A Survey of Group Invariant Butson Matrices and Their Relation to Generalized Bent Functions and Various Other Objects

Bernhard Schmidt
Division of Mathematical Sciences
School of Physical & Mathematical Sciences
Nanyang Technological University
Singapore 637371
Republic of Singapore

January 9, 2019

Abstract

This survey concerns the following closely related concepts.

- Group invariant Butson matrices,
- generalized bent functions,
- cyclic n-roots,
- generalized Hadamard matrices,
- abelian splitting semiregular difference sets.

We explain the connections between these notions and show that group invariant Butson matrices can be viewed as their "common denominator". We also review the most relevant known results on these objects, some of which are quite recent.

1 Introduction

The notions of group invariant Butson and generalized Hadamard matrices, bent functions, cyclic n-roots, and abelian semiregular relative difference sets are closely related. In fact, they have a "common denominator", which is *group invariant Butson matrices*. Bent functions, group invariant generalized Hadamard matrices, and abelian semiregular relative difference sets are all either equivalent to group invariant Butson matrices or to group invariant Butson matrices with additional properties. The first purpose of this survey is to explain these connections and to provide a general framework and notation for their discussion. The second purpose is to review some "old" results in the light of this framework. The final purpose is to survey some more recent results on generalized Bent functions and group and group invariant Butson matrices, which seems appropriate, as this area has been quite active over the last decade.

We will start our discussion with the definition of group invariant Butson matrices in the following section and deal with their relations to the other notions subsequently.

We first fix some notation and basics we will use throughout this paper. For a positive integer a, write $\zeta_a = \exp(2\pi i/a)$ and let U_a denote the set of ath roots of unity in $\mathbb{C}$, i.e.,

$$U_a = \{\zeta_a^j : j = 0, \ldots, a-1\}.$$

The cyclic group of order a is denoted by $\mathbb{Z}_a$ and we identify $\mathbb{Z}_a$ with $\{0, \ldots, a-1\}$, the group operation being addition of integers modulo a.

For a prime p and an integer t, let $\nu_p(t)$ denote the p-adic valuation of t, that is, $p^{\nu_p(t)}$ is the largest power of p dividing t. For groups K and W, we say that K has a **direct factor W** if $K \cong W \times V$ for some group V.

Let G be a multiplicatively written finite abelian group (we use multiplicative notation in this section, as this is standard when group rings are used, but we will switch to additive notation in the remaining sections). Let $\exp(G)$ denote the least common multiple of the orders the elements of G.

A $|G| \times |G|$ matrix $A = (a_{g,k})_{g,k \in G}$ is called ***G*-invariant** (or just **group invariant**) if $a_{gl,kl} = a_{g,k}$ for all $g, k, l \in G$.

Let R be a ring and let $R[G]$ denote the group ring of G over R. The elements of $R[G]$ have the form $X = \sum_{g \in G} a_g g$ with $a_g \in R$. The a_g's are called the **coefficients** of X. Two elements $X = \sum_{g \in G} a_g g$ and $Y = \sum_{g \in G} b_g g$ in $R[G]$ are equal if and only if $a_g = b_g$ for all $g \in G$. A subset S of G is identified with the group ring element $\sum_{g \in S} g$. For the identity element 1_G of G and $\lambda \in R$, we write λ for the group ring element $\lambda 1_G$. For $R = \mathbb{Z}[\zeta_h]$ and $X = \sum_{g \in G} a_g g \in \mathbb{Z}[\zeta_h][G]$, we write

$$X^{(-1)} = \sum_{g \in G} \overline{a_g} g^{-1},$$

where $\overline{a_g}$ denotes the complex conjugate of a_g.

The group of complex characters of G is denoted by $\hat{G}$. The **trivial character** χ_0 is defined by $\chi_0(g) = 1$ for all $g \in G$. The **order** of a character χ is the smallest positive integer e such that $\chi(g)^e = 1$ for all $g \in G$. For $D = \sum_{g \in G} a_g g \in R[G]$ and $\chi \in \hat{G}$, write $\chi(D) = \sum_{g \in G} a_g \chi(g)$. The following is a standard result and a proof can be found [3, Ch. VI], for instance.

Result 1.1. *Let G be a finite abelian group and $D = \sum_{g \in G} a_g g \in \mathbb{C}[G]$. Then*

$$a_g = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(Dg^{-1})$$

for all $g \in G$. Consequently, if $D, E \in \mathbb{C}[G]$ and $\chi(D) = \chi(E)$ for all nontrivial characters χ of G, then $D = E + \alpha G$ for some $\alpha \in \mathbb{C}$. Furthermore, $\chi(G) = 0$ for every nontrivial character χ of G.

2 Connection Between Group Invariant Butson Matrices and Other Notions

In this section, we clarify the connection between group invariant Butson matrices and the other objects mentioned in the introduction. We start with the definition and characterization of group invariant Butson matrices.

2.1 Group Invariant Butson Matrices

Let h be a positive integer. An $n \times n$-matrix H with entries from U_h 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 say that H is a $\mathbf{BH(}\boldsymbol{n, h}\mathbf{)}$ matrix. If H is a G-invariant $\mathrm{BH}(|G|, h)$ matrix for some group G, then H is said to be a $\mathbf{BH(}\boldsymbol{G, h}\mathbf{)}$ **matrix**.

The next result is from [8]. We include a proof for the convenience of the reader.

Lemma 2.1. *Let G be a finite abelian group, let h be a positive integer, and let a_g, $g \in G$, be complex hth root of unity. Consider the element $D = \sum_{g\in G} a_g g$ of $\mathbb{Z}[\zeta_h][G]$ and the G-invariant matrix $H = (H_{g,k})$, $g, k \in G$ given by $H_{g,k} = a_{g-k}$. Then H is a $\mathrm{BH}(G, h)$ matrix if and only if*

$$DD^{(-1)} = |G|. \tag{1}$$

Moreover, (1) holds if and only if

$$|\chi(D)|^2 = |G| \text{ for all } \chi \in \hat{G}. \tag{2}$$

Proof. Let $g \in G$ be arbitrary. The coefficient of g in $DD^{(-1)}$ is

$$\sum_{\substack{k,l\in G \\ k-l=g}} a_k \overline{a_l} = \sum_{l\in G} a_{l+g}\overline{a_l}.$$

On the other hand, the inner product of row $x + g$ and row x of H is

$$\sum_{k\in G} H_{x+g,k}\overline{H_{x,k}} = \sum_{k\in G} a_{x+g-k}\overline{a_{x-k}} = \sum_{l\in G} a_{l+g}\overline{a_l}$$

Hence (1) holds if and only if any two distinct rows of H have inner product 0, that is, if and only if H is a $\mathrm{BH}(G, h)$ matrix. Finally, the equivalence of (1) and (2) follows from Result 1.1. □

2.2 Generalized Bent Functions

The term "bent function" has been used with various meanings in the literature. We use the most general natural extension of the original version of

"bent functions" studied by Rothaus [22, 23]. Let q, m, h be positive integers. A function $f : \mathbb{Z}_q^m \to \mathbb{Z}_h$ is called a **generalized bent function (GBF)** if

$$\left| \sum_{x \in \mathbb{Z}_q^m} \zeta_h^{f(x)} \zeta_q^{-vx^T} \right|^2 = q^m \text{ for all } v \in \mathbb{Z}_q^m. \tag{3}$$

Here vx^T denotes the usual dot product, that is, $vx^T = \sum_{i=1}^m v_i x_i$ for $v = (v_1, \ldots, v_m)$ and $x = (x_1, \ldots, x_m)$.

Remark 2.2. *Suppose that a GBF $f : \mathbb{Z}_q^m \to \mathbb{Z}_h$ exists and that k is a multiple of h. Then there is a GBF $\mathbb{Z}_q^m \to \mathbb{Z}_k$.*

Indeed, the function g given by $g(x) = (k/h)f(x)$ for all $x \in \mathbb{Z}_q^m$ is a GBF.

The following shows that GBFs are a special kind of group invariant Butson matrices.

Proposition 2.3. *Let q, m, h be positive integers, and let $f : \mathbb{Z}_q^m \to \mathbb{Z}_h$ be a function. Then f is a GBF if and only if the element*

$$D := \sum_{x \in \mathbb{Z}_q^m} \zeta_h^{f(x)} x$$

of $\mathbb{Z}[\zeta_h][\mathbb{Z}_q^m]$ defines a $\mathrm{BH}(\mathbb{Z}_q^m, h)$ matrix via Lemma 2.1.

Proof. Write $G = \mathbb{Z}_q^m$. Let $v \in G$ and consider the map

$$\chi_v : G \to \mathbb{C}, \ x \mapsto \zeta_q^{-vx^T}.$$

Note that $\chi_v(x + y) = \chi_v(x)\chi_v(y)$ for all $x, y \in G$. Thus χ_v is a character of G. Moreover, it is easy to check that $\chi_v \neq \chi_w$ whenever $v \neq w$. As $|\hat{G}| = |G|$, we conclude

$$\hat{G} = \{\chi_v : v \in G\} \tag{4}$$

Note that

$$\chi_v(D) = \sum_{x \in G} \zeta_h^{f(x)} \chi_v(x) = \sum_{x \in G} \zeta_h^{f(x)} \zeta_q^{-vx^T}. \tag{5}$$

By (2), (4), and (5), we indeed have that f is a GBF if and only if D defines a $\mathrm{BH}(\mathbb{Z}_q^m, h)$ matrix. □

2.3 Cyclic n-Roots

Cyclic n-roots were introduced by Björck [4] in 1989 and provide an alternative approach to Butson matrices invariant under cyclic groups. The main construction of cyclic n-roots was obtained by Backelin [2] in the same year, but it seems that later quite a number of researchers working on equivalent problems were not aware of Backelin's result, with the effect that his construction or special cases of it were rediscovered in some publications.

Let n be a positive integer. A vector $(z_0, \ldots, z_{n-1})^T \in \mathbb{C}^n$ is called a **cyclic n-root** if it satisfies the following system of equations

$$\begin{aligned} z_0 + z_1 + \cdots + z_{n-1} &= 0 \\ z_0z_1 + z_1z_2 + \cdots + z_{n-1}z_0 &= 0 \\ z_0z_1z_2 + z_1z_2z_2 + \cdots + z_{n-1}z_0z_1 &= 0 \\ \vdots \qquad\qquad & \qquad \vdots \\ z_0z_1\cdots z_{n-2} + z_1z_2\cdots z_{n-1} + \cdots + z_{n-1}z_0\cdots z_{n-3} &= 0 \\ z_0z_1\cdots z_{n-1} &= 1. \end{aligned} \tag{6}$$

For $(x_0, \ldots, x_{n-1})^T \in \mathbb{C}^n$ with $x_i \neq 0$ for all i, we define a corresponding vector $(z_0, \ldots, z_{n-1})^T \in \mathbb{C}^n$ by

$$z_i = \frac{x_i}{x_{i+1}} \text{ for } i = 1, \ldots, n-1, \tag{7}$$

where the indices are taken modulo n. Note that $z_0z_1\cdots z_{n-1} = (x_0/x_1)\cdots(x_{n-1}/x_0) = 1$. Using (7), we see that (6) holds if and only if

$$\begin{aligned} \frac{x_1}{x_0} + \frac{x_2}{x_1} + \cdots + \frac{x_0}{x_{n-1}} &= 0 \\ \frac{x_2}{x_0} + \frac{x_3}{x_1} + \cdots + \frac{x_1}{x_{n-1}} &= 0 \\ \frac{x_3}{x_0} + \frac{x_4}{x_1} + \cdots + \frac{x_2}{x_{n-1}} &= 0 \\ \vdots \qquad\qquad & \qquad \vdots \\ \frac{x_{n-1}}{x_0} + \frac{x_0}{x_1} + \cdots + \frac{x_{n-2}}{x_{n-1}} &= 0. \end{aligned} \tag{8}$$

Recall that U_h denotes the set of complex hth roots of unity. The following clarifies the connection between cyclic n-roots and Butson matrices.

Proposition 2.4. *Let n and h be a positive integers and let $x_0, \ldots, x_{n-1} \in U_h$. Let g be a generator of $\mathbb{Z}_n$. Then $D = \sum_{i=0}^{n-1} x_i g^i$ defines a $\mathrm{BH}(\mathbb{Z}_n, h)$ matrix if and only if the vector $(z_0, \ldots, z_{n-1})^T$ given by (7) is a cyclic n-root.*

Proof. Note the $\overline{x} = 1/x$ for all $x \in U_n$. The coefficient of g^i in $DD^{(-1)}$ is

$$\sum_{\substack{j,k=0 \\ j-k=i}}^{n-1} x_j \overline{x_k} = \sum_{j=0}^{k-1} x_{i+k} \overline{x_k} = \sum_{j=0}^{n-1} \frac{x_{i+k}}{x_k},$$

where the indices are take modulo n. Hence $DD^{(-1)} = n$ if and only if $\sum_{j=0}^{k-1} x_{i+k}/x_k = 0$ for $i = 1, \ldots, n-1$, that is, if and only if (8) holds. Moreover, by Lemma 2.1, we have $DD^{(-1)} = n$ if and only if D defines a $\mathrm{BH}(\mathbb{Z}_n, h)$ matrix. This completes the proof, since (8) holds if and and only if the vector $(z_0, \ldots, z_{n-1})^T$ given by (7) is a cyclic n-root. □

2.4 Generalized Hadamard Matrices

Let K be a finite abelian group and let n be a positive integer. An $n \times n$ matrix $H = (H_{ij})$ with entries from K is called a **generalized Hadamard matrix** if there is a positive integer λ such that

$$\sum_{j=1}^{n} H_{ij} {H_{kj}}^{-1} = \lambda K \tag{9}$$

in $\mathbb{Z}[K]$ for all i, k with $i \neq k$. We also say that H is a $\mathbf{GH(\boldsymbol{n}, \boldsymbol{K})}$ **matrix**.

Proposition 2.5. *Let K be a finite abelian group and let n be a positive integer. Write $h = \exp(K)$. Suppose that $H = (H_{ij})$ is a matrix with entries from K. Then H is a $\mathrm{GH}(n, K)$ matrix if and only if $(\chi(H_{ij}))$ is a $\mathrm{BH}(n, h)$ matrix for all nontrivial characters χ of K.*

Proof. Suppose that $(\chi(H_{ij}))$ is a $\mathrm{BH}(n, h)$ matrix for all nontrivial characters χ of K. We have to show that H is a $\mathrm{GH}(n, K)$ matrix. Let i, k be arbitrary with $1 \leq i, k \leq n$ and $i \neq k$. We have to prove that (9) holds. For every nontrivial character χ of K, we have

$$\chi\left(\sum_{j=1}^{n} H_{ij} {H_{kj}}^{-1}\right) = \sum_{j=1}^{n} \chi(H_{ij}) \overline{\chi(H_{kj})} = 0, \tag{10}$$

since $(\chi(H_{ij}))$ is a $\mathrm{BH}(n,h)$ matrix by assumption. By Result 1.1 and (10), we have

$$\sum_{j=1}^{n} H_{ij}{H_{kj}}^{-1} = \lambda K$$

for some $\lambda \in \mathbb{C}$. Applying the trivial character of K to this equation, we conclude that $|K|$ divides n and that $\lambda = n/|K|$. This shows that H is a $\mathrm{GH}(n,K)$ matrix.

Conversely, if H is a $\mathrm{GH}(n,K)$ matrix and χ is a nontrivial character of K, then

$$\sum_{j=1}^{n} \chi(H_{ij})\overline{\chi(H_{kj})} = \chi\left(\sum_{j=1}^{n} H_{ij}{H_{kj}}^{-1}\right) = \lambda\chi(K) = 0$$

by (9) and Result 1.1. Hence $(\chi(H_{ij}))$ is a $\mathrm{BH}(n,h)$ matrix. □

Corollary 2.6. *Let p be a prime and let n be a positive integer. Every $\mathrm{GH}(n,\mathbb{Z}_p)$ matrix B uniquely corresponds to a $\mathrm{BH}(n,p)$ matrix A. Moreover, A is G-invariant for an abelian group G if and only if B is G-invariant.*

Proof. If a $\mathrm{GH}(n,\mathbb{Z}_p)$ matrix exists, then there is a $\mathrm{BH}(n,p)$ matrix by Proposition 2.5. To prove the converse, suppose that a $\mathrm{BH}(n,p)$ matrix $A = (A_{ij})$ exists. Write $A_{ij} = \zeta_p^{a_{ij}}$ with $a_{ij} \in \mathbb{Z}$. Let g be a generator of $\mathbb{Z}_p$ and set $B_{ij} = g^{a_{ij}}$. Obviously, $B = (B_{ij})$ is G-invariant if and only if A is G-invariant. Let χ be the character of $\mathbb{Z}_p$ with $\chi(g) = \zeta_p$. Then $(\chi(B_{ij})) = A$ is a $\mathrm{BH}(n,p)$ matrix. Let τ be any nontrivial character of $\mathbb{Z}_p$. Then there is automorphism σ of $\mathbb{Q}(\zeta_p)$ with $\tau(g) = \sigma(\chi(g))$ for all $g \in G$. Since the property of being a $\mathrm{BH}(n,p)$ matrix is preserved under such automorphisms, this shows that $(\tau(B_{ij}))$ is a $\mathrm{BH}(n,p)$ matrix for all nontrivial characters τ of $\mathbb{Z}_p$. Hence (B_{ij}) is a $\mathrm{GH}(n,\mathbb{Z}_p)$ matrix by Proposition 2.5. □

2.5 Abelian Splitting Semiregular Relative Difference Sets

Let M and N be finite abelian groups, write $m = |M|$, $n = |N|$, and assume that n divides m. An m-subset R of $G = M \times N$ is called an $\boldsymbol{(m,n,m,m/n)}$

relative difference set if

$$RR^{(-1)} = m + \frac{m}{n}(G - N), \tag{11}$$

that is, if each element of $G \backslash N$ has exactly m/n representations as a quotient of two elements of R and no nonidentity element of N has such a representation. Alternatively, we say that R is a **difference set in G relative to N**. Such a relative difference set is called **abelian** (as G is abelian), **splitting** (as N is a direct factor of G), and **semiregular** (this refers the fact that $|R| = |G|/|N|$).

Note that no coset of N in G contains more than one element of R by (11). Hence R meets every coset of N in G in exactly one element and we can write

$$R = \sum_{g \in M} n_g g \tag{12}$$

with $n_g \in N$. Set $e = \exp(N)$. For every character χ of N, we define a map

$$\rho_\chi : \mathbb{Z}[G] \to \mathbb{Z}[\zeta_e][M]$$

by $\rho_\chi(h) = \chi(h)$ for $h \in N$, $\rho_\chi(g) = g$ for $g \in M$, and extension to $\mathbb{Z}[G]$ by linearity. Note that $\rho_\chi(R) = \sum_{g \in M} \chi(n_g) g$.

Proposition 2.7. *Let M and N be finite abelian groups, write $m = |M|$, $n = |N|$, and assume that n divides m. Let R be a subset of G that meets every coset of N in G in exactly one element and write $R = \sum_{g \in M} n_g g$ as in (12). Then R is an $(m, n, m, m/n)$ relative difference set in G if and only if, for every nontrivial character χ of N, the element*

$$\rho_\chi(R) = \sum_{g \in M} \chi(n_g) g$$

of $\mathbb{Z}[\zeta_e][M]$ defines a $\mathrm{BH}(M, e)$ matrix via Lemma 2.1.

Proof. Suppose that R is an $(m, n, m, m/n)$ relative difference set. Then

$$|\tau(R)|^2 = m \tag{13}$$

for every character τ of G which in nontrivial on N by (11). Let χ be any fixed nontrivial character of N, and let ψ be any character of M. Define a

corresponding character $\psi \otimes \chi$ of G by $\psi \otimes \chi(gh) = \psi(g)\chi(h)$ for all $g \in M$ and $h \in N$. Then $\psi \otimes \chi$ is nontrivial on N and thus

$$|\psi(\rho_\chi(R))|^2 = \left|\sum_{g \in M} \chi(n_g)\psi(g)\right|^2 = |\psi \otimes \chi(R)|^2 = m$$

by (13). By Lemma 2.1, this shows that $\rho_\chi(R)$ is a BH(M, e) matrix.

Conversely, if $\rho_\chi(R)$ defines a BH(M, e) matrix for every nontrivial character χ of N, we similarly can use Lemma 2.1 to show that $|\tau(R)|^2 = m$ for all characters τ of G that are nontrivial on N. Moreover, we have $\tau(R) = \sum_{g \in M} \tau(g)$ for all characters τ of G that are trivial on N, but nontrivial on G. Finally, we have $\chi_0(R) = |R| = m$ for the trivial character χ_0 of G. In summary, we have shown that

$$\tau(RR^{(-1)}) = \tau\left(m + (m/n)(G - N)\right)$$

for all characters τ of G. By Lemma 1.1, we conclude that (11) holds, i.e., R is an $(m, n, m, m/n)$ relative difference set, as required. □

3 Review of Some "Old" Results

In this section, we review some "old" results from the perspective presented in the previous section. In the corollaries, we describe what these results mean in terms of group invariant Butson matrices.

Result 3.1 (Rothaus [22, 23])**.** *A GBF $\mathbb{Z}_2^m \to \mathbb{Z}_2$ exists if and only if m is even.*

Corollary 3.2. *There is a* BH$(\mathbb{Z}_2^m, 2)$ *matrix if and only if m is even.*

Proof. This follows from Proposition 2.3 and Result 3.1. □

Result 3.3 (Jungnickel [15])**.** *Let p be an odd prime and let G be an elementary abelian group of order p^{a+b}, where a and b are positive integers with $b \leq a$. For every subgroup N of G order order p^b, there exists a (p^a, p^b, p^a, p^{a-b}) difference set in G relative to N.*

Corollary 3.4. *Let p be an odd prime and let G be an elementary abelian p-group G. Then there exists a* $\mathrm{BH}(G, p)$ *matrix.*

Proof. This follows from Proposition 2.7 and Result 3.3. □

In particular, there exists a circulant $\mathrm{BH}(p, p)$ matrix for every odd prime p (this special case of Result 3.3 already was obtained by Butson [6]).

In fact, there are many other groups of prime power order that contain abelian splitting relative difference sets and thus provide group invariant Butson matrices. The work of Davis and Jedwab [7] contains a complete list of such groups known to contain relative difference sets.

Result 3.5 (Kumar, Scholtz, Welch [16])**.** *Let q and m be positive integers. A generalized bent function from $\mathbb{Z}_q^m$ to $\mathbb{Z}_q$ exists whenever m is even or $q \not\equiv 2 \pmod 4$.*

Corollary 3.6. *Let q and m be positive integers. A* $\mathrm{BH}(\mathbb{Z}_q^m, q)$ *matrix exists whenever m is even or $q \not\equiv 2 \pmod 4$.*

Proof. This follows from Proposition 2.3 and Result 3.5. □

In particular, a circulant $\mathrm{BH}(q, q)$ exists for all positive integers q with $q \not\equiv 2 \pmod 4$.

Result 3.7 (Backelin [2])**.** *Let $n \not\equiv 2 \pmod 4$ be a positive integer and assume that n is divisible by r^2 for some integer $r > 1$. Then there is a cyclic n-root $(z_0, \ldots, z_{n-1})^T$ with $z_i \in U_{n/r}$ for all i.*

We remark that the condition $n \not\equiv 2 \pmod 4$ is necessary for Backelin's result to hold, but is missing in his paper.

Corollary 3.8. *Let $n \not\equiv 2 \pmod 4$ be a positive integer which is divisible by r^2 for some integer $r > 1$. Then there is a (circulant)* $\mathrm{BH}(\mathbb{Z}_n, n/r)$ *matrix.*

Proof. This follows from Proposition 2.4 and Result 3.7. □

By Corollary 3.8, there is a $\mathrm{BH}(\mathbb{Z}_{p^2}, p)$ matrix for every prime p. Hence, by Corollary 2.6, there is a circulant $\mathrm{GH}(p^2, p)$ for all primes p. This special case of Backelin's result was rediscovered in [9].

Result 3.9 (Brock [5], Winterhof [29]). *Suppose that n is a positive integer and p is a prime divisor of n such that*

(i) $\nu_p(n)$ *is odd,*

(ii) p *does not divide* h*,*

(iii) $p^j \equiv -1 \pmod{n}$ *for some positive integer* j*.*

Then there is no $\mathrm{BH}(n,h)$ *matrix.*

4 Survey of Some Recent Results

4.1 Constructions

Result 4.1 (K.-U. Schmidt [25]). *A GBF* $\mathbb{Z}_2^m \to \mathbb{Z}_4$ *exists for all positive integers* m*.*

We remark that a proof of Result 4.1 is also contained in [27].

Next, we describe a construction of group invariant Butson matrices based on bilinear forms on finite abelian groups. Let G be a finite abelian group and let e be a positive integer. We say that a map $f : G \times G \to \mathbb{Z}_e$ is a **bilinear form** if

$$\begin{aligned} f(g+h,k) &= f(g,k) + f(h,k) \text{ and} \\ f(g,h+k) &= f(g,h) + f(g,k) \end{aligned} \tag{14}$$

for all $g,h,k \in G$. Note that (14) implies

$$\begin{aligned} f(\alpha g,k) &= \alpha f(g,h) \text{ and} \\ f(g,\alpha h) &= \alpha f(g,h) \end{aligned}$$

for all $g,h \in G$ and $\alpha \in \mathbb{Z}$. If $f(g,h) = f(h,g)$ for all $g,h \in G$, then f is **symmetric**. If $f(g,h) = 0$, then g and h are said to be **orthogonal**. We say that f is **nondegenerate** if there is no $g \in G \setminus \{0\}$ such that $f(g,h) = 0$ for all $h \in G$. In the following, the elementary abelian group of order 2^c is identified with $\{(g_1,\ldots,g_{2^c}) : g_i \in \{0,1\}\}$.

For an abelian group G and $g \in G$, we say that $h \in G$ is a **square root** of g if $g = 2h$ and we write $h = g/2$.

Result 4.2 (Duc, Schmidt [8]). *Let K be a finite abelian group and write $e = \exp(G)$ and $K = G \times L$, where either $L = \{0\}$ or L is an elementary abelian 2-group. Let a, d be any nonnegative integers such that $|L| = 2^{2a+d}$ and write $c = 2a + d$. Let $F : (\mathbb{Z}_2)^{2a} \to \mathbb{Z}_2$ be a GBF and set*

$$s_L(g_1, \ldots, g_c) = 2F(g_1, \ldots, g_{2a}) + \sum_{i=2a+1}^{c} g_i$$

for $(g_1, \ldots, g_c) \in L$.

Let U be a subgroup of G such that every element of U has a square root in G. Suppose that $f : G \times G \to \mathbb{Z}_e$ is bilinear, symmetric, and nondegenerate, and that no element of $G \setminus U$ is orthogonal to all elements of U. Let $R \subset G$ be a complete system of coset representatives of U in G with $0 \in R$. For every $x \in K$, there are unique $x_1 \in U$, $x_2 \in R$, and $x_3 \in L$ with $x = x_1 + x_2 + x_3$. Let β be any integer coprime to $|G|$. Define a matrix $H = (H_{y,x})_{y,x \in K}$ by

$$H_{y,x} = \zeta_e^{f((x-y)_1/2,(x-y)_1)+\beta f((x-y)_1,(x-y)_2)} \zeta_4^{s_L(x_3+y_3)}. \tag{15}$$

Then H is a $\mathrm{BH}(K, e_1)$ matrix, where

$$e_1 = \begin{cases} \exp(U) & \text{if } L = \{0\}, \\ \mathrm{lcm}(2, \exp(U)) & \text{if } L \text{ is of square order}, \\ \mathrm{lcm}(4, \exp(U)) & \text{otherwise.} \end{cases}$$

Result 4.2 can be used to prove the following.

Corollary 4.3 (Duc, Schmidt [8]). *Let K be a finite abelian group and let h be a positive integer such that*

$$v_p(h) \geq \lceil v_p(\exp(K))/2 \rceil \text{ for every prime divisor } p \text{ of } |K|, \tag{16}$$

$$\nu_2(h) \geq 2 \text{ if } \nu_2(|K|) \text{ is odd and } K \text{ has a direct factor } \mathbb{Z}_2. \tag{17}$$

Then there exists a $\mathrm{BH}(K, h)$ matrix.

Applied to circulant Butson matrices, Corollary 4.3 gives the next result.

Corollary 4.4 (Duc, Schmidt [8]). *If v and h are positive integers with*

(i) $v_p(h) \geq \lceil v_p(v)/2 \rceil$ for every prime divisor p of v and

(ii) $\nu_2(h) \geq 2$ if $v \equiv 2 \pmod 4$,

then a (circulant) $\mathrm{BH}(\mathbb{Z}_v, h)$ matrix exists.

4.2 Necessary Conditions

Recently, necessary conditions for the existence of generalized bent functions (GBFs) have been studied quite intensively [1, 10, 11, 13, 14, 18, 19, 20, 21]. We provide an (incomplete) overview of this work here. Recall that GBFs $\mathbb{Z}_q^m \to \mathbb{Z}_q$ exist whenever m is even or $q \not\equiv 2 \pmod 4$. Hence all necessary conditions for the existence of GBFs concern the case where m is odd and $q \equiv 2 \pmod 4$.

Definition 4.5. Let p be a prime, let m be a positive integer, and write $m = p^a m'$ with $(p, m') = 1$, $a \geq 0$. If there is an integer j with $p^j \equiv -1 \pmod{m'}$, then p is called *self-conjugate modulo* m. A composite integer n is called self-conjugate modulo m if every prime divisor of n has this property.

Result 4.6 ([1, 13, 16, 21])**.** *Suppose that there is a GBF from $\mathbb{Z}_q^m$ to $\mathbb{Z}_q$, where $q = 2r$ and r is an odd integer. Then 2 is not self-conjugate modulo r. Moreover, if $m = 1$, then r is not self-conjugate modulo r. In particular, if $m = 1$, then r is not a prime power.*

There are quite a number of further necessary conditions known for the existence of GBFs, most of which concern GBFs from $\mathbb{Z}_{2r}^m$ to $\mathbb{Z}_{2r}$ where r is the product of two prime powers. We do not state them here, however, since a nice overview of these results is given in [14].

Result 4.7 (Liu, Feng, Feng [19])**.** *Let m and h be odd positive integers, let a be a positive integer, and let p be an odd prime.*

- *There is no GBF $\mathbb{Z}_2^m \to \mathbb{Z}_{p^a}$.*
- *If*
  (i) $p \equiv 3$ or $5 \pmod 8$ or
  (ii) $p \equiv 1 \pmod 8$ and $\mathrm{ord}_p(2)$ is even,

  then there is no GBF $\mathbb{Z}_2^m \to \mathbb{Z}_{2p^a}$.
- *If 2 is self-conjugate modulo h, then there is no GBF $\mathbb{Z}_2^m \to \mathbb{Z}_h$ and no GBF $\mathbb{Z}_2^m \to \mathbb{Z}_{2h}$.*

We note that [19] contains further, more technical, necessary conditions for existence of GBFs.

Coming back to the construction of Butson matrices using bilinear forms, it turns out that, for prime powers v, the conditions in Corollary 4.4 are in fact necessary for the existence of a $\mathrm{BH}(\mathbb{Z}_v, h)$ matrix:

Theorem 4.8 (Duc, Schmidt [8]). *Let v be a power of a prime p and let h be a positive integer. A (circulant) $\mathrm{BH}(\mathbb{Z}_v, h)$ matrix exists if and only if*

$$v_p(h) \geq \lceil v_p(v)/2 \rceil \text{ and } (v, h) \neq (2, 2). \tag{18}$$

Finally, we list the main results of [18].

Result 4.9 (Leung, Schmidt [18]). *Let m be an odd positive integer, let p be an odd prime, and suppose that a GBF from $\mathbb{Z}_{2p^a}^m$ to $\mathbb{Z}_{2p^a}$ exists. Then the following hold.*

- $p \leq 2^{2m} + 2^m + 1$.
- $\mathrm{ord}_p(2)$ *is even and* $\mathrm{ord}_p(2) \leq 2^{m-1}$.
- *If* $m \geq 7$, *then* $p \leq 2^{2m}/9$ *or* $\mathrm{ord}_p(2) \leq (2^m + 3)/5$.
- *If* $m = 3$, *then* $p = 7$.
- *If* $m = 5$, *then* $p \in \{7, 23, 31, 73, 89\}$.
- *If* $m = 7$, *then* $p \in \{7, 23, 31, 47, 71, 73, 79, 89, 103, 223, 233, 337, 431, 601, 631, 881, 1103, 1801\}$.

References

[1] E. Akyildiz, I. S. Güloglu, M. Ikeda: A note of generalized bent functions. *J. Pure Appl. Algebra* **106** (1996), 1–9.

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

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

[4] G. Björck: *Fourier transforms and cyclic p-roots*. Reports No. 9, Matematiska Institute, Stockholms Universitet, 1989.

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

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

[7] J.A. Davis and J. Jedwab: A unifying construction of difference sets. *J. Combin. Theory A* **80** (1997), 13–78.

[8] T. D. Duc, B. Schmidt: Bilinear Forms on Finite Abelian Groups and Group-Invariant Butson Matrices. Submitted.

[9] W. de Launey: Circulant $GH(p^2, \mathbb{Z}_p)$ Exist for All Primes p. *Graphs Comb.* **8** (1992), 317–321.

[10] K. Feng: Generalized bent functions and class group of imaginary quadratic fields. *Sci. China Ser. A* **44** (2001), 562–570.

[11] K. Feng, F. Liu: New Results on the Nonexistence of Generalized Bent Functions. *IEEE Trans. Inf. Theory* **49** (2003), 3066–3071.

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

[13] M. Ikeda: A remark on the non-existence of generalized bent functions. *Lect. Notes Pure Appl. Math.* **204** (1999), 109–119.

[14] Y. Jiang, Y. Deng: New results on nonexistence of generalized bent functions. *Des. Codes Cryptogr.* **75** (2015), 375–385.

[15] D. Jungnickel: On automorphism groups of divisible designs. *Canadian J. Math.* **34**, 257–297.

[16] P. V. Kumar, R. A. Scholtz, L. R. Welch: Generalized bent functions and their properties. *J. Combin. Theory Ser. A* **40** (1985), 90–107.

[17] P. H. J. Lampio, P. Östergård, F. Szöllősi: Orderly generation of Butson Hadamard matrices. Preprint. `arXiv:1707.02287`.

[18] K. H. Leung, B. Schmidt: Nonexistence Results on Generalized Bent Functions $\mathbb{Z}_q^m \to \mathbb{Z}_q$ with Odd m and $q \equiv 2 \pmod 4$. Submitted.

[19] H. Liu, K. Feng, R. Feng: Nonexistence of generalized bent functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_m$. *Des. Codes Cryptogr.* **82** (2017), 647–662.

[20] F. Liu, Z. Ma Z, K. Feng K: New results on non-existence of generalized bent functions (II). *Sci. China A* **45** (2002), 721–730.

[21] D. Pei: On nonexistence of generalized bent functions. *Lect. Notes Pure Appl. Math.* **141** (1993), 165–172.

[22] O. S. Rothaus: On Bent Functions. Institute of Defense Analysis, USA, W. P. 169 (1966).

[23] O. S. Rothaus: On 'bent' functions. *J. Combin. Theory Ser. A* **20** (1976), 300–305.

[24] B. Schmidt: *Characters and Cyclotomic Fields in Finite Geometry*, Lecture Notes in Mathematics, 1797, Springer-Verlag, Berlin 2002.

[25] K.-U. Schmidt: Quaternery constant-amplitude codes for multicode CDMA. *IEEE Trans. Inform. Thoery* **55** (2009), 1824–1832.

[26] P. Sole, N. Tokareva: Connections between quaternary and binary bent functions. `https://eprint.iacr.org/2009/544.pdf`.

[27] R. Stanica, T. Martinsen, S. Gangopadhyay, B. K. Sing: Bent and generalized bent Boolean functions. *DesĊodes Cryptogr.* **69** (2013), 77–94.

[28] F. Szöllősi: *Construction, classification and parametrization of complex Hadamard matrices* Ph.D. Thesis. `arXiv:1110.5590`.

[29] A. Winterhof: On the non-existence of generalized Hadamard matrices. *J. Statist. Plann. Inference* **84** (2000), 337–342.