $D = E$.

In our study, we focus on the ring $R = \mathbb{Z}[[\zeta_h]]$. Let $D = \sum_{g \in G} a_g g$, $a_g \in R$ for all $g \in G$, be an element of $R[G]$. Let $t$ be an integer coprime to $h$ and let $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_h)/\mathbb{Q})$ be defined by $\zeta_h^\sigma = \zeta_h^t$. Let $D^{(t)}$ denote

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

6
As mentioned in the introduction, a BH\((G, h)\) matrix is equivalent to the
group-ring equation \(DD^{(-1)} = |G|\) for some \(D \in \mathbb{Z}[\zeta_h][G]\). We will use this
equivalence repeatedly and state the result here, see [12, Lemma 3.3] for a
proof.

**Result 2.3.** Let \(G\) be a finite abelian group, let \(h\) be a positive integer, and
let \(a_g, g \in G\), be integers. Consider the element \(D = \sum_{g \in G} \zeta_h^{a_g} g\) of \(\mathbb{Z}[\zeta_h][G]\)
and the \(G\)-invariant matrix \(H = (H_{g,k}), g, k \in G\), given by \(H_{g,k} = \zeta_h^{a_k-g}\).
Then \(H\) is a BH\((G, h)\) matrix if and only if
\[
DD^{(-1)} = |G|.
\]

Next, we discuss some number-theoretic results which will be needed later.

**Definition 2.4.** Let \(p\) be a prime, let \(n\) be a positive integer and write \(n = p^an'\), where \(\gcd(p,n') = 1\). The prime \(p\) is
self-conjugate modulo \(n\) if there exists an integer \(j\) such that \(p^j \equiv -1 \pmod{n'}\). A composite integer
\(m\) is self-conjugate modulo \(n\) if every prime divisor of \(m\) has this property.

The next result is from [20, Proposition 2.11].

**Result 2.5.** Let \(X = \sum_{i=0}^{m-1} a_i \zeta_m^i \in \mathbb{Z}[\zeta_m]\) so that \(X \bar{X} = n\). Let \(u\) be the
largest divisor of \(n\) which is self-conjugate modulo \(m\). Write \(u = w^2k\), where
\(k = \prod_{i=1}^r p_i\) is the square-free part of \(u\). Then \(k\) divides \(m\).

Furthermore, for each \(i = 1, \ldots, r\), denote
\[
\Theta_i = \begin{cases} 
1 - \zeta_4 & \text{if } p_i = 2, \\
\sum_{j=1}^{p_i-1} \left(\frac{j}{p_i}\right) \zeta_{p_i}^j & \text{otherwise.}
\end{cases}
\]

where \((-)\) is the Legendre symbol. Then
\[
w \prod_{i=1}^r \Theta_i \text{ divides } X.
\]

The last result in this section is a generalization of Ma’s lemma, see [21],
see also [26, Lemma 1.5.1]. The proof of this result is similar to the proof of
the original result. We provide it here for the convenience of the reader.
Result 2.6. Let $p$ be a prime and let $G$ be a finite abelian group whose Sylow $p$-subgroup $S$ is cyclic. Let $P$ be the subgroup of $S$ of order $p$. Let $t, h \in \mathbb{Z}^+$ such that $h$ is not divisible by $p$. If $D \in \mathbb{Z}[\zeta_h][G]$ satisfies
\[
\chi(D) \equiv 0 \pmod{p^t}
\]
for all characters $\chi \in \hat{G}$ of order divisible by $|S|$, then there exist $X, Y \in \mathbb{Z}[\zeta_h][S]$ such that
\[
D = p^t X + PY.
\]

Proof. Write $G = S \times H$. Note that $p \nmid |H|$. Let $s \in \mathbb{Z}^+$ such that $|S| = p^s$ and let $g$ be a generator of the cyclic group $S$. Let $\psi$ be a character of $S$ of order $p^s$. First, we claim that we can assume $D \in \mathbb{Z}[\zeta_h][S]$. Write
\[
D = \sum_{k \in H} D_k, D_k \in \mathbb{Z}[\zeta_h][S].
\]
For any character $\gamma$ of $H$, $\psi \gamma$ is a character of $G$ defined by $\psi \gamma(xy) = \psi(x) \gamma(y)$ for any $x \in S, y \in H$. Note that the order of $\psi \gamma$ is divisible by $p^s$. By (3), we have
\[
\psi \gamma(D) = \sum_{k \in H} \psi(D_k) \gamma(k) \equiv 0 \pmod{p^t}.
\]
Let $M = (\gamma(k))_{\gamma \in \hat{H}, k \in H}$ be an $|H| \times |H|$ matrix and let $u = (\psi(D_k))_{k \in H}$ be a column vector of length $|H|$. As the equation (5) holds for any character $\gamma$ of $H$, all entries of $Mu$ are divisible by $p^t$. Since $M^{-1} = M^*/|H|$ and $\gcd(p, |H|) = 1$, we obtain
\[
\psi(D_k) \equiv 0 \pmod{p^t} \text{ for all } k \in H.
\]
As (6) holds for any character $\psi$ of $S$ of order $p^s$, we can assume that $D \in \mathbb{Z}[\zeta_h][S]$ and the claim is proved.

Now define
\[
\rho : \mathbb{Z}[\zeta_h][S] \rightarrow \mathbb{Z}[\zeta_{p^s}],
\]
\[
\sum_{i=0}^{p^s-1} a_i g^i \rightarrow \sum_{i=0}^{p^s-1} a_i \zeta_{p^s}^i, \quad a_i \in \mathbb{Z}[\zeta_h] \forall i.
\]
We claim that
\[
\ker(\rho) = \{ PY : Y \in \mathbb{Z}[\zeta_h][S] \}. \tag{7}
\]
Let \( \sum_{i=0}^{p^s-1} a_i g^i \in \ker(\rho) \), then \( \sum_{i=0}^{p^s-1} a_i \zeta_{p^s}^i = 0 \). Since \( p \) does not divide \( h \), the minimal polynomial of \( \zeta_{p^s} \) over \( \mathbb{Z}[\zeta_h] \) is \( \phi(x) = 1 + x^{p^s-1} + \cdots + x^{p^s-1(p-1)} \). We obtain
\[
\sum_{i=0}^{p^s-1} a_i x^i = \phi(x)f(x), \quad f(x) \in \mathbb{Z}[\zeta_h][x],
\]
so \( \sum_{i=0}^{p^s-1} a_i g^i = \phi(g)f(g) = Pf(g) \), which proves (7).

Lastly since \( \rho(D) \equiv 0 \pmod{p^t} \), there exists \( X \in \mathbb{Z}[\zeta_h][S] \) so that \( \rho(D) = p^t \rho(X) \). We obtain \( (D - p^t X) \in \ker(\rho) \) and hence
\[
D = p^t X + PY \quad \text{for some} \quad Y \in \mathbb{Z}[\zeta_h][S].
\]

\[\square\]

3 A Theorem on Weil numbers

We start this section with a bound on the norm of a cyclotomic integer. This bound appeared in [13, Theorem 3.1]. We provide the proof here for the convenience of the reader.

Result 3.1. Let \( \alpha = \sum_{i=0}^{m-1} c_i \zeta_m^i \), \( c_i \in \mathbb{Z} \), be an element of \( \mathbb{Z}[\zeta_m] \). Then
\[
|N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\alpha)| \leq \left( \frac{m}{\phi(m)} \sum_{i=0}^{m-1} c_i^2 \right)^{\phi(m)/2}. \tag{8}
\]

Proof. Put \( f(x) = \sum_{i=0}^{m-1} c_i x^i \in \mathbb{Z}[x] \), then \( \alpha = f(\zeta_m) \) and the conjugates of \( \alpha \) in \( \mathbb{Q}(\zeta_m) \) are \( f(\zeta_{m}^t) \), where \( t \) is coprime to \( m \). We have
\[
\sum_{i=0}^{m-1} |f(\zeta_{m}^t)|^2 = \sum_{i,j,t=0}^{m-1} c_i c_j \zeta_{m}^{(i-j)t} = m \sum_{i=0}^{m-1} c_i^2.
\]
By the inequality of arithmetic and geometric means, we obtain

\[
|N(f(\zeta_m))| = \prod_{\gcd(t,m) = 1} \left| f(\zeta_m^t) \right| \\
\leq \left( \frac{\sum_{(t,m) = 1} |f(\zeta_m^t)|^2}{\varphi(m)} \right)^{\varphi(m)/2} \\
\leq \left( \frac{m}{\varphi(m)} \sum_{i=0}^{m-1} c_i^2 \right)^{\varphi(m)/2}.
\]

**Theorem 3.2.** Let \( m \) be a positive integer. Let \( X = \sum_{i=1}^{m-1} c_i \zeta_m^i, c_i \in \mathbb{Z}, \) be an element of \( \mathbb{Z}[\zeta_m] \) such that \( X \bar{X} = n. \) Assume that there exists an integer \( j \) and a divisor \( k \) of \( m \) such that \( k \) is divisible by every prime factor of \( m \) and

\[
X \zeta_m^j \in \mathbb{Z}[\zeta_k],
\]

Put \( d_i = c_{im/k-j} \) for \( 0 \leq i \leq k-1. \) Then

\[
n \leq \min \left\{ \left( \frac{k-1}{\varphi(k)} \sum_{i=0}^{k-1} d_i \right)^2, \left( \frac{k}{\varphi(k)} \sum_{i=0}^{k-1} d_i^2 \right) \right\}.
\]

**Proof.** Replacing \( X \) by \( X \zeta_m^j, \) if necessary, we can assume \( X \in \mathbb{Z}[\zeta_k]. \) Let

\[
m = \prod_{i=1}^{r} p_i^{s_i} \text{ and } k = \prod_{i=1}^{r} p_i^{t_i},
\]

be the prime factorizations of \( m \) and \( k, \) where \( s_i, t_i \in \mathbb{Z} \) and \( 1 \leq t_i \leq s_i \) for all \( i. \) A basis for \( \mathbb{Q}(\zeta_m) \) over \( \mathbb{Q}(\zeta_k) \) is

\[
\mathcal{B} = \left\{ \prod_{i=1}^{r} \zeta_{p_i}^{l_i} : 0 \leq l_i \leq p_i^{s_i-t_i} - 1 \right\}.
\]
Writing $X$ as a combination of elements in $B$ over $\mathbb{Q}(\zeta_k)$, we have

$$X = \sum_{0 \leq x_i \leq p_i^{s_i-1}} \sum_{0 \leq y_i \leq p_i^{t_i-1}} c_{x_1 \ldots x_r, y_1 \ldots y_r} \prod_{i=1}^r \zeta_{p_i^{s_i-1}}^{x_i+y_i p_i^{s_i-t_i}}$$

where the set of $c_{x_1 \ldots x_r, y_1 \ldots y_r}$'s is a permutation of the set of $c_i$'s and each $A_x, x \in B$, is an element of $\mathbb{Q}(\zeta_k)$. As $X \in \mathbb{Q}(\zeta_k)$ and $B$ is a basis for $\mathbb{Q}(\zeta_m)$ over $\mathbb{Q}(\zeta_k)$, we have $A_x = 0$ for any $x \neq 1$. Hence

$$X = A_1 = \sum_{0 \leq y_i \leq p_i^{t_i-1}} c_{0 \ldots 0, y_1 \ldots y_r} \prod_{i=1}^r \zeta_{p_i^{t_i}}^{y_i}.$$

Note that the roots of unity in $A_1$ involve the terms $\prod_{i=1}^r \zeta_{p_i^{s_i-1}}^{x_i+y_i p_i^{s_i-t_i}}$. When writing $\zeta_j^m$ in the form $\prod_{i=1}^r \zeta_{p_i^{s_i-1}}^{x_i+y_i p_i^{s_i-t_i}}$, we have $j \equiv y_i p_i^{s_i-t_i} \pmod{p_i^{s_i}}$ for all $i$. So $j \equiv 0 \pmod{m/k}$ for all $i$, which implies $j \equiv 0 \pmod{m/k}$. Therefore, in the original expression $X = \sum_{i=0}^{m-1} c_i \zeta_i^m$, only the exponents divisible by $m/k$ survive in $X = A_1$. We obtain

$$X = \sum_{i=0}^{k-1} d_i \zeta_k^i, \quad d_i = c_{im/k}.$$

Thus

$$n = |X|^2 \leq \left( \sum_{i=1}^k |d_i| \right)^2. \quad (11)$$

Note that $n^{\varphi(k)/2} = N_{\mathbb{Q}(\zeta_k)/\mathbb{Q}}(X)$, as $X \bar{X} = n$. The inequality (11) is proved by (11) and Lemma 3.1.

To apply Theorem 3.2, we need to find a divisor $k$ of $m$ which contains all prime divisors of $m$ and satisfies $X \zeta_m^j \in \mathbb{Z}[\zeta_k]$ for some $j \in \mathbb{Z}$. Fortunately, the field-descent method by Schmidt [26, 27] provides exactly what we need.
Result 3.3. If $X \in \mathbb{Z}[\zeta_m]$ satisfies $X \bar{X} = n$, then there exists an integer $j$ and a divisor $F(m, n)$ of $m$ which is divisible by every prime divisor of $m$ such that $X \zeta_m^j \in \mathbb{Z}[\zeta_{F(m, n)}]$.

The number $F(m, n)$ is defined as follows:

Definition 3.4. Let $m$ and $n$ be positive integers and let $m = \prod_{i=1}^{t} p_i^{c_i}$ be the prime factorization of $m$. For each prime divisor $q$ of $n$, define

$$\tilde{m}_q = \begin{cases} \prod_{p_i \neq q} p_i & \text{if } m \text{ is odd or } q = 2, \\ 4 \prod_{p_i \neq 2, q} p_i & \text{otherwise}. \end{cases}$$

Let $D(n)$ denote the set of all prime divisors of $n$. Let

$$F(m, n) = \prod_{i=1}^{t} p_i^{b_i}$$

be the minimum multiple of $\prod_{i=1}^{t} p_i$ such that for every pair $(i, q)$ with $1 \leq i \leq t$ and $q \in D(n)$, at least one of the following conditions is satisfied:

(a) $q = p_i$ and $(p_i, b_i) \neq (2, 1)$, or

(b) $b_i = c_i$, or

(c) $q \neq p_i$ and $q^{\text{ord}_{\tilde{m}_q}(q)} \not\equiv 1 \pmod{p_i^{b_i+1}}$.

We obtain an immediate corollary using Theorem 3.2 and Result 3.3.

Corollary 3.5. Let $m$ be a positive integer and let $X = \sum_{i=0}^{m-1} c_i \zeta_m^i$, $a_i \in \mathbb{Z}$, be an element of $\mathbb{Z}[\zeta_m]$ such that $X \bar{X} = n$. Then there exists an integer $j$ such that $X \zeta_m^j \in \mathbb{Z}[\zeta_{F(m, n)}]$. Moreover, putting $d_i = c_{im/F(m,n)-j}$ for $0 \leq i \leq F(m, n) - 1$, we have

$$n \leq \min \left\{ \left( \sum_{i=0}^{F(m,n)-1} |d_i| \right)^2, \left( \frac{F(m,n)}{\varphi(F(m,n))} \sum_{i=0}^{F(m,n)-1} d_i^2 \right) \right\}. \quad (12)$$

In the coming sections, we will apply Theorem 3.2 to study necessary conditions for the existence of group-invariant Butson matrices.
4 Necessary conditions

We will focus only on two types of matrices: BH($\mathbb{Z}_n$, $h$) matrices and BH($G, 2p^b$) matrices, where $p$ is an odd prime and $n, h, b$ are positive integers.

4.1 The existence of BH($\mathbb{Z}_n$, $h$) matrices

For positive integers $k$ and $n$, let $n_k$ denote the largest divisor of $n$ which is coprime to $k$ and put $n(k) = n/n_k$. By Result ??, there exist BH($\mathbb{Z}_n$, $h$) matrices whenever $n$ divides $(h, n)^2$ and $n$ and $h$ are not both congruent to 2 modulo 4. We conjecture that these conditions are also necessary for the existence of BH($\mathbb{Z}_n$, $h$) matrices.

Conjecture 4.1. Let $n$ and $h$ be positive integers. Then there exists a BH($\mathbb{Z}_n$, $h$) matrix if and only if

(i) $\nu_p(h) \geq \lceil \nu_p(n)/2 \rceil$ for every prime divisor $p$ of $n$, and

(ii) $\nu_2(h) \geq 2$ if $n \equiv 2 \pmod{4}$.

A special case of Conjecture 4.1 is the circulant Hadamard matrix conjecture which was mentioned in the introduction. Unfortunately, we are far from proving Conjecture 4.1. In support of it, we prove that $n \leq (h, n)^2$ under certain restrictions between $n$ and $h$.

Theorem 4.2. Let $n$ and $h$ be positive integers and put $m = \text{lcm}(n, h)$. Suppose that a BH($\mathbb{Z}_n$, $h$) matrix exists. Furthermore, assume that for any prime divisor $p$ of $n$, we have

(i) $p$ divides $h$, and

(ii) $q^{\nu_p(n)/q^\nu_p(n) - 1} \not\equiv 1 \pmod{p^{\nu_p(n)(h) + 1}}$ for any prime divisor $q \neq p$ of $n$,

where $\bar{m}_q$ is defined in Definition 3.4. Then

$$n \leq (h, n)^2.$$  

(13)
Proof. Let $H$ be a $BH(\mathbb{Z}_n, h)$ matrix and let its first row be $(\zeta_h^{a_0}, \ldots, \zeta_h^{a_{n-1}})$, $a_i \in \mathbb{Z}$. Let $g$ be a generator of the cyclic group $\mathbb{Z}_n$ and let $D = \sum_{i=0}^{n-1} \zeta_h^{a_i} g^i$ be an element of the group ring $\mathbb{Z}[\zeta_h][\mathbb{Z}_n]$. We obtain, by Result 2.3,

$$DD^{(-1)} = n. \quad (14)$$

Let the character $\chi$ of the group $\mathbb{Z}_n$ be defined by $\chi(g) = \zeta_n$. Put

$$X = \chi(D) = \sum_{i=0}^{n-1} \zeta_{h}^{a_i} \zeta_{n}^{i} \in \mathbb{Z}[\zeta_n].$$

By Result 3.3 there exists an integer $j$ such that $X \zeta_m^j \in \mathbb{Z}[\zeta_{F(m,n)}]$. Since $\gcd(m/h, m/n) = 1$, there exist integers $\alpha$ and $\beta$ such that $\alpha m/h + \beta m/n = j$. Replacing $D$ by $D \zeta_h^{-\alpha} g^{-\beta}$, if necessary, we can assume that $X \in \mathbb{Z}[\zeta_{F(m,n)}]$. Thus $X \in \mathbb{Z}[\zeta_h]$, as $F(m, n)$ divides $h$ by the definition of $F(m, n)$ and by the conditions (i) and (ii). With $h$ in the place of $k$, all conditions in Theorem 3.2 are satisfied. Note that

$$X = \sum_{i=0}^{n-1} \zeta_{h}^{a_i(m/h)+i(m/n)}.$$

To apply (10), we need to find the exponents in $X$ which are divisible by $m/h$. These are the ones containing the indices $i$ such that $n/(h, n)$ divides $i$. There are $(h, n)$ such exponents, as $0 \leq i \leq n - 1$. Recall that $X \in \mathbb{Z}[\zeta_h]$. When expressing $X$ in the form $\sum_{i=0}^{h-1} d_i \zeta_h^i$, we have $\sum_{i=0}^{h-1} d_i = (h, n)$. We obtain, by (10),

$$n \leq (h, n)^2.$$

Note that the condition (ii) in Theorem 4.2 is true by default if $n$ is a power of a prime $p$. To apply Theorem 3.2 in this case, it remains to prove that $p$ divides $h$. Assume the validity of this claim, the inequality $n \leq (h, n)^2$ becomes $v_p(h) \geq \lceil v_p(n)/2 \rceil$. This is exactly the necessary condition in the second part of Result 1.5 for the existence of $BH(\mathbb{Z}_p, h)$ matrices.

Remark 4.3. As mentioned in the introduction, there are 2755 open cases for the existence of a $BH(\mathbb{Z}_n, h)$ matrix with $1 \leq n, h \leq 100$. Theorem 4.2
confirms the nonexistence of 8 of these cases and we are left with 2747 cases. The parameters \((n, h)\) which are eliminated by Theorem 4.2 are

\[(54, 6), (54, 12), (54, 24), (54, 30), (54, 48), (54, 60), (54, 66), (54, 96).\]

Eventually, the restriction \(n, h \leq 100\) is somewhat strict for Theorem 4.2 to apply. If we allow \(n, h \leq 200\), Theorem 4.2 can rule out 24 more cases:

\[n = 54, h \in \{102, 120, 132, 138, 150, 174, 186, 192\}\]

\[n = 162, h \in \{6, 12, 24, 30, 48, 60, 66, 96, 102, 132, 138, 150, 174, 186, 192\}\]

For the next result, we recall the self-conjugacy concept in Definition 2.4. We would like to study the part of \(n\) which is self-conjugate modulo \(m = \text{lcm}(n, h)\).

**Theorem 4.4.** Let \(n\) and \(h\) be positive integers and put \(m = \text{lcm}(n, h)\). If a \(BH(Z_n, h)\) matrix exists, then any prime divisor of \(n\) which is self-conjugate modulo \(m\) divides \(h\).

**Proof.** Suppose that there exists a prime divisor \(p\) of \(n\) which is self-conjugate modulo \(m\) and \(p \nmid h\). Letting \(g\) be a generator of the group \(Z_n\) and defining \(D = \sum_{i=0}^{n-1} \zeta_h^{a_i} g^i\) as in the proof of Theorem 4.2, we have \(DD^{(-1)} = n\). For any character \(\chi\) of \(Z_n\), we have

\[|\chi(D)|^2 = n, \quad \chi(D) \in \mathbb{Z}[\zeta_m]. \tag{15}\]

Applying \(\chi_0\) to (15) and putting \(Y = \chi_0(D) \in \mathbb{Z}[\zeta_h]\), we obtain \(|Y|^2 = n\). As \(p\) is self-conjugate modulo \(m\) and \(h \mid m\), \(p\) is also self-conjugate modulo \(h\). By Result 2.3 and by the condition \(p \nmid h\), we obtain \(v_p(n) = 2t\) for some \(t \in \mathbb{Z}^+\). We also have \(v_p(m) = 2t\), as \(m = \text{lcm}(n, h)\). Moreover, since \(|\chi(D)|^2 = n\) and \(\chi(D) \in \mathbb{Z}[\zeta_m]\), Result 2.5 implies \(p^t \mid \chi(D)\) for any character \(\chi\) of \(Z_n\). By Result 2.6, we obtain

\[D = p^t X + PY, \tag{16}\]

where \(P\) is the cyclic subgroup of \(Z_n\) of order \(p\), and \(X, Y \in \mathbb{Z}[\zeta_h][Z_n]\). As \(kP = P\) for any \(k \in P\), we can assume that in (16), \(Y\) contains only coset representatives of \(Z_n/P\). Comparing the coefficients on a fixed coset of \(P\), the equation (16) implies

\[\zeta_h^{a_i} \equiv \zeta_h^{a_i+n/p} \equiv \cdots \equiv \zeta_h^{a_i+(p-1)n/p} \pmod{p^t}\]

for any \(0 \leq i \leq n/p - 1\).
Hence \( \zeta_h^{a_j} \equiv \zeta_h^{a_{j+n/p}} \pmod{p^j} \) for all \( j \).

Suppose that \( \zeta_h^{a_j} = \zeta_h^{a_{j+n/p}} \) for all \( j \). We have \( D = PZ \) with 
\[ Z = \sum_{i=0}^{n/p-1} \zeta_h^i g^i. \]
Let \( \tau \) be a primitive character of \( C_n \), then \( \tau(D) = 0 \), contradicting with (15).

Therefore, there exists \( j \) such that \( \zeta_h^{a_j} \neq \zeta_h^{a_{j+n/p}} \). The condition \( \zeta_h^{a_j} \equiv \zeta_h^{a_{j+n/p}} \pmod{p^t} \) implies that \( t = 1 \) and \( p = 2 \) (note that \( |\zeta_h^{a_j} - \zeta_h^{a_{j+n/p}}| \leq 2 \)).
The congruence \( \zeta_h^{a_j} \equiv \zeta_h^{a_{j+n/2}} \pmod{2} \) happens only when \( 2 \mid h \) and \( a_{j+n/2} = a_j + h/2 \), contradicting with the assumption that \( p \) does not divide \( h \).  

**Corollary 4.5.** If \( n \) and \( h \) are coprime positive integers such that a BH\((\mathbb{Z}_n, h)\) matrix exists, then no prime divisor of \( n \) is self-conjugate modulo \( nh \).

**Remark 4.6.** By Remark 4.3 there are 2747 open cases left for the existence of BH\((\mathbb{Z}_n, h)\) matrices in which \( 1 \leq n, h \leq 100 \). Theorem 4.4 eliminates 130 of these cases and there are 2617 cases left. The excluded cases are:

- \( n = 12, h \in \{3, 9, 27, 33, 57, 81, 99\} \)
- \( n = 18, h \in \{4, 10, 14, 28, 34, 38, 50, 58, 62, 74, 76, 82, 86, 98\} \)
- \( n = 20, h \in \{5, 25, 65\} \)
- \( n = 36, h \in \{2, 3, 4, 9, 14, 27, 28, 33, 38, 57, 62, 74, 76, 81, 86, 98, 99\} \)
- \( n = 44, h \in \{11, 33, 57, 99\} \)
- \( n = 45, h \in \{5, 10, 15, 25, 30\} \)
- \( n = 48, h \in \{3, 9, 27, 33, 57, 81, 99\} \)
- \( n = 50, h \in \{6, 14, 18, 21, 26, 34, 42, 46, 54, 58, 63, 69, 74, 82, 86, 87, 94, 98\} \)
- \( n = 52, h \in \{13, 65\} \)
- \( n = 63, h \in \{7, 14, 28, 38, 49, 62, 74, 76, 98\} \)
- \( n = 68, h \in \{17\} \)
- \( n = 75, h \in \{3, 6, 9, 18, 21, 26, 27, 42, 46, 54, 63, 69, 81, 87, 94\} \)
- \( n = 76, h \in \{19, 33, 57, 99\} \)
- \( n = 80, h \in \{5, 25, 65\} \)
- \( n = 90, h \in \{10, 50\} \)
- \( n = 98, h \in \{4, 8, 10, 22, 26, 34, 44, 46, 50, 82, 86, 88, 92\} \)
- \( n = 100, h \in \{5, 21, 25, 63, 65, 69, 87\} \).

In preparation for the next theorem, we need the following result, see [27, Lemma 2.5] for a proof.
Result 4.7. Let $m \in \mathbb{Z}^+$ and let $k$ be a divisor of $m$. Let $t$ and $s$ be the numbers of prime divisors of $m$ and $k$, respectively. Write $X = \sum_{i=0}^{m-1} a_i \zeta_m^i$, where $a_i \in \mathbb{Z}$ for all $i$. Then there exists an integral basis $\mathcal{B}_{m,k}$ of $\mathbb{Q}(\zeta_m)$ over $\mathbb{Q}(\zeta_k)$ which contains $\varphi(m/k)$ roots of unity. Furthermore, if $0 \leq a_i \leq C$ for all $i$, then we can express $X$ as

$$X = \sum_{x \in \mathcal{B}_{m,k}} x \left( \sum_{j=0}^{k-1} c_{xj} \zeta_k^j \right),$$

where the delta function $\delta_{ts}$ is defined by

$$\delta_{ts} = \begin{cases} 0 & \text{if } t \neq s, \\ 1 & \text{if } t = s. \end{cases}$$

(17)

Theorem 4.8. Let $n$ and $h$ be positive integers and put $m = \text{lcm}(n,h)$. Let $u$ be the largest divisor of $n$ which is self-conjugate modulo $m$. Write $u = w^2 k$, where $k$ is the square-free part of $u$. Let $t$ and $r$ be the numbers of prime divisors of $h$ and $k$, respectively. Suppose that a $BH(\mathbb{Z}_n,h)$ matrix exists. Then

$$w \leq 2^{t-r-1+\delta_{ts}} (h,u) \sqrt{\frac{k}{\varphi(k)}},$$

(18)

Proof. Similar to the proof of Theorem 4.2, we have $DD^{(-1)} = n$, where $D = \sum_{i=0}^{n-1} \zeta_n^a g^i \in \mathbb{Z}[\zeta_n][\mathbb{Z}_n]$ and $g$ is a generator of $\mathbb{Z}_n$. Hence for any character $\chi$ of $\mathbb{Z}_n$, we have

$$|\chi(D)|^2 = n, \; \chi(D) \in \mathbb{Z}[\zeta_m].$$

(19)

Put $v = n/u$. Note that $(u,v) = 1$. Let $\tau$ be a character of $\mathbb{Z}_n$ which is primitive on the subgroup $\mathbb{Z}_u = \langle g^v \rangle$ of $\mathbb{Z}_n$, that is $\tau(g^v) = \zeta_u$. Let $R = \{1, g, \ldots, g^{v-1}\}$ be a set of coset representatives of $\mathbb{Z}_u$ in $\mathbb{Z}_n$. We claim that there exists $x \in R$ such that $\tau(D \cap k\mathbb{Z}_u) \neq 0$. Assume otherwise, then $\tau(D) = \tau(D \cap \mathbb{Z}_n) = \sum_{x \in R} \tau(D \cap x\mathbb{Z}_u) = 0$, contradicting with (19). For this value of $x$, we have $\tau(D^{-1} \cap \mathbb{Z}_u) = \tau(x^{-1}) \tau(D \cap x\mathbb{Z}_u) \neq 0$. Thus replacing $D$ by $Dx^{-1}$ (if necessary), we can assume that

$$\tau(D \cap \mathbb{Z}_u) 
eq 0.$$
Write \( k = \prod_{i=1}^{r} p_i \). By Result 2.5, we have \((w \prod_{i=1}^{r} \Theta_i) | \chi(D)\) for any character \( \chi \) of \( \mathbb{Z}_n \). Furthermore, by Result 2.1, we have

\[
\sum_{\chi \in \mathbb{Z}_n} \chi \tau(D) = |\mathbb{Z}_n^+|\tau(D \cap \mathbb{Z}_u) = v \left( \sum_{i=0}^{u-1} \zeta_h^b \zeta_u^i \right),
\]

(20)

where \( D \cap \mathbb{Z}_u = \sum_{i=0}^{u-1} \zeta_h^{a_{vi}} g^{vi} \) and \( b_i = a_{vi} \). Since \((u, v) = 1\) and each term on the left side of (20) is divisible by \((w \prod_{i=1}^{r} \Theta_i)\), we obtain

\[
\left( w \prod_{i=1}^{r} \Theta_i \right) \text{ divides } \left( \sum_{i=0}^{u-1} \zeta_h^b \zeta_u^i \right).
\]

(21)

Put \( l = \text{lcm}(h, u) \) and write \( X = \sum_{i=0}^{u-1} \zeta_h^b \zeta_u^i \) (note that \( X = \tau(D \cap \mathbb{Z}_u) \neq 0 \)) in the form

\[
X = \sum_{i=0}^{l-1} c_i \zeta_l^i, \quad c_i \in \mathbb{Z}^+.
\]

(22)

By Theorem 4.4, any prime divisor of \( u \) divides \( h \), so the numbers of prime divisors of \( l \) and \( h \) are the same, both equal to \( t \). Put \( d = (h, u) \). We claim that

\[
0 \leq c_i \leq d \quad \text{for any } i = 0, \ldots, l - 1.
\]

(23)

For a fixed \( 0 \leq i \leq l - 1 \), let \( x \) (mod \( h/d \)) and \( y \) (mod \( u/d \)) be the unique integers such that \((u/d)x + (h/d)y = i\). All the solutions \( j \) (mod \( h \)) and \( f \) (mod \( u \)) to \( \zeta_l^i = \zeta_h^j \zeta_u^f \) are

\[
j = x + l \frac{h}{d}, \quad f = y - l \frac{u}{d}, \quad 0 \leq l \leq d - 1.
\]

There are at most \( d \) solutions and the claim (23) is proved.

By Result 4.7 and (23), we can express \( X \) in the form (22) as a combination of the elements of \( \mathcal{B}_{l,k} \) over \( \mathbb{Q}(\zeta_k) \) as follows

\[
X = \sum_{x \in \mathcal{B}_{l,k}} x \left( \sum_{j=0}^{k-1} c_{xj} \zeta_k^j \right),
\]

where

\[
|c_{xj}| \leq 2^{t-r-1+\delta r}d \quad \text{for all } x \in \mathcal{B}_{l,k}, 0 \leq j \leq k - 1.
\]

(24)
Note that by \( (21) \), \((w \prod_{i=1}^{r} \Theta_i) \in Q(\zeta_k)\) divides \(X \in Q(\zeta_i)\). Hence \((w \prod_{i=1}^{r} \Theta_i)\) divides \(\left( \sum_{j=0}^{k-1} c_{xj} \zeta_k^j \right)\) for each \(x \in B_{l,k}\). As \(X \neq 0\), there exists \(x \in B_{l,k}\) so that \(Y = \sum_{j=0}^{k-1} c_{xj} \zeta_k^j \neq 0\) and
\[
\left( w \prod_{i=1}^{r} \Theta_i \right) \text{ divides } Y. \quad (25)
\]

Note that each \(\Theta_i\) has norm \(\sqrt{p_i}\). Using \((24)\), \((25)\) and the inequality \((8)\), we obtain
\[
(w^2 k)^{\varphi(k)/2} = \left| N_{Q(\zeta_k)/Q} \left( w \prod_{i=1}^{r} \Theta_i \right) \right| \leq \left| N_{Q(\zeta_k)/Q}(Y) \right| \leq \left( \frac{k}{\varphi(k)} \sum_{j=0}^{k-1} c_{xj}^2 \right)^{\varphi(k)/2} \leq \left( 4^{t-1+\delta_r \ell} d^2 \frac{k^2}{\varphi(k)} \right)^{\varphi(k)/2},
\]
proving \((18)\). \(\square\)

**Corollary 4.9.** Let \(n\) and \(b\) be positive integers and let \(p\) be a prime. Suppose that a \(BH(\mathbb{Z}_n, p^b)\) matrix exists. Then \(n = p^c m\) for some positive integers \(c\) and \(m\) with \(\gcd(p, m) = 1\). Moreover if \(p\) is selfconjugate modulo \(m\), then
\[
b \geq \lfloor c/2 \rfloor. \quad (26)
\]

**Proof.** The claim that \(n = p^c m\) with \(c \in \mathbb{Z}^+\) follows directly from Result \([13]\).

We apply the inequality \((18)\) to prove the second claim. In this case, we have \(u = p^c\), \(w = p^{(c/2)}\), \(t = 1\), \(r \in \{0, 1\}\) and \(k \in \{1, p\}\). We have
\[
p^{(c/2)} \leq (p^b, p^c) \sqrt{\frac{p}{p-1}} < p^{b+1},
\]
proving \((26)\). \(\square\)

**Remark 4.10.** By Remark \([4,6]\) there are 2617 open cases for the existence of \(BH(\mathbb{Z}_n, h)\) matrices in which \(1 \leq n, h \leq 100\). Theorem \([1,3]\) eliminates 4 of these cases, which are \((n, h) \in \{(96, 6), (96, 18), (96, 22), (96, 54)\}\). There are 2613 cases left.
Similar to Theorem 4.2, the condition \( n, h \leq 100 \) has a severe impact on the strength of Theorem 4.8. The result applies better for larger values of \( n \) and \( h \). For example if we allow \( n, h \leq 200 \), then Theorem 4.8 excludes up to 28 cases which cannot be ruled out by other conditions:
\[
\begin{align*}
n & = 96, \quad h \in \{6, 18, 22, 54, 118, 162, 166\}, \\
n & = 144, \quad h = 2, \\
n & = 162, \quad h \in \{15, 21, 51, 75, 87, 93, 111, 123, 147, 159, 183\}, \\
n & = 192, \quad h \in \{6, 18, 22, 54, 118, 162, 166\}.
\end{align*}
\]

### 4.2 The existence of BH\((G, 2p^b)\) matrices

Let \( G \) be an abelian group, let \( p \) be an odd prime and let \( b \) be a positive integer. The main result of this section relies on the following result by Leung and Schmidt, see [19, Theorem 22 and Theorem 23].

**Result 4.11.** Let \( p \) be an odd prime and let \( a \) be a positive integer. Let \( m \) be a nonsquare integer and let \( q_1, \ldots, q_s \) be all distinct prime divisors of \( m \). Put \( f = \gcd(\text{ord}_p(q_1), \ldots, \text{ord}_p(q_s)) \). Suppose that \( X \in \mathbb{Z}[\zeta_p^a] \) satisfies \( |X|^2 = m \). Then the following hold:

(i) \( f \) is an odd integer.

(ii) Either \( f \leq m \) or \( p \leq (f^2 - m)/(f - m) \).

(iii) \( p \leq m^2 + m + 1 \).

**Theorem 4.12.** Let \( b \) be a positive integer, let \( p \) be an odd prime and let \( G \) be an abelian group. Write \( |G| = p^c m \), where \( c \geq 0 \) and \( p \) does not divide \( m \). Suppose that \( m \) is not a square. Let \( q_1, \ldots, q_s \) be all distinct prime divisors of \( m \). Put \( f = \gcd(\text{ord}_p(q_1), \ldots, \text{ord}_p(q_s)) \). If either a BH\((G, p^b)\) matrix or a BH\((G, 2p^b)\) matrix exists, then the following hold:

(i) \( f \) is odd.

(ii) Either \( f \leq m \) or \( p \leq (f^2 - m)/(f - m) \).

(iii) \( p \leq m^2 + m + 1 \).
Proof. As $BH(G, p^b) \subset BH(G, 2p^b)$, it suffices to assume that a $BH(G, 2p^b)$ matrix $H$ exists. Let the first row of $H$ be $(\zeta^{a_g}_{2p^b})_{g \in G}$, $a_g \in \mathbb{Z}$ for all $g \in G$. By Result 2.3, we have
\[ DD^{(-1)} = p^c m, \quad D = \sum_{g \in G} \zeta^{a_g}_{2p^b} g \in \mathbb{Z}[\zeta_{2p^b}][G]. \]

Put $X = \chi_0(D) = \sum_{g \in G} \zeta^{a_g}_{2p^b}$. We obtain
\[ X \bar{X} = p^c m, \quad X \in \mathbb{Z}[\zeta_{2p^b}] = \mathbb{Z}[\zeta_{p^b}]. \]

In the ring $\mathbb{Z}[\zeta_{p^b}]$, we have $p\mathbb{Z}[\zeta_{p^b}] = (1 - \zeta_{p^b})^{\varphi(p^b)}$ and $(1 - \zeta_{p^b})$ is the only prime ideal above $p$. Thus $(1 - \zeta_{p^b})^{\varphi(p^b)c/2}$ divides $(X)$ as ideals of $\mathbb{Z}[\zeta_{p^b}]$.

Putting $Y = X(1 - \zeta_{p^b})^{-\varphi(p^b)c/2} \in \mathbb{Z}[\zeta_{p^b}]$, we obtain
\[ YY = m. \]

The conclusion follows directly from Result 4.11. \qed

Corollary 4.13. If $G$ is an abelian group with $|G| = 2p^c$ for some non-negative integer $c$ and odd prime $p$, then a $BH(G, 2p^b)$ matrix or a $BH(G, p^b)$ matrix exists only when $p = 7$.

Proof. Using Theorem 4.12 part (iii) for $m = 2$, we obtain $p \leq 7$. The case $p = 3$ or $p = 5$ cannot satisfy the condition $f = \text{ord}_p(2)$ is odd. Therefore, the only possible value for $p$ is $p = 7$. \qed

We note that the case $p = 7$ is also ruled out by Leung and Schmidt \[19\] by a rather complicated argument. We will not discuss it here. In summary, there is no $BH(G, 2p^b)$ matrix or $BH(G, p^b)$ matrix in which $G$ is an abelian group of order $2p^c$ for some non-negative integer $c$.

Remark 4.14. By Remark 4.10, there are 2613 open cases for the existence of a $BH(\mathbb{Z}_n, h)$ matrix with $1 \leq n, h \leq 100$. Theorem 4.12 confirms the nonexistence of 43 cases and there are 2570 cases left. The excluded cases are
\[(6, 6), (6, 18), (6, 54), (10, 10), (10, 50), (18, 18), (18, 54), (22, 22),\]

21
(24, 6), (24, 18), (24, 54), (26, 26), (34, 34), (38, 38), (40, 10), (40, 50),
(46, 23), (46, 46), (50, 50), (54, 18), (54, 54), (58, 58), (62, 31), (62, 62),
(69, 23), (69, 46), (72, 6), (72, 10), (72, 18), (72, 34), (72, 38), (72, 50), (72, 54), (72, 58),
(72, 74), (72, 82), (72, 86), (74, 74), (82, 82), (86, 86), (88, 22), (94, 47), (94, 94)

5 Application to Perfect Polyphase Arrays

We recall from the introduction that a perfect $h$-phase sequence of length $n$
is equivalent to a BH($\mathbb{Z}_n, h$) matrix. Theorem 4.2, Theorem 4.4, Theorem
4.8 and Theorem 4.12 give various necessary conditions for the existence of
such sequences.

Moreover, let $A = (a_{i_1,\ldots,i_k})$ be a multi-dimensional array of size $n_1 \times \cdots \times n_k$. The auto-correlation functions of $A$ are defined as follows:

$$R_{s_1,\ldots,s_k} = \sum_{i_1,\ldots,i_k} a_{i_1,\ldots,i_k} \bar{a}_{i_1+s_1,\ldots,i_k+s_k}.$$  

The array $A$ is a perfect $h$-phase array if each of its entry is a complex $h$th
root of unity and all nontrivial auto-correlation functions of $A$ are equal to
0, that is

$$R_{s_1,\ldots,s_k} = 0$$

whenever $(s_1,\ldots,s_k) \neq (0,\ldots,0)$, where the indices are taken modulo $n_j$ for
1 $\leq j \leq k$.

In this section, we prove that a set of $k$ BH($\mathbb{Z}_{n_i}, h$) matrices, $1 \leq i \leq k$,
can be used to construct a perfect $h$-phase array of size $n_1 \times \cdots \times n_k$. The
following result is proved in [12], see also [23].

**Result 5.1.** Let $n$ and $h$ be positive integers. Then a BH($\mathbb{Z}_n, h$) matrix exists
whenever $n$ and $h$ satisfy the following condition:

$$n \mid (h,n)^2 \text{ and } (v_2(n), v_2(h)) \neq (1,1).$$  

The table below gives parameters of known arrays, see [5].
To prepare for the main result of this section, we need the following lemmas

Lemma 5.2. Let $h_1$ and $h_2$ be positive integers and put $h = \text{lcm}(h_1, h_2)$. Let $G_1$ and $G_2$ be abelian groups and assume that $H_1$ is a $\text{BH}(G_1, h_1)$ matrix and $H_2$ is a $\text{BH}(G_2, h_2)$ matrix. Then the Kronecker product $H_1 \otimes H_2$ is a $\text{BH}(G_1 \times G_2, h)$ matrix.

Proof. Assume that $H_1 = (h_{x_1,y_1})_{x_1,y_1 \in G_1}$ and $H_2 = (k_{x_2,y_2})_{x_2,y_2 \in G_2}$. The elements of the matrix $H_1 \otimes H_2$ are indexed by $G_1 \times G_2$ in which the $(x_1, x_2) \times (y_1, y_2)$ element is $h_{x_1,y_1}k_{x_2,y_2}$. Let $(a_1, a_2)$ be any element in $G_1 \times G_2$. The $(a_1 + x_1, a_2 + x_2) \times (a_1 + y_1, a_2 + y_2)$ element of $H_1 \otimes H_2$ is

$$h_{a_1+x_1,a_1+y_1}k_{a_2+x_2,a_2+y_2} = h_{x_1,y_1}k_{x_2,y_2},$$

as $H_1$ is $G_1$-invariant and $H_2$ is $G_2$-invariant. Thus, the matrix $H_1 \otimes H_2$ is $G_1 \times G_2$-invariant.

Lastly, each entry of $H_1 \otimes H_2$ is the product of a $(h_1)$th root of unity and a $(h_2)$th root of unity, so it is a $h$th root of unity. \[\square\]

Lemma 5.3. Let $k, h, n_1, \ldots, n_k$ be positive integers. Then a $\text{BH}(\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}, h)$ matrix exists if and only if a perfect $h$-phase array of size $n_1 \times \cdots \times n_k$ exists.
Proof. Put $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ and suppose that a BH($G, h$) matrix exists. For each $1 \leq i \leq k$, let $g_i$ be a generator of $\mathbb{Z}_{n_i}$. By Result 2.3, there exists $D \in \mathbb{Z}[\zeta_h][G]$ such that $DD^{-1} = n_1 \cdots n_k$. Write

$$D = \sum_{0 \leq i_1, \ldots, i_k \leq n_i - 1} a_{i_1, \ldots, i_k} g_1^{i_1} \cdots g_k^{i_k},$$

where each $a_{i_1, \ldots, i_k} \in \mathbb{Z}[\zeta_h]$ is a complex $h$th root of unity. Note that

$$DD^{-1} = \sum_{0 \leq s_j \leq n_j - 1} \left( \sum_{0 \leq i_j \leq n_j - 1} a_{i_1 + s_1, \ldots, i_k + s_k} \pi_{i_1, \ldots, i_k} \right) g_1^{s_1} \cdots g_k^{s_k},$$

As $DD^{-1} = n_1 \cdots n_k$, we obtain

$$\sum_{i_1, \ldots, i_k} a_{i_1 + s_1, \ldots, i_k + s_k} \pi_{i_1, \ldots, i_k} = \begin{cases} n_1 \cdots n_k & \text{if } s_1 = \cdots = s_k = 0, \\ 0 & \text{otherwise.} \end{cases} \quad (27)$$

Define the array $A$ of size $n_1 \times \cdots \times n_k$ by

$$A = (a_{i_1, \ldots, i_k}), \quad 0 \leq i_j \leq n_j - 1 \text{ for all } j.$$

The equation (27) implies that $A$ is perfect. Conversely, it is straightforward to verify that a perfect array $A$ implies the existence of a group ring element $D \in \mathbb{Z}[\zeta_h][G]$ whose coefficients are complex $h$th roots of unity such that $DD^{-1} = n$, which implies a BH($G, h$) matrix by Result 2.3.

**Theorem 5.4.** Suppose that $k, h, n_1, \ldots, n_k$ are positive integers such that

$$n_i \mid (h, n_i)^2 \text{ and } (v_2(n_i), v_2(h)) \neq (1, 1) \text{ for any } 1 \leq i \leq k. \quad (*)$$

Then a perfect $h$-phase multi-dimensional array of size $n_1 \times \cdots \times n_k$ exists.

**Proof.** The conditions (*) imply that BH($\mathbb{Z}_{n_i}, h$) matrices exist for any $i = 1, \ldots, k$. By Lemma 5.2, a BH($\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}, h$) matrix exists. The desired array is constructed as in Lemma 5.3. \qed
References

[1] Physical Channels and Modulation (Release 13), document 3 GPP TS 36.211 V13.4.0, Jan. 2017.

[2] Global Positioning Systems Directorate Systems Engineering & Integration Interface Specification, document IS-GPS-200H, Mar. 2014.

[3] J. Backelin: Square multiples $n$ gives infinite many cyclic $n$-roots. Reports, Matematiska Institutionen, Stockholms Universitet, 8 (1989), 1 – 2.

[4] T. Beth, D. Jungnickel, H. Lenz: Design Theory (2nd edition), Cambridge University Press 1999.

[5] S. T. Blake, T. E. Hall, A. Z. Tirkel: Arrays over roots of unity with perfect autocorrelation and good ZCZ cross-correlation, Adv. Math. Commun. 7 (2013), 231 – 242.

[6] L. Bomer, M. Antweiler: Perfect N-phase sequences and arrays [spread spectrum communication], IEEE J. Sel. Areas Commun., 10 (1992), 782 – 789.

[7] Z. I. Borevich, I. R. Shafarevich: Number Theory, Academic Press, 1966.

[8] B. W. Brock: Hermitian congruence and the existence and completion of generalized Hadamard matrices, J. Combin. Theory Ser. A 49 (1988), 233 – 261.

[9] A. T. Butson: Generalized Hadamard Matrices, Proc. Amer. Math. Soc. 13 (1962), 894 – 898.

[10] J. H. Conway, A. J. Jones: Trigonometric diophantine equations (On vanishing sums of roots of unity) Acta Arithmetica (1976).

[11] W. de Launey: On the nonexistence of generalized weighing matrices, Ars Comn. 17 (1984), A, 117 – 132.

[12] T. D. Duc, B. Schmidt: Bilinear Forms on Finite Abelian Groups and Group-Invariant Butson Matrices, Submitted.
[13] T. D. Duc, K. H. Leung, B. Schmidt: Upper Bounds for Cyclotomic Numbers, Submitted.

[14] P. Z. Fan, M. Darnell: Sequence Design for Communications Applications. Hoboken, NJ, USA: Wiley, 1996.

[15] T. Feng, K. H. Leung, B. Schmidt, K. W. Smith: Hadamard difference sets related to Lander’s conjecture, J. Alg. 403 (2014) 29 – 47.

[16] S. W. Golomb, G. Gong: Signal Design for Good Correlation: For Wireless Communication, Cryptography and Radar. New York, NY, USA: Cambridge Univ. Press, 2005.

[17] G. Hiranandani, J. M. Schlenker: Small circulant complex Hadamard matrices of Butson type, Eur. J. Com. 51 (2016), 306 – 314.

[18] T. Y. Lam, K. H. Leung: On vanishing sums of roots of unity, J. Algebra 224 1 (2000), 91 – 109.

[19] K. H. Leung, B. Schmidt: Nonexistence Results on Generalized Bent Functions \( \mathbb{Z}_m \rightarrow \mathbb{Z}_q \) with odd \( m \) and \( q \equiv 2 \pmod{4} \), Preprint.

[20] K. H. Leung, B. Schmidt: The anti-field-descent method, J. Combin. Theory Ser. A 139 (2016), 87 – 131.

[21] S. L. Ma: Polynomial addition sets. Ph.D. thesis, University of Hong Kong, 1985.

[22] S. L. Ma, W. S. Ng: On non-existence of perfect and nearly perfect sequences, Int. J. Inform. Coding Theory, 1 (2009), 15 – 38.

[23] W. H. Mow: A new unified construction of perfect root-of-unity sequences, Proc. IEEE 4th Int. Symp. Spread Spectr. Techn. Appl., 3 (1996), 955 – 959.

[24] H.J. Ryser: Combinatorial Mathematics. Wiley, New York 1963.

[25] B. Schmidt: A Survey of Group Invariant Butson Matrices and Their Relation to Generalized Bent Functions and Various Other Objects.
[26] B. Schmidt: *Characters and Cyclotomic Fields in Finite Geometry*, Lecture Notes in Mathematics, 1797, Springer-Verlag, Berlin 2002.

[27] B. Schmidt: Cyclotomic integers and finite geometry. *J. Am. Math. Soc.* 12 (1999), 929 – 952.