Cryptography and Communications (2024) 16:323–337
https://doi.org/10.1007/s12095-023-00657-z

RESEARCH

Generalized partially bent functions, generalized perfect arrays, and cocyclic Butson matrices

J. A. Armario[1] · R. Egan[2] · D. L. Flannery[3]

Received: 29 August 2022 / Accepted: 14 June 2023 / Published online: 23 August 2023
© The Author(s) 2023

Abstract
In a recent survey, Schmidt compiled equivalences between generalized bent functions, group invariant Butson Hadamard matrices, and abelian splitting relative difference sets. We establish a broader network of equivalences by considering Butson matrices that are cocyclic rather than strictly group invariant. This result has several applications; for example, to the construction of Boolean functions whose expansions are generalized partially bent functions, including cases where no bent function can exist.

Keywords Generalized bent functions · Butson Hadamard matrices · Generalized perfect arrays · Cocycles

Mathematics Subject Classification 15B34 · 05B20 · 94D05

1 Introduction

Let $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ be a Boolean function with n a positive integer, and set $F(v) = (-1)^{f(v)}$ for $v \in \mathbb{Z}_2^n$ (throughout, we view $\mathbb{Z}_t$ for an integer $t > 1$ as $\{0, 1, \ldots, t-1\}$ under addition modulo t). The Walsh–Hadamard transform $\hat{F}$ of F is defined by

$$\hat{F}(u) = \sum_{v \in \mathbb{Z}_2^n} (-1)^{u \cdot v} F(v),$$

✉ J. A. Armario
armario@us.es

R. Egan
ronan.egan@dcu.ie

D. L. Flannery
dane.flannery@universityofgalway.ie

[1] Departamento de Matemática Aplicada I, Universidad de Sevilla, Avda. Reina Mercedes s/n, 41012 Sevilla, Spain

[2] School of Mathematical Sciences, Dublin City University, Dublin, Ireland

[3] School of Mathematical and Statistical Sciences, University of Galway, Galway, Ireland

where $u \cdot v$ denotes the inner product $uv^\top$ of u and v. The Walsh–Hadamard transform is used to analyze cryptographic properties of Boolean functions. A Boolean function f is *bent* if $|\hat{F}(u)|$ is constant for all $u \in \mathbb{Z}_2^n$. Parseval's theorem (see, e.g., [5, (8.36), p. 322]) gives

$$\sum_{v \in \mathbb{Z}_2^n} \hat{F}(v)^2 = 2^{2n}.$$

Hence, f can be bent only if n is even. If the Walsh–Hadamard transform takes no more than one non-zero absolute value, then it is *plateaued*.

A bent function is so-called because it is as far from being linear as possible. However, bent functions are not balanced (another desirable cryptographic property), while plateaued functions can be balanced and have large nonlinearity. These highly non-linear functions offer a robust defence against linear cryptanalysis [6, Chapter 3].

Bent functions are equivalent to certain Hadamard matrices and difference sets; see, e.g., [11, Lemma 14.3.2] and [6, Corollary 3.30]. The concept has been generalized, yielding equivalences between associated objects. Indeed, our paper is inspired by Schmidt's survey [16], which describes equivalences between generalized bent functions, group invariant Butson Hadamard matrices, and splitting relative difference sets. There is also a connection to perfect arrays, not covered in [16].

We study how the aforementioned equivalences are affected when the property of being group invariant is broadened to *cocyclic development*. For example, a group-invariant Butson Hadamard matrix is a type of cocyclic matrix. As a consequence, we incorporate generalized partially bent functions [18], and construct a family of generalized partially bent functions with domain for which no generalized bent functions exist.

We now outline the paper. Preliminary definitions and results are given in Section 2. Section 3 is devoted to generalized perfect arrays and generalized partially bent functions. In Section 4, we prove the main theorem: a series of equivalences between cocyclic Butson Hadamard matrices, generalized perfect arrays, non-splitting relative difference sets, generalized plateaued functions, and generalized partially bent functions. (For certain parameters, the equivalences that we exhibit have those in [16] as special cases.) In Section 5 we give some examples illustrating the main theorem.

2 Background

We adopt the following definition from [16]. For integers $q, m, h > 0$, and ζ_k the complex k^{th} root of unity $\exp(2\pi\sqrt{-1}/k)$, a map $f : \mathbb{Z}_q^m \to \mathbb{Z}_h$ is a *generalized bent function (GBF)* if

$$\left| \sum_{x \in \mathbb{Z}_q^m} \zeta_h^{f(x)} \zeta_q^{-w \cdot x} \right|^2 = q^m \quad \forall\, w \in \mathbb{Z}_q^m,$$

$|z|$ as usual denoting the modulus of $z \in \mathbb{C}$. Thus, a GBF for $q = h = 2$ and even m is a bent function. For $h = q$, Kumar, Scholtz, and Welch [9] prove that GBFs exist if m is even or $q \not\equiv 2 \mod 4$. However, no GBF with $h = q$, m odd, and $q \equiv 2 \mod 4$ is known [10, p. 2].

A further generalization is relevant to our paper. If the values of

$$\left| \sum_{x \in \mathbb{Z}_q^m} \zeta_h^{f(x)} \zeta_q^{-w \cdot x} \right|^2$$

as w ranges over $\mathbb{Z}_q^m$ lie in $\{0, \alpha\}$ for a single non-zero α, then f is a *generalized plateaued function* (cf. the definition of plateaued Walsh–Hadamard transform). Mesnager, Tang, and Qi [14] discuss such functions under the conditions that q is prime and h is a q-power. They call f an *s-generalized plateaued function* when α has the form q^{m+s}.

We examine the role of GBFs and generalized plateaued functions in cocyclic design theory [3, 6]. Some requisite definitions follow. Let G and U be finite groups, with U abelian. A map $\psi : G \times G \to U$ such that

$$\psi(a, b)\psi(ab, c) = \psi(a, bc)\psi(b, c) \quad \forall\, a, b, c \in G$$

is a *cocycle* (*over G, with coefficients in U*). Cocycles ψ are assumed to be *normalized*, meaning that $\psi(1, 1) = 1$. For any (normalized) map $\phi : G \to U$, the cocycle $\partial\phi$ defined by $\partial\phi(a, b) = \phi(a)^{-1}\phi(b)^{-1}\phi(ab)$ is a *coboundary*. The set of cocycles $\psi : G \times G \to U$ equipped with pointwise multiplication is an abelian group, $Z^2(G, U)$. Factoring out $Z^2(G, U)$ by the subgroup $B^2(G, U)$ of coboundaries gives the *second cohomology group*, $H^2(G, U)$. The elements of $H^2(G, U)$, namely cosets of $B^2(G, U)$, are *cohomology classes*. Each $\psi \in Z^2(G, U)$ is displayed as a *cocyclic matrix* M_ψ. That is, under an indexing of rows and columns by the elements of G, the $|G| \times |G|$ matrix M_ψ has entry $\psi(a, b)$ in position (a, b). We focus on abelian G and cyclic U; say $G = \mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_m}$ and $U = \langle\zeta_h\rangle \cong \mathbb{Z}_h$, where $\langle\zeta_h\rangle := \{\zeta_h^i \mid 0 \le i \le h-1\}$ is generated (multiplicatively) by ζ_h.

Denote the set of $n \times n$ matrices with entries in a set S by $\mathcal{M}_n(S)$. A matrix $M \in \mathcal{M}_n(\langle\zeta_k\rangle)$ is a *Butson (Hadamard) matrix* if $MM^* = nI_n$, where I_n is the $n \times n$ identity matrix and M^* is the complex conjugate transpose of M. We write $\mathrm{BH}(n, k)$ to denote the (possibly empty) set of all Butson matrices in $\mathcal{M}_n(\langle\zeta_k\rangle)$. For example, at every order n we have the Fourier matrix $\left[\zeta_n^{(i-1)(j-1)}\right]_{i,j=1}^n \in \mathrm{BH}(n, n)$. Hadamard matrices of order n are the elements of $\mathrm{BH}(n, 2)$. We quote a number-theoretic constraint on the existence of elements of $\mathrm{BH}(n, k)$.

Theorem 1 *([3, Theorem 2.8.4]) If $\mathrm{BH}(n, k) \neq \emptyset$ and $p_1, \ldots, p_r$ are the primes dividing k, then $n = a_1 p_1 + \cdots + a_r p_r$ for non-negative integers $a_1, \ldots, a_r$.*

Two matrices $H, H' \in \mathcal{M}_n(\langle\zeta_k\rangle)$ are *equivalent* if $PHQ^* = H'$ for monomials $P, Q \in \mathcal{M}_n(\langle\zeta_k\rangle \cup \{0\})$. This equivalence relation induces a partition of $\mathrm{BH}(n, k)$.

Our interest is in cocyclic Butson matrices. Let G be a group of order n. A cocycle $\psi \in Z^2(G, \langle\zeta_k\rangle)$ such that $M_\psi \in \mathrm{BH}(n, k)$ is *orthogonal*. In particular, group invariant Butson matrices are cocyclic. The orthogonal cocycles involved here are coboundaries, as we now explain. A matrix $X \in \mathcal{M}_n(\langle\zeta_k\rangle)$ is *group invariant*, over G, if $X = [x_{a,b}]_{a,b\in G}$ and $x_{ac,bc} = x_{a,b}$ for all $a, b, c \in G$. Such an X is equivalent to a *group-developed matrix* $[\chi(ab)]_{a,b\in G}$ for some map $\chi : G \to \langle\zeta_k\rangle$ (see, e.g., [3, 10.2.2]). In turn $[\chi(ab)]$ and $M_{\partial\chi}$ are equivalent: setting P to be the G-indexed diagonal matrix with $\chi(a)$ in row a, we have $P[\chi(ab)]P^* = M_{\partial\chi}$. A group-developed Butson matrix has constant row and column sum (in $\mathbb{C}$). Together with Theorem 1, there are strong restrictions on group-developed elements of $\mathrm{BH}(n, k)$.

Lemma 1 *([4, Lemma 5.2]) Set $r_j = \mathrm{Re}(\zeta_k^j)$ and $s_j = \mathrm{Im}(\zeta_k^j)$. A matrix in $\mathrm{BH}(n, k)$ with constant row and column sums exists only if there are $x_0, \ldots, x_{k-1} \in \{0, 1, \ldots, n\}$ such that $\left(\sum_{j=0}^{k-1} r_j x_j\right)^2 + \left(\sum_{j=0}^{k-1} s_j x_j\right)^2 = n$ and $\sum_{j=0}^{k-1} x_j = n$.*

It follows from Lemma 1 that if $k = 2$ then n is an integer square, and if $k = 4$ then n is the sum of two integer squares.

Cocyclic designs give rise to relative difference sets, and vice versa [3, Sections 10.4, 15.4]. Let E be a group with normal subgroup N, where $|N| = n$ and $|E : N| = v$. A *(v,n,k,λ)-relative difference set in E relative to N* (the *forbidden subgroup*) is a k-subset R of a transversal for N in E such that $|R \cap xR| = \lambda$ for all $x \in E \setminus N$. We call R *abelian* if E is abelian, and *splitting* if N is a direct factor of E.

The final piece of background concerns arrays. Let $\mathbf{s} = (s_1, \ldots, s_m)$ be an m-tuple of integers $s_i > 1$, and let $G = \mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_m}$. A *h-ary s-array* is just a set map $\phi : G \to \mathbb{Z}_h$ (normalized when necessary). If $h = 2$, then the array is *binary*. For $w \in G$, the *periodic autocorrelation of ϕ at shift w*, denoted $AC_\phi(w)$, is defined by

$$AC_\phi(w) = \sum_{g \in G} \zeta_h^{\phi(g)-\phi(g+w)}.$$

If $AC_\phi(w) = 0$ for all $w \neq 0$, then ϕ is *perfect*.

Lemma 2 *Let D_m be the m^{th} Kronecker power of the $q \times q$ Fourier matrix, i.e., $(D_m)_{i,j} = \zeta_q^{\alpha_{i-1}\cdot\alpha_{j-1}}$, where $\alpha_0 = (0, \ldots, 0), \alpha_1 = (0, 0, \ldots, 1), \ldots, \alpha_{q^m-1} = (q-1, \ldots, q-1)$. Then, for any map $\phi : \mathbb{Z}_q^m \to \mathbb{Z}_h$,*

$$(AC_\phi(\alpha_0), \ldots, AC_\phi(\alpha_{q^m-1}))D_m = \Big(\Big|\sum_{x \in \mathbb{Z}_q^m} \zeta_h^{\phi(x)}\zeta_q^{-\alpha_0\cdot x}\Big|^2, \ldots, \Big|\sum_{x \in \mathbb{Z}_q^m} \zeta_h^{\phi(x)}\zeta_q^{-\alpha_{q^m-1}\cdot x}\Big|^2\Big).$$

Proof We adapt the proof of the lemma (for Boolean functions) in [2, Section 2]. First,

$$\sum_{i \geq 0} AC_\phi(\alpha_i)\zeta_q^{\alpha_i\cdot\alpha_j} = \sum_{i \geq 0}\sum_{k \geq 0} \zeta_h^{\phi(\alpha_k)-\phi(\alpha_k+\alpha_i)}\zeta_q^{\alpha_i\cdot\alpha_j}.$$

After replacing α_i by $\alpha_i - \alpha_k$, the double summation becomes

$$\begin{aligned}\sum_{i \geq 0}\sum_{k \geq 0} \zeta_h^{\phi(\alpha_k)-\phi(\alpha_i)}\zeta_q^{\alpha_i\cdot\alpha_j-\alpha_k\cdot\alpha_j} &= \sum_{k \geq 0} \zeta_h^{\phi(\alpha_k)}\zeta_q^{-\alpha_k\cdot\alpha_j}\sum_{i \geq 0} \zeta_h^{-\phi(\alpha_i)}\zeta_q^{\alpha_i\cdot\alpha_j} \\ &= \Big|\sum_{x \in \mathbb{Z}_q^m} \zeta_h^{\phi(x)}\zeta_q^{-\alpha_j\cdot x}\Big|^2,\end{aligned}$$

as required. □

Our fundamental motivating result is extracted mostly from [16].

Theorem 2 *Let $f : \mathbb{Z}_q^m \to \mathbb{Z}_h$ be a map. The following are equivalent*:

1. *f is a GBF*;
2. *$M_{\partial f} \in BH(q^m, h)$*;
3. *f is a perfect h-ary $(q, \ldots, q)$-array.*

Additionally, if h is prime and divides q^m, then (1)–(3) are equivalent to

4. *$\{(f(x), x) \mid x \in \mathbb{Z}_q^m\}$ is a splitting $(q^m, h, q^m, q^m/h)$-relative difference set in $\mathbb{Z}_h \times \mathbb{Z}_q^m$.*

Proof The equivalences (1) ⇔ (2) ⇔ (4) come from Propositions 2.3 and 2.7 of [16] (h prime is a sufficient condition to ensure (2) ⇒ (4)). Lemma 2 implies (1) ⇔ (3). □

We investigate the effect on Theorem 2 when non-coboundary cocyclic Butson matrices, generalized perfect arrays, and non-splitting abelian relative difference sets are considered in (2), (3), (4), respectively. To this end, we need some material of a more specialized nature, which is presented over the next two sections.

3 More on arrays and bent functions

There is an equivalence between binary arrays and non-splitting abelian relative difference sets, as set out in [8]. Subsequently, a bridge to the theory of cocyclic Hadamard matrices was identified [7]. The main tool here is the notion of a generalized perfect binary array (GPBA). Guided by [1, Section 3], we extend the notion of GPBA from binary to h-ary arrays, $h \geq 2$, and show how this conforms with a variant of bent functions.

Definition 1 Let $\phi\colon G \to \mathbb{Z}_h$ be an $\mathbf{s}$-array, where $\mathbf{s} = (s_1, \ldots, s_m)$ and $G = \mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_m}$. Let $\mathbf{z} = (z_1, \ldots, z_m) \in \{0, 1\}^m$. The *expansion of ϕ of type* $\mathbf{z}$ is the map ϕ' from $E := \mathbb{Z}_{(z_1(h-1)+1)s_1} \times \cdots \times \mathbb{Z}_{(z_m(h-1)+1)s_m}$ to $\mathbb{Z}_h$ defined by

$$\phi'\colon (g_1, \ldots, g_m) \mapsto \phi(a) + b \mod h,$$

where $b = \sum_{i=1}^{m} \lfloor g_i/s_i \rfloor$ and $a \equiv (g_1, \ldots, g_m) \mod \mathbf{s}$, i.e., $a = (g_1 \mod s_1, \ldots, g_m \mod s_m)$.

We distinguish two subgroups of the extension group E in Definition 1:

$L = \{(g_1, \ldots, g_m) \in E \mid g_i = y_i s_i \text{ with } 0 \leq y_i < h \text{ if } z_i = 1, \text{ and } y_i = 0 \text{ if } z_i = 0\}$,
$K = \{(g_1, \ldots, g_m) \in L \mid \sum_i (g_i/s_i) \equiv 0 \mod h\}$.

Note that

$L \cong \mathbb{Z}_h^n$ where $n = \mathrm{wt}(\mathbf{z}) = \sum_i z_i$;
$E/L \cong G$;
if $\mathbf{z} \neq \mathbf{0}$ then $L/K = \langle (0, \ldots, 0, s_i, 0, \ldots, 0) + K \rangle \cong \mathbb{Z}_h$, for any i such that $z_i = 1$.

With these subgroups of E now defined, we will be able to see how the expansion of an $\mathbf{s}$-array is natural, and how it allows us to generalize the notion of perfect array.

Lemma 3 *Let ϕ be a h-ary $(s_1, \ldots, s_m)$-array with expansion $\phi'\colon E \to \mathbb{Z}_h$. If $e \in E$ and $g = (g_1, \ldots, g_m) \in L$, then $\phi'(e + g) \equiv \phi'(e) + b \mod h$ where $b = \sum_i g_i/s_i$.*

Proof This is routine, from the definitions. □

Corollary 1 *Under the hypotheses of Lemma 3, $AC_{\phi'}(g) = \zeta_h^{-b}|E|$ for any $g \in L$.*

Definition 2 A h-ary $\mathbf{s}$-array ϕ with expansion $\phi'\colon E \to \mathbb{Z}_h$ of type $\mathbf{z}$ is *generalized perfect* if $AC_{\phi'}(g) = 0$ for all $g \in E \setminus L$; in short, ϕ is a GPhA($\mathbf{s}$) of type $\mathbf{z}$. We write GPhA(c^m) when $\mathbf{s}$ is the vector $(c, \ldots, c)$ of length m for a constant c.

So a GPhA($\mathbf{s}$) of type $\mathbf{0}$ is exactly a perfect h-ary $\mathbf{s}$-array.

Definition 3 (cf. [18, Definition 2.2]) A map $f\colon \mathbb{Z}_q^m \to \mathbb{Z}_h$ such that $|AC_f(x)| \in \{0, q^m\}$ for all $x \in \mathbb{Z}_q^m$ is a *generalized partially bent function* (GPBF).

Let ϕ be a h-ary $(q, \ldots, q)$-array of type $\mathbf{1}$. By Corollary 1, $|\phi'(g)| = (hq)^m \ \forall g \in L$. If ϕ is generalized perfect, then by definition $|\phi'(g)| = 0 \ \forall x \in \mathbb{Z}_{hq}^m \setminus L$, so ϕ' is generalized partially bent. However, the converse does not hold, as evidenced by the following simple example. Define $\phi\colon \mathbb{Z}_2^2 \to \mathbb{Z}_2$ by $\phi(0, 1) = 1$ and $\phi(0, 0) = \phi(1, 0) = \phi(1, 1) = 0$. The expansion of ϕ of type $\mathbf{1}$ is a GPBF, but ϕ is not a GP2A(2^2) of type $\mathbf{1}$ (writing $\mathbf{1}$ for the all 1s vector). We obtain the converse by imposing more conditions.

Proposition 1 *Let ϕ be an array $\mathbb{Z}_h^m \to \mathbb{Z}_h$ such that for each $y = (y_1, \ldots, y_m) \in \mathbb{Z}_h^m \setminus \{\mathbf{0}\}$ with $\sum_i y_i \equiv 0 \mod h$, there exists $x = (x_1, \ldots, x_m) \in \mathbb{Z}_h^m$ satisfying*

$$\phi(x+y) + \sum_i \lfloor (x_i + y_i)/h \rfloor \not\equiv \phi(x) + \phi(y) \mod h. \tag{1}$$

Then the expansion ϕ' of ϕ of type **1** *is a GPBF if and only if ϕ is a GPhA(h^m) of type* **1**.

Proof In this proposition, $E = \mathbb{Z}_{h^2}^m$ and $L = \{0, h, \ldots, (h-1)h\}^m \cong \mathbb{Z}_h^m$. Suppose that ϕ' is a GPBF. Then ϕ is a GPhA(h^m) if $|AC_{\phi'}(g)| < h^{2m}$ for all $g \in E \setminus L$. So we prove that $\phi'(w) - \phi'(w+g) \not\equiv \phi'(x) - \phi'(x+g) \mod h$ for some $w, x \in E$. Taking $w = 0$, and assuming that ϕ is normalized, this non-congruence becomes $\phi'(x+g) \not\equiv \phi'(x) + \phi'(g)$.

Suppose that

$$\phi'(0) - \phi'(g),\ \phi'(g) - \phi'(2g),\ \ldots,\ \phi'((h-1)g) - \phi'(hg)$$

are all congruent modulo h (otherwise, the required x may be found as a multiple of g). Adding these h terms gives

$$\phi'(0) - \phi'(hg) \equiv 0 \mod h \ \Rightarrow\ \phi'(hg) \equiv 0 \mod h.$$

Consequently $\sum_i g_i \equiv 0 \mod h$.

If $g = (g_1, \ldots, g_m)$ with $0 \le g_i < h$, then the right-hand side of (1) for $y = g$ is $\phi'(x) + \phi'(g)$, and the left-hand side is $\phi'(x+g)$; so we are done.

Now let $g = a + l$ with $a = (g_1 \mod h, \ldots, g_m \mod h)$ and $l \in L$. Then $\sum_i a_i \equiv 0$, because $hg = ha$ in E. Using Lemma 3, and adding $b = \sum_i l_i/h$ to both sides of (1) for $y = a$, we see that $\phi'(x+g) \not\equiv \phi'(x) + \phi'(g)$. This completes the proof. □

4 Equivalences between arrays, bent functions, and associated combinatorial objects

Let $\mathbf{s}$, $\mathbf{z}$, G, K, L, E be as in Section 3, with $\mathbf{z} \neq \mathbf{0}$. We have a short exact sequence

$$1 \longrightarrow \langle \zeta_h \rangle \xrightarrow{\iota} E/K \xrightarrow{\beta} G \longrightarrow 0, \tag{2}$$

where $\beta(g+K) \equiv g \mod \mathbf{s}$ and ι sends ζ_h to a generator of $L/K \cong \mathbb{Z}_h$. In the standard way we extract a cocycle $\mu_{\mathbf{z}} \in Z^2(G, \langle \zeta_h \rangle)$ from (2), depending on the choice of a transversal map $\tau : G \to E/K$ (see, e.g., [3, § 12.1.3]). Set $\tau(x) = x + K$ (a mild abuse of notation), so that $\beta \circ \tau = \mathrm{id}_G$; then $\mu_{\mathbf{z}}(x, y) = \iota^{-1}(\tau(x) + \tau(y) - \tau(x+y))$.

Proposition 2 *(cf. [7, Lemma 3.1]) Define $\gamma_t \in Z^2(\mathbb{Z}_t, \langle \zeta_h \rangle)$ by $\gamma_t(j,k) = \zeta_h^{\lfloor (j+k)/t \rfloor}$. Then*

(i) $\mu_{\mathbf{z}}(x, y) = \prod_{i \text{ with } z_i = 1} \gamma_{s_i}(x_i, y_i)$;

(ii) $\mu_{\mathbf{z}} \in B^2(G, \langle \zeta_h \rangle)$ *if and only if s_i is coprime to h whenever $z_i = 1$.*

In the opposite direction, each cocycle $\psi \in Z^2(G, \langle \zeta_h \rangle)$ determines a central extension E_ψ of $\langle \zeta_h \rangle$ by G: namely, the group with elements $\{(\zeta_h^j, g) \mid 0 \le j < h,\ g \in G\}$ and multiplication defined by $(u, g)(v, h) = (uv\psi(g, h), gh)$. More properly, the central extension is the short exact sequence

$$1 \longrightarrow \langle \zeta_h \rangle \xrightarrow{\iota'} E_\psi \xrightarrow{\beta'} G \longrightarrow 0, \tag{3}$$

where $\iota'(u) = (u, 0)$ and $\beta'(u, x) = x$.

The next two results mimic Proposition 4 and Lemma 3 of [1], respectively.

Proposition 3 *If $\mu_{\mathbf{z}}$ and $\psi \in Z^2(G, \langle\zeta_h\rangle)$ are in the same cohomology class, say $\psi = \mu_{\mathbf{z}}\partial\phi$, then (2) and (3) are equivalent as short exact sequences. Specifically, for the transversal map τ as defined before Proposition 2, the map Γ sending $(u, x) \in E_\psi$ to $\iota(u\phi(x)^{-1})+\tau(x) \in E/K$ is an isomorphism that makes the diagram*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \langle\zeta_h\rangle & \xrightarrow{\iota'} & E_\psi & \xrightarrow{\beta'} & G & \longrightarrow & 0 \\ & & \| & & \Gamma\downarrow & & \| & & \\ 1 & \longrightarrow & \langle\zeta_h\rangle & \xrightarrow{\iota} & E/K & \xrightarrow{\beta} & G & \longrightarrow & 0 \end{array}$$

commute.

Remark 1 In Proposition 3, the ϕ has multiplicative target group $\langle\zeta_h\rangle$. When considering ϕ as an array, we may replace the multiplicative group $\langle\zeta_h\rangle$ by the additive group $\mathbb{Z}_h$, without bothering to change notation. Likewise, note that E_ψ is treated multiplicatively, whereas E and its subgroups and quotients are treated additively.

Lemma 4 *Assuming the set-up of Proposition 3, Γ maps the subset $\{(1, x) \mid x \in G\}$ of E_ψ onto $\{g + K \in E/K \mid \phi'(g) \equiv 0 \mod h\}$.*

Proof As ϕ' is constant on each coset of K in E by Lemma 3, the stated subset of E/K is well-defined. If $\phi(x) = \zeta_h^j$ then $\Gamma((1, x)) = -jy + x + K$ where $\iota(\zeta_h) = y + K$ generates L/K. Remember that y may be chosen as $(0, \ldots, 0, s_i, 0, \ldots, 0)$ for some i. Again by Lemma 3, $\phi'(-jy + x) = j - j\sum_i (y_i/s_i) \equiv 0 \mod h$. Conversely, suppose that $\phi'(g) = 0$. Put $a \equiv g \mod \mathbf{s}$ and $b \equiv \sum_i \lfloor g_i/s_i \rfloor \mod h$; so $\phi(a) = \phi'(g) - b \equiv -b \mod h$. Therefore, because $g - a - (0, \ldots, 0, bs_i, 0, \ldots, 0) \in K$, we get that $g + K = \iota(\phi(a)^{-1}) + a + K = \Gamma((1, a))$. □

Remark 2 $\{(1, x) \mid x \in G\}$ is a full transversal for the cosets of $\langle\zeta_h\rangle$ in E_ψ.

Next we present two lemmas about special subsets of E, to be used in the proof of the impending theorem. For $0 \le i \le h - 1$, define $N^i_{\phi'} = \{g \in E \mid \phi'(g) \equiv i \mod h\}$ and $L_i = \{g \in L \mid \sum_k (g_k/s_k) \equiv i \mod h\}$.

Lemma 5 *$N^i_{\phi'} + L_j = N^{i+j}_{\phi'}$ (elementwise sum in E), reading indices modulo h.*

Proof If $x \in N^i_{\phi'}$ and $g \in L_j$, then $\phi'(x + g) \equiv \phi'(x) + \sum_k (g_k/s_k) \equiv i + j$ by Lemma 3. Hence $N^i_{\phi'} + L_j \subseteq N^{i+j}_{\phi'}$. Since $-L_j = L_{h-j}$, this containment implies that $N^{i+j}_{\phi'} - L_j \subseteq N^i_{\phi'}$, and so $N^{i+j}_{\phi'} = N^i_{\phi'} + L_j$. □

Lemma 6 *For all i, j and $e \in E$, $|N^i_{\phi'} \cap (e + N^i_{\phi'})| = |N^j_{\phi'} \cap (e + N^j_{\phi'})|$.*

Proof The equation $x - y = e$ has precisely $|N^i_{\phi'} \cap (e + N^i_{\phi'})|$ solutions $(x, y) \in N^i_{\phi'} \times N^i_{\phi'}$. By Lemma 5, for $g \in L_{j-i}$ each such (x, y) gives a solution $(\tilde{x}, \tilde{y}) = (x + g, y + g) \in N^j_{\phi'} \times N^j_{\phi'}$ of the equation $\tilde{x} - \tilde{y} = e$. Thus $|N^i_{\phi'} \cap (e + N^i_{\phi'})| \le |N^j_{\phi'} \cap (e + N^j_{\phi'})|$. The equality follows after swapping i and j. □

We also need a fact about vanishing sums of roots of unity (see, e.g., [3, Lemma 2.8.5]).

Lemma 7 *For prime h, if $\sum_{i=0}^{h-1} \alpha_i \zeta_h^i = 0$ with $\alpha_i \in \mathbb{Z}$, then $\alpha_0 = \alpha_1 = \cdots = \alpha_{h-1}$.*

Theorem 3 *Let ϕ be a h-ary $\mathbf{s}$-array of type $\mathbf{z} \neq \mathbf{0}$, where h is a prime dividing $v := |G| = \prod_i s_i$ (Definition 1), and let*

$$R = \{g + K \in E/K \mid \phi'(g) \equiv 0 \mod h\}.$$

Then ϕ is a GPhA($\mathbf{s}$) of type $\mathbf{z}$ if and only if R is a $(v, h, v, v/h)$-relative difference set in E/K with forbidden subgroup L/K.

Proof For $e \in E$ and $0 \leq k < h$, define $B_k^{(e)} = \sum_{i=0}^{h-1} |N_{\phi'}^i \cap (N_{\phi'}^{i-k} - e)|$. We readily see that

$$AC_{\phi'}(e) = \sum_{g \in E} \zeta_h^{\phi'(g)-\phi'(g+e)} = \sum_{k=0}^{h-1} B_k^{(e)} \zeta_h^k.$$

If $e \notin L$ then we use Lemma 7 and $\sum_{k=0}^{h-1} B_k^{(e)} = |E|$ to infer

$$AC_{\phi'}(e) = 0 \;\Leftrightarrow\; B_k^{(e)} = |E|/h \quad \forall k. \tag{4}$$

Suppose that ϕ is generalized perfect. If $e \notin L$ then $|N_{\phi'}^i \cap (e + N_{\phi'}^i)| = |E|/h^2$ by (4) and Lemma 6. On the other hand, $|N_{\phi'}^i \cap (e + N_{\phi'}^i)| = 0$ if $e \in L \setminus K$, by Lemma 3. Hence the number of solutions $(x+K, y+K) \in R \times R$ of $x+K-(y+K) = e+K$ is 0 if $e \in L \setminus K$ and $|E|/(|K|h^2)$ if $e \notin L$. Accordingly R is an $\big(|E : L|, |L : K|, |R|, |E|/(|K|h^2)\big)$-relative difference set in E/K, with forbidden subgroup L/K. Also $|E : L| = |G|$, $|L : K| = h$, and $|R| = |G|$ by Lemma 4. Thus R has the claimed parameters.

Now suppose that R is a $(v, h, v, v/h)$-relative difference set in E/K with forbidden subgroup L/K. Then $|N_{\phi'}^i \cap (N_{\phi'}^i - e)| = |E|/h^2$ for any $e \in E \setminus L$; thus $B_0^{(e)} = |E|/h$. Further, if $z \in L_k$ then $N_{\phi'}^{i-k} - e + z = N_{\phi'}^i - e$ by Lemma 5, giving $B_0^{(e)} = B_k^{(e-z)}$. Since $B_0^{(e)}$ is constant as e ranges over $E \setminus L$, this means that

$$B_0^{(e)} = B_i^{(e)} = |E|/h \quad \forall i \text{ and } \forall e \notin L.$$

By (4), ϕ is a GPhA($\mathbf{s}$). □

Remark 3 For an equivalence between difference sets and almost perfect arrays, see [15].

Proposition 4 *([4, Theorem 4.1]) Let H be a finite group whose order is divisible by a prime h. Then $\psi \in Z^2(H, \langle\zeta_h\rangle)$ is orthogonal if and only if $\{(1, x) \mid x \in H\}$ is a $(|H|, h, |H|, |H|/h)$-relative difference set in E_ψ with forbidden subgroup $\langle(\zeta_h, 1)\rangle$.*

Theorem 4 *For prime h, a (normalized) h-ary $\mathbf{s}$-array ϕ is a GPhA($\mathbf{s}$) of type $\mathbf{z} \neq \mathbf{0}$ if and only if $\mu_{\mathbf{z}}\partial\phi$ is orthogonal.*

Proof This is a consequence of Theorem 3, Proposition 4, and Lemma 4. □

The next theorem connects generalized plateaued functions to GPhAs.

Theorem 5 *Let $\phi\colon \mathbb{Z}_q^m \to \mathbb{Z}_h$ be a map, where h is a prime dividing q. The following are equivalent*:

1. *ϕ is a GPhA(q^m) of type $\mathbf{1}$;*

2. *The expansion* $\phi' \colon \mathbb{Z}_{hq}^m \to \mathbb{Z}_h$ *of* ϕ *of type* $\mathbf{1}$ *is a generalized plateaued function, i.e.,*

$$\Big| \sum_{x \in \mathbb{Z}_{hq}^m} \zeta_h^{\phi'(x)} \zeta_{hq}^{-v \cdot x} \Big|^2 = \begin{cases} (h^2 q)^m & v \in \mathcal{F} \\ 0 & v \in \mathbb{Z}_{hq}^m \setminus \mathcal{F}, \end{cases}$$

where $\mathcal{F} = \{v \in \mathbb{Z}_{hq}^m \mid v \equiv \mathbf{1} \mod h\}$.

Proof Let $u = (y_1 q, \ldots, y_m q) \in L$ and $v = (y_1' q + a_1, \ldots, y_m' q + a_m) \in E = \mathbb{Z}_{hq}^m$ where $0 \le y_j, y_j' \le h-1$ and $0 \le a_j \le q-1$. Then $u \cdot v \equiv (a_1 y_1 + \cdots + a_m y_m) q \mod hq$. Hence, if ϕ is a GPhA(q^m) of type $\mathbf{1}$, then by Lemma 2 and Corollary 1,

$$\Big| \sum_{x \in \mathbb{Z}_{hq}^m} \zeta_h^{\phi'(x)} \zeta_{hq}^{-v \cdot x} \Big|^2 = \sum_{u \in L} AC_{\phi'}(u) \zeta_{hq}^{u \cdot v} = (hq)^m \sum_{0 \le y_1, \ldots, y_m \le h-1} \zeta_{hq}^{-(y_1 + \cdots + y_m) q + u \cdot v}$$

The rightmost displayed summation is equal to

$$(hq)^m \sum_{0 \le y_1, \ldots, y_m \le h-1} \zeta_h^{(a_1 - 1) y_1 + \cdots + (a_m - 1) y_m} = \begin{cases} (h^2 q)^m & a_k \equiv 1 \mod h \ \ \forall k \\ 0 & \text{otherwise.} \end{cases}$$

This proves (1) $\Rightarrow$ (2). We get (2) $\Rightarrow$ (1) similarly, appealing once more to Lemma 2 and taking into account that $D_m D_m^* = (hq)^m I_m$. □

Now we can fulfil our intention as stated just after Theorem 2.

Theorem 6 *Let* h *be a prime divisor of* q*, and let* $\phi \colon \mathbb{Z}_q^m \to \mathbb{Z}_h$ *be an array with expansion* ϕ' *of type* $\mathbf{z} \neq \mathbf{0}$.

(a) The following are equivalent:

- *(i)* $\mu_{\mathbf{z}} \partial \phi$ *is symmetric and orthogonal, i.e.,* $M_{\mu_{\mathbf{z}} \partial \phi}$ *is a symmetric Butson Hadamard matrix*;
- *(ii)* ϕ *is a GPhA*(q^m) *of type* $\mathbf{z}$;
- *(iii)* $\{g + K \in E/K \mid \phi'(g) = 0\}$ *is a non-splitting* $(q^m, h, q^m, q^m/h)$*-relative difference set in* E/K *with forbidden subgroup* L/K.

(b) If $\mathbf{z} = \mathbf{1}$ *then (i)–(iii) are equivalent to*

- *(iv)* ϕ' *is a generalized plateaued function, i.e.,*

$$\Big| \sum_{x \in \mathbb{Z}_{hq}^m} \zeta_h^{\phi'(x)} \zeta_{hq}^{-v \cdot x} \Big|^2 = \begin{cases} (h^2 q)^m & v \in \mathcal{F} \\ 0 & \text{otherwise,} \end{cases}$$

where $\mathcal{F} = \{v \in \mathbb{Z}_{hq}^m \mid v \equiv \mathbf{1} \mod h\}$.

(c) Let $h = q$ *and* $\mathbf{z} = \mathbf{1}$*. Suppose that, for all* $y \in \mathbb{Z}_h^m \setminus \{\mathbf{0}\}$ *with* $\sum y_i \equiv 0 \mod h$*, there exists* $x \in \mathbb{Z}_h^m$ *satisfying* (1)*. Then (i)–(iv) are equivalent to*

- *(v)* ϕ' *is a GPBF.*

Proof The equivalences (i) $\Leftrightarrow$ (ii), (ii) $\Leftrightarrow$ (iii), (ii) $\Leftrightarrow$ (iv), and (ii) $\Leftrightarrow$ (v) follow from Theorems 4, 3, 5, and Proposition 1. (Proposition 2 (ii) justifies non-splitting in (iii).) □

Remark 4 In [18, Definition 2.2], a map $\phi\colon \mathbb{Z}_q^m \to \mathbb{Z}_q$ is called a generalized partially bent function if $(q^m - N_F)(q^m - N_C) = q^m$ where

$$N_F = |\{v \in \mathbb{Z}_q^m \mid \sum_{x\in\mathbb{Z}_q^m} \zeta_q^{\phi(x)-v\cdot x} = 0\}| \quad \text{and} \quad N_C = |\{v \in \mathbb{Z}_q^m \mid AC_{-\phi}(v) = 0\}|.$$

Previously, Carlet [2, Definition 1] introduced partially bent functions for $q = 2$. The coincidence with our Definition 3 is shown in [17, Theorem 2] and [13, Proposition 8]. Observe that, for $\mathbf{z} = \mathbf{1}$, we have $|L| \cdot |\mathcal{F}| = (hq)^m$, $|L| = (hq)^m - N_C$, and $|\mathcal{F}| = (hq)^m - N_F$.

Remark 5 For q prime, if $\phi : \mathbb{Z}_q^m \to \mathbb{Z}_q$ is a GPqA(q^m) of type $\mathbf{1}$, then ϕ' is a $2m$-generalized plateaued function.

5 Examples

Example 1 Let ϕ be the map on $\mathbb{Z}_2^3$ with layers

$$A_0 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \quad \text{and} \quad A_1 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}.$$

Here A_i is the layer on $\{i\} \times \mathbb{Z}_2 \times \mathbb{Z}_2$, and $\phi(i, j, k) = A_i(j, k)$. Then ϕ is a GPBA(2^3), i.e., a GP2A(2^3) of type $\mathbf{1}$. It has orthogonal cocycle $\mu_{\mathbf{1}}\partial_2\partial_3\partial_4\partial_6$, where $\partial_i = \partial\phi_i$ for the multiplicative Kronecker delta ϕ_i of α_i, with $\alpha_0 = (0, 0, 0)$, $\alpha_1 = (0, 0, 1)$, etc. We label rows and columns with the elements of $\mathbb{Z}_2^3 = \{\alpha_0, \ldots, \alpha_7\}$ in this ordering, and display the cocyclic Hadamard matrix $M_{\mu_{\mathbf{1}}\partial\phi}$ as a Hadamard (entrywise) product $M_{\mu_{\mathbf{1}}} \circ M_{\partial\phi}$ in logarithmic form:

$$\begin{bmatrix} 0&0&0&0&0&0&0&0 \\ 0&1&0&1&0&1&0&1 \\ 0&0&1&1&0&0&1&1 \\ 0&1&1&0&0&1&1&0 \\ 0&0&0&0&1&1&1&1 \\ 0&1&0&1&1&0&1&0 \\ 0&0&1&1&1&1&0&0 \\ 0&1&1&0&1&0&0&1 \end{bmatrix} \circ \begin{bmatrix} 0&0&0&0&0&0&0&0 \\ 0&0&1&1&0&0&1&1 \\ 0&1&0&1&1&0&1&0 \\ 0&1&1&0&1&0&0&1 \\ 0&0&1&1&0&0&1&1 \\ 0&0&0&0&0&0&0&0 \\ 0&1&1&0&1&0&0&1 \\ 0&1&0&1&1&0&1&0 \end{bmatrix} = \begin{bmatrix} 0&0&0&0&0&0&0&0 \\ 0&1&1&0&0&1&1&0 \\ 0&1&1&0&1&0&0&1 \\ 0&0&0&0&1&1&1&1 \\ 0&0&1&1&1&1&0&0 \\ 0&1&0&1&1&0&1&0 \\ 0&1&0&1&0&1&0&1 \\ 0&0&1&1&0&0&1&1 \end{bmatrix}.$$

The expansion $\phi'\colon \mathbb{Z}_4^3 \to \mathbb{Z}_2$ is defined by the layers B_i on $\{i\} \times \mathbb{Z}_4 \times \mathbb{Z}_4$, $0 \le i \le 3$, where

$$B_i = \begin{cases} \begin{bmatrix} A_0 & A_0 \oplus J \\ A_0 \oplus J & A_0 \end{bmatrix} & i = 0, 2 \\ \\ \begin{bmatrix} A_1 \oplus J & A_1 \\ A_1 & A_1 \oplus J \end{bmatrix} & i = 1, 3, \end{cases}$$

J denoting the all 1s matrix. We have $L = \langle(2, 0, 0), (0, 2, 0), (0, 0, 2)\rangle = \{(0, 0, 0), (0, 0, 2), (0, 2, 0), (0, 2, 2), (2, 0, 0), (2, 0, 2), (2, 2, 0), (2, 2, 2)\}$,

$$AC_{\phi'}(v) = \begin{cases} (-1)^{\mathrm{wt}(v)}\, 64 & v \in L \\ 0 & v \notin L, \end{cases}$$

$\mathcal{F} = \{(1,1,1),(1,1,3),(1,3,1),(1,3,3),(3,1,1),(3,1,3),(3,3,1),(3,3,3)\}$, and

$$\Big|\sum_{x\in\mathbb{Z}_4^3} \zeta_2^{\phi'(x)}\zeta_4^{-v\cdot x}\Big|^2 = \begin{cases} 512 & v\in\mathcal{F} \\ 0 & v\notin\mathcal{F}. \end{cases}$$

Therefore ϕ' is a GPBF.

Example 2 The map $\phi = \begin{bmatrix} 0&1&1&1\\ 1&1&0&1\\ 0&1&0&0\\ 0&0&0&1 \end{bmatrix}$ on $\mathbb{Z}_4^2$ is a GPBA(4^2) of type **1**. It has orthogonal cocycle $\mu_{\mathbf{1}}\partial\phi$. If we label rows and columns with the elements of $\mathbb{Z}_4^2 = \{\alpha_0 = (0,0), \alpha_1 = (0,1), \alpha_2 = (0,2), \ldots, \alpha_{15} = (3,3)\}$, then the cocyclic Hadamard matrix $M_{\mu_{\mathbf{1}}} \circ M_{\partial\phi}$ in logarithmic form is the Hadamard product of

$$\begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1\\
0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\
0&1&1&1&0&1&1&1&0&1&1&1&0&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1\\
0&0&0&1&0&0&0&1&0&0&0&1&1&1&1&0\\
0&0&1&1&0&0&1&1&0&0&1&1&1&1&0&0\\
0&1&1&1&0&1&1&1&0&1&1&1&1&0&0&0\\
0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\
0&0&0&1&0&0&0&1&1&1&1&0&1&1&1&0\\
0&0&1&1&0&0&1&1&1&1&0&0&1&1&0&0\\
0&1&1&1&0&1&1&1&1&0&0&0&1&0&0&0\\
0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1\\
0&0&0&1&1&1&1&0&1&1&1&0&1&1&1&0\\
0&0&1&1&1&1&0&0&1&1&0&0&1&1&0&0\\
0&1&1&1&1&0&0&0&1&0&0&0&1&0&0&0
\end{bmatrix}$$

with

$$\begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&1&1&1&0&0&0&1&1&0&1&0&0&1\\
0&1&0&1&0&1&0&1&1&0&1&0&1&0&1&0\\
0&1&1&0&1&0&0&1&1&1&0&0&0&0&1&1\\
0&1&0&1&1&0&0&1&1&0&1&0&0&1&1&0\\
0&1&1&0&0&0&0&0&1&1&0&0&1&0&1&0\\
0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&1\\
0&0&1&1&1&0&1&0&0&1&1&0&1&1&1&1\\
0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0\\
0&1&0&1&0&1&0&1&0&0&0&0&0&0&0&0\\
0&1&1&0&1&0&0&1&1&0&0&1&0&1&1&0\\
0&0&0&0&0&0&0&0&1&0&1&0&1&0&1&0\\
0&1&1&0&0&1&0&1&1&0&0&1&1&0&1&0\\
0&0&0&0&1&0&0&1&1&0&1&0&0&0&1&1\\
0&0&1&1&1&1&1&1&0&0&1&1&1&1&1&1\\
0&1&0&1&0&0&1&1&0&0&0&0&0&1&1&0
\end{bmatrix}$$

which is equal to

$$\begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&1&1&0&1&0&1&1&1&1&0&0&0\\
0&1&1&0&0&1&1&0&1&0&0&1&1&0&0&1\\
0&0&0&1&1&1&1&0&1&0&1&1&0&1&0&0\\
0&1&0&1&1&0&0&1&1&0&1&0&1&0&0&1\\
0&1&1&1&0&0&0&1&1&1&0&1&0&1&0&0\\
0&0&1&1&0&0&0&0&0&0&1&1&1&1&1&1\\
0&1&0&0&1&1&0&1&0&0&0&1&0&1&1&1\\
0&0&1&1&1&1&0&0&1&1&0&0&0&0&1&1\\
0&1&0&0&0&1&0&0&1&1&1&0&1&1&1&0\\
0&1&0&1&1&0&1&0&0&1&0&1&1&0&1&0\\
0&1&1&1&0&1&1&1&0&0&1&0&0&0&1&0\\
0&1&1&0&1&0&1&0&0&1&1&0&0&1&0&1\\
0&0&0&1&0&1&1&1&0&1&0&0&1&1&0&1\\
0&0&0&0&0&0&1&1&1&1&1&1&0&0&1&1\\
0&0&1&0&1&0&1&1&1&0&0&0&1&1&1&0
\end{bmatrix}.$$

The expansion $\phi' : \mathbb{Z}_8^2 \to \mathbb{Z}_2$ is defined by

$$\begin{bmatrix}
0&1&1&1&1&0&0&0\\
1&1&0&1&0&0&1&0\\
0&1&0&0&1&0&1&1\\
0&0&0&1&1&1&1&0\\
1&0&0&0&0&1&1&1\\
0&0&1&0&1&1&0&1\\
1&0&1&1&0&1&0&0\\
1&1&1&0&0&0&0&1
\end{bmatrix},$$

with $L = \{(0,0), (0,4), (4,0), (4,4)\}$,

$$AC_{\phi'}(v) = \begin{cases} (-1)^{\mathrm{wt}(v)}\, 64 & v \in L \\ 0 & v \notin L, \end{cases}$$

$$\mathcal{F} = \{(1,1), (1,3), (1,5), (1,7), (3,1), (3,3), (3,5), (3,7), (5,1), (5,3), (5,5), (5,7), (7,1), (7,3), (7,5), (7,7)\},$$

and

$$\Big| \sum_{x \in \mathbb{Z}_8^2} \zeta_2^{\phi'(x)} \zeta_8^{-v \cdot x} \Big|^2 = \begin{cases} 256 & v \in \mathcal{F} \\ 0 & v \notin \mathcal{F}. \end{cases}$$

Therefore ϕ' is a GPBF.

Example 3 The map $\phi = \begin{bmatrix} 0&0&0\\ 0&1&0\\ 2&2&1 \end{bmatrix}$ on $\mathbb{Z}_3^2$ is a GP3A(3^2) of type **1**. It has orthogonal cocycle $\mu_{\mathbf{1}}\partial\phi$. Labeling the rows and columns with the elements of $\mathbb{Z}_3^2 = \{\alpha_0 = (0,0), \alpha_1 =$

$(0,1), \alpha_2 = (0,2), \ldots, \alpha_8 = (2,2)\}$, we display the cocyclic Butson matrix $M_{\mu_\mathbf{1}} \circ M_{\partial\phi}$:

$$\begin{bmatrix} 0&0&0&0&0&0&0&0&0 \\ 0&0&1&0&0&1&0&0&1 \\ 0&1&1&0&1&1&0&1&1 \\ 0&0&0&0&0&0&1&1&1 \\ 0&0&1&0&0&1&1&1&2 \\ 0&1&1&0&1&1&1&2&2 \\ 0&0&0&1&1&1&1&1&1 \\ 0&0&1&1&1&2&1&1&2 \\ 0&1&1&1&2&2&1&2&2 \end{bmatrix} \circ \begin{bmatrix} 0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&2&0&0&2&1 \\ 0&0&0&0&0&2&1&2&0&1 \\ 0&1&0&2&1&1&1&1&2 \\ 0&2&2&1&2&1&0&0&1 \\ 0&0&1&1&1&2&1&1&2 \\ 0&0&2&1&0&1&2&0&0 \\ 0&2&0&1&0&1&0&2&0 \\ 0&1&1&2&1&2&0&0&2 \end{bmatrix} = \begin{bmatrix} 0&0&0&0&0&0&0&0&0 \\ 0&0&1&1&2&1&0&2&2 \\ 0&1&1&0&0&2&2&1&2 \\ 0&1&0&2&1&1&2&2&0 \\ 0&2&0&1&2&2&1&1&0 \\ 0&1&2&1&2&0&2&0&1 \\ 0&0&2&2&1&2&0&1&1 \\ 0&2&1&2&1&0&1&0&2 \\ 0&2&2&0&0&1&1&2&1 \end{bmatrix}.$$

The expansion $\phi' \colon \mathbb{Z}_9^2 \to \mathbb{Z}_3$ is defined by

$$\begin{bmatrix} 0&0&0&1&1&1&2&2&2 \\ 0&1&0&1&2&1&2&0&2 \\ 2&2&1&0&0&2&1&1&0 \\ 1&1&1&2&2&2&0&0&0 \\ 1&2&1&2&0&2&0&1&0 \\ 0&0&2&1&1&0&2&2&1 \\ 2&2&2&0&0&0&1&1&1 \\ 2&0&2&0&1&0&1&2&1 \\ 1&1&0&2&2&1&0&0&2 \end{bmatrix},$$

with $L = \{(0,0), (0,3), (0,6), (3,0), (3,3), (3,6), (6,0), (6,3), (6,6)\}$,

$$AC_{\phi'}((v_1,v_2)) = \begin{cases} 81\,\zeta_3^{-(v_1+v_2)/3} & (v_1,v_2) \in L \\ 0 & (v_1,v_2) \notin L, \end{cases}$$

$\mathcal{F} = \{(1,1), (1,4), (1,7), (4,1), (4,4), (4,7), (7,1), (7,4), (7,7)\}$, and

$$\Big| \sum_{x \in \mathbb{Z}_9^2} \zeta_3^{\phi'(x)} \zeta_9^{-v\cdot x} \Big|^2 = \begin{cases} 729 & v \in \mathcal{F} \\ 0 & v \notin \mathcal{F}. \end{cases}$$

Thus ϕ' is a GPBF. Also ϕ' is a 4-generalized plateaued function (see Remark 5).

It may be checked that the sufficient condition (1) is satisfied in each of the Examples 1–3.

We now recite a bit more algebraic design theory in preparation for our penultimate result, which provides an infinite family of GPhAs of type **1** arising from Example 1.

Proposition 5 *(cf. [3, Theorem 15.8.4]) Let* $G_\mathbf{s} = \mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_m}$, $G_\mathbf{t} = \mathbb{Z}_{t_1} \times \cdots \times \mathbb{Z}_{t_n}$, *and* $G = G_\mathbf{s} \times G_\mathbf{t}$. *Suppose that* $\psi\partial\phi_\mathbf{s} \in Z^2(G_\mathbf{s}, \langle\zeta_{k_1}\rangle)$ *and* $\rho\partial\phi_\mathbf{t} \in Z^2(G_\mathbf{t}, \langle\zeta_{k_2}\rangle)$ *are orthogonal. Let* $k = \mathrm{lcm}(k_1, k_2)$. *Define* $\varphi \in Z^2(G, \langle\zeta_k\rangle)$ *by*

$$\varphi(g_s g_t, h_s h_t) = \psi(g_s, h_s)\rho(g_t, h_t),$$

and define a map ϕ *on* G *by*

$$\phi(g_s g_t) = \phi_\mathbf{s}(g_s)\phi_\mathbf{t}(g_t).$$

Then $\varphi\partial\phi \in Z^2(G, \langle\zeta_k\rangle)$ *is orthogonal, with cocyclic matrix* $[\psi\partial\phi_\mathbf{s}] \otimes [\rho\partial\phi_\mathbf{t}]$.

Corollary 2 *Let $h = q$ be prime. If there exist symmetric cocyclic matrices in $BH(q^m, h)$ and $BH(q^n, h)$, corresponding to a $GPhA(q^m)$ of type* **1** *and a $GPhA(q^n)$ of type* **1**, *respectively, then there exists a symmetric cocyclic matrix in $BH(q^{m+n}, h)$ corresponding to a $GPhA(q^{m+n})$ of type* **1**.

Proof Since the Kronecker product of symmetric matrices is symmetric, it remains only to observe that the product matrix in $\mathrm{BH}(q^{m+n}, h)$ corresponds to an array of type **1**. This also follows from the construction and Theorem 6. □

Example 1 furnishes a symmetric orthogonal cocycle $\mu_{\mathbf{1}}\partial\phi \in Z^2(\mathbb{Z}_2^3, \mathbb{Z}_2)$ with nontrivial coboundary $\partial\phi$. By iteration of Proposition 5 (Kronecker multiplying $\mu_{\mathbf{1}}\partial\phi$ by powers of $\mu_{\mathbf{1}} \in Z^2(\mathbb{Z}_2, \mathbb{Z}_2)$), we get a symmetric orthogonal cocycle $\mu_{\mathbf{1}}\partial\chi \in Z^2(\mathbb{Z}_2^k, \mathbb{Z}_2)$. Then χ is a $\mathrm{GPBA}(2^k)$ of type **1**. Thus, for all $k \geq 3$ there exists a map $\mathbb{Z}_2^k \to \mathbb{Z}_2$ with expansion a GPBF; whereas for odd k, recall that no GBF—i.e., no bent function—can exist. We note that for odd k this map is a *Boolean near-bent function* [12, Section 16.1.1]. Chapter 16 of [12] may be consulted for similar existence results, e.g., on plateaued and partially bent functions.

Acknowledgements The first author was supported by project FQM-016 funded by JJAA (Spain).

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Armario, J.A., Flannery, D.L.: Generalized binary arrays from quasi-orthogonal cocycles. Des. Codes Cryptogr. **87**(10), 2405–2417 (2019)
2. Carlet, C.: Partially-bent functions. Des. Codes Cryptogr. **3**(2), 135–145 (1993)
3. de Launey, W., Flannery, D. L.: Algebraic design theory, Math. Surveys Monogr. 175, American Mathematical Society, Providence, RI (2011)
4. Egan, R., Flannery, D. L., Ó Catháin, P.: Classifying cocyclic Butson Hadamard matrices. In: Colbourn, C. (Ed.) Algebraic Design Theory and Hadamard Matrices, Springer Proc. Math. Stat, vol. 133, pp. 93–106 (2015)
5. Elliott, D.F., Rao, K.R.: Fast Transforms: Algorithms, Applications, Academic Press Inc, USA, Analyses (1982)
6. Horadam, K.J.: Hadamard matrices and their applications. Princeton University Press, Princeton, NJ (2007)
7. Hughes, G.: Non-splitting abelian $(4t, 2, 4t, 2t)$ relative difference sets and Hadamard cocycles. Europ. J. Combin. **21**(3), 323–331 (2000)
8. Jedwab, J.: Generalized perfect arrays and Menon difference sets. Des. Codes Cryptogr. **2**(1), 19–68 (1992)
9. Kumar, P.V., Scholtz, R.A., Welch, L.R.: Generalised bent functions and their properties. J. Combin. Theory Ser. A **40**, 90–107 (1985)
10. Leung, K.H., Schmidt, B.: Nonexistence results on generalized bent functions $\mathbb{Z}_q^m \to \mathbb{Z}_q$ with odd m and $q \equiv 2 \pmod 4$. J. Combin. Theory Ser. A **163**, 1–33 (2019)
11. MacWilliams, F. J., Sloane, N. J. A.: The theory of error-correcting codes. II, North-Holland Mathematical Library, vol. 16, North-Holland Publishing Co., Amsterdam-New York-Oxford (1977)
12. Mesnager, S.: Bent functions: Fundamentals and Results. Springer, New York (2016)
13. Mesnager, S., Özbudak, F., Sınak, A.: Characterizations of partially bent and plateaued functions over finite fields. Arithmetic of Finite Fields, 224–241, Lecture Notes in Comput. Sci., vol. 11321, Springer (2018)

14. Mesnager, S., Tang, C., Qi, Y.: Generalized plateaued functions and admissible (plateaued) functions. IEEE Trans. Inf. Theory **63**(10), 6139–6148 (2017)
15. Özden, B., Yayla, O.: Almost p-ary sequences. Cryptogr. Commun. **12**(6), 1057–1069 (2020)
16. Schmidt, B.: A survey of group invariant Butson matrices and their relation to generalized bent functions and various other objects. Radon Ser. Comput. Appl. Math. **23**, 241–251 (2019)
17. Wang, J.: The linear kernel of Boolean functions and partially bent functions. Systems Sci. Math. Sci. **10**(1), 6–11 (1997)
18. Wang, X., Zhou, J.: Generalized partially bent functions. In: Future Generation Communication and Networking (FGCN 2007). vol. 1, pp. 16–21, IEEE (2007)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.