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

J. A. Armario*, R. Egan**, and D. L. Flannery**

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

**School of Mathematics, Statistics and Applied Mathematics, National University of Ireland, Galway, Galway H91TK33, Ireland

Abstract

In a recent survey, Schmidt discusses connections between generalized bent functions, group invariant Butson Hadamard matrices, and certain splitting relative difference sets. We lift results from this base case by establishing broader connections between non-splitting relative difference sets, cocyclic Butson Hadamard matrices, generalized partially bent functions, and generalized perfect arrays.

This paper is inspired by Schmidt's survey [9]. We first provide background on some of the objects named in the title, before stating our main results.

Let q, m, h be positive integers, and let ζ_k be the complex k^{th} root of unity $\exp(2\pi\sqrt{-1}/k)$. Schmidt [9, Section 2.2] defines a map $f\colon \mathbb{Z}_q^m \to \mathbb{Z}_h$ to be a *generalized bent function* (GBF) if

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

where $|z|$ as usual denotes the modulus of $z \in \mathbb{C}$.

One of our aims is to investigate the role of GBFs within cocyclic design theory. Some requisite definitions follow. Let G and U be finite groups, with U abelian. A map $\psi\colon G \times G \to U$ 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). We may assume that ψ is normalized, meaning that $\psi(1,1) = 1$. For any (normalized) map $\phi\colon G \to U$, 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 $\psi\colon G \times G \to U$ forms an abelian group $Z^2(G,U)$ under pointwise multiplication. Each cocycle $\psi \in Z^2(G,U)$ may be displayed as a *cocyclic matrix*, denoted M_ψ. That is, under some indexing of rows and columns by G, the entry in position (a,b) of M_ψ is $\psi(a,b)$. We focus on the case $G = \mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_m}$ and $U = \langle \zeta_h \rangle \cong \mathbb{Z}_h$.

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 $\mathrm{BH}(n,k)$ for the set of all Butson matrices in

$\mathcal{M}_n(\langle\zeta_k\rangle)$. The simplest examples are the Fourier matrices $F_n = \left[\zeta_n^{(i-1)(j-1)}\right]_{i,j=1}^n \in \mathrm{BH}(n,n)$. Hadamard matrices of order n, as they are usually defined, are the elements of $\mathrm{BH}(n,2)$.

Matrices H, $H' \in \mathcal{M}_n(\langle\zeta_k\rangle)$ such that $PHQ^* = H'$ for monomials $P, Q \in \mathcal{M}_n(\langle\zeta_k\rangle \cup \{0\})$ are *equivalent*. Equivalence preserves the Butson property: if $H \in \mathrm{BH}(n,k)$ and H' is equivalent to H, then $H' \in \mathrm{BH}(n,k)$ too.

Our interest is in *cocyclic* Butson matrices. If $|G| = n$, $\psi \in Z^2(G, \langle\zeta_k\rangle)$, and $M_\psi \in \mathrm{BH}(n,k)$, then the cocycle ψ is said to be *orthogonal*.

Remark 1 An $n \times n$ matrix X is *group invariant*, over a group G of order n, if $X = [x_{a,b}]_{a,b\in G}$ and $x_{ac,bc} = x_{a,b}$ for all $a, b, c \in G$. A group invariant Butson matrix is equivalent to a cocyclic Butson matrix whose underlying orthogonal cocycle is a coboundary (over the same group).

Cocyclic designs are known to give rise to (relative) difference sets, and vice versa; see, e.g., [3, Sections 10.4, 15.4]. Let E be a group with a normal subgroup N of order n and index 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

$$|R \cap xR| = \lambda \quad \forall x \in E \setminus N.$$

We call R *abelian* if E is abelian, and *splitting* if N is a direct factor of E.

The final piece of preliminary 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* $\mathbf{s}$-*array* is merely a set map $\phi\colon G \to \mathbb{Z}_h$. When $h = 2$, the array is *binary*. For $w \in G$, we define the *periodic autocorrelation at shift* w of an array ϕ, denoted $AC_\phi(w)$, by

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

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

Now we have the ingredients to state the fundamental motivating result, extracted mostly from [9].

Theorem 1 *Suppose that h divides q^m, and let f be a map $\mathbb{Z}_q^m \to \mathbb{Z}_h$. The following are equivalent.*

1. *f is a GBF.*
2. *$\left[\zeta_h^{f(x-y)}\right]_{x,y} \in \mathrm{BH}(q^m, h)$ is equivalent to a coboundary matrix indexed by $\mathbb{Z}_q^m$.*
3. *f is a perfect h-ary $(q, \ldots, q)$-array.*
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 $\mathbb{Z}_h \times \mathbb{Z}_q^m$.*

We investigate the effect on the equivalences of Theorem 1 when non-splitting abelian relative difference sets are considered in point 4; i.e., non-coboundary cocyclic Butson matrices are considered in point 2. To that end, we need some more specialized material.

Jedwab [5] introduced *generalized* perfect binary arrays (GPBA), and showed that each GPBA is equivalent to a certain non-splitting abelian relative difference set. Hughes [4] later identified its orthogonal cocycle arising from the relevant central extension. We recast these ideas for h-ary arrays (cf. [1, Section 3]).

Definition 1 Let $\mathbf{s}$, G, be as above, and let $\mathbf{z} = (z_1, \ldots, z_m) \in \{0,1\}^m$. The *expansion* of an array $\phi\colon G \to \mathbb{Z}_h$ *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

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

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

Remark 2 The definition above reduces to the one in [5] when $h = 2$.

We isolate the following subgroups of E as in Definition 1:

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

Proposition 1 *Let ϕ be a h-ary $\mathbf{s}$-array and let ϕ' be its expansion of type $\mathbf{z}$. Then*

$$AC_{\phi'}(g) = \zeta_h^{-b}\, AC_{\phi'}(0) = \zeta_h^{-b} \prod_{i=1}^{m} (z_i(h-1)+1)s_i \quad \forall g \in L,$$

where $b = \sum_i g_i/s_i$ for $g = (g_1, \ldots, g_m) \in L$. Furthermore, if $g \notin L$ then $|AC_{\phi'}(g)| < |AC_{\phi'}(0)|$.

Let $\mathbf{z} \neq \mathbf{0}$. We have a short exact sequence

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

where $\beta(g + K) = g \mod \mathbf{s}$ and ι sends ζ_h to a generator of $L/K \cong \mathbb{Z}_h$. In the standard way, (1) determines a cocycle $\mu_{\mathbf{z}} \in Z^2(G, \langle \zeta_h \rangle)$ depending on the choice of a transversal map $\tau\colon G \to E/K$. We set $\tau(x) = x + K$ (with a slight abuse of notation), and then $\mu_{\mathbf{z}}(x, y) = \iota^{-1}(\tau(x) + \tau(y) - \tau(x + y))$.

Proposition 2 (cf. [4, Lemma 3.1]) *Define $\gamma_m \in Z^2(\mathbb{Z}_m, \langle \zeta_h \rangle)$ by $\gamma_m(j,k) = \zeta_h^{\lfloor (j+k)/m \rfloor}$, evaluating the exponent as an ordinary integer. Then $\mu_{\mathbf{z}}(x, y) = \prod_{z_i=1} \gamma_{s_i}(x_i, y_i)$.*

Example 1 Let $A_0 = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right]$ and $A_1 = \left[\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right]$. The binary map A on $\mathbb{Z}_2^3$ with layers A_0 and A_1 (A_i denotes the layer on $\{i\} \times \mathbb{Z}_2 \times \mathbb{Z}_2$) is a GPBA$(2,2,2)$ of type $\mathbf{z} = (1,1,1)$. Its (orthogonal) cocycle is $\mu_{\mathbf{z}} \partial_2 \partial_3 \partial_4 \partial_6$, where ∂_i is the coboundary associated to the multiplicative Kronecker delta ϕ_i of α_i, with $\alpha_1 = (0,0,0)$, $\alpha_2 = (0,0,1)$, and so on.

Definition 2 A h-ary $\mathbf{s}$-array ϕ is a *generalized perfect h-ary $\mathbf{s}$-array of type* $\mathbf{z}$ if $AC_{\phi'}(g) = 0$ for all $g \in E \setminus L$; in short, we say that ϕ is a GPhA$(\mathbf{s})$.

Remark 3 If $\mathbf{z} = \mathbf{0}$ then a GPhA$(\mathbf{s})$ is a perfect h-ary $\mathbf{s}$-array.

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

Mesnager, Tang, and Qi in [7] extend the notion of GBF to that of generalized plateaued function $f\colon \mathbb{Z}_p^m \to \mathbb{Z}_{p^k}$, p prime. Our main result, as follows, connects these functions to GPBFs, and 'lifts' Theorem 1.

Theorem 2 *Let h be a prime and q be a multiple of h. Further, let $\phi\colon \mathbb{Z}_q^m \to \mathbb{Z}_h$ be a map and $\phi'\colon \mathbb{Z}_{hq}^m \to \mathbb{Z}_h$ be the expansion of ϕ for $\mathbf{z} = (1, 1, \ldots, 1)$. The following are equivalent.*

1. *ϕ' is a GPBF.*
2. *$\mu_{\mathbf{z}}\partial\phi$ is orthogonal, i.e., $M_{\mu_{\mathbf{z}}\partial\phi} \in \mathrm{BH}(q^m, h)$.*
3. *ϕ is a $\mathrm{GPhA}(q^m)$ of type $\mathbf{z} = (1, 1, \ldots, 1)$.*
4. *$\{g + K \in E/K \mid \phi'(g) = 0\}$ is a non-splitting $(q^m, h, q^m, q^m/h)$-relative difference set in E/K with forbidden subgroup H/K.*
5. *ϕ' is a generalized plateaued function, i.e.,*

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

where $\mathcal{F} := \{v = (v_1, \ldots, v_m) \in \mathbb{Z}_{hq}^m \mid v_i \equiv 1 \mod q \ \forall\, i, 1 \le i \le m\}$.

Corollary 1 *A necessary condition for existence of a $\mathrm{GPhA}(q^m)$ of type $\mathbf{z} = (1, 1, \ldots, 1)$ is $h = q$.*

Remark 4 Regarding point 4 of Theorem 2, cf. the conditions outlined in [8] for existence of relative difference sets in abelian p-groups.

Remark 5 If $h = q$ in Theorem 2, then $|L| \cdot |\mathcal{F}| = (hq)^m$. This identity is the condition under which in [11, Definition 2.2] (resp., [2, Definition 1]) a map $f\colon \mathbb{Z}_q^m \to \mathbb{Z}_q$ (resp., $q = 2$) is called a generalized partially bent function. The coincidence with our Definition 3 is proved in [10, Theorem 2] for $q = 2$ and in [6, Proposition 8] for $q > 2$.

Remark 6 For even m, prime $h = q$, and $\mathbf{z} = (1, 1, \ldots, 1)$, the expansion $\phi'\colon \mathbb{Z}_{h^2}^m \to \mathbb{Z}_h$ in Theorem 2 is an $(m/2)^{\text{th}}$-order generalized plateaued function, because $(h^2 h)^m = (h^2)^{m+m/2}$ (see [6, Definition 2]).

Example 2 Let ϕ' be the expansion of the binary array in Example 1. We see that $\phi'\colon \mathbb{Z}_4^3 \to \mathbb{Z}_2$ is defined by the layers on $\{i\} \times \mathbb{Z}_4 \times \mathbb{Z}_4$ for $i = 0, 1, 2, 3$ by

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

with J denoting an all 1s matrix; i.e., $B_0 = B_2 = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$, $B_1 = B_3 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$.

Now $L = \{(0,0,0), (0,0,2), (0,2,0), (0,2,2), (2,0,0), (2,0,2), (2,2,0), (2,2,2)\}$ and

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

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

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

Therefore ϕ' is a GPBF.

References

[1] J. A. Armario and D. L. Flannery, *Generalized binary arrays from quasi-orthogonal cocycles.* Des. Codes Cryptogr. 87 (2019), no. 2, 2405–2417.

[2] C. Carlet, *Partially-bent functions.* Des. Codes Cryptogr. 3 (1993), no. 2, 135–145.

[3] W. de Launey and D. L. Flannery, *Algebraic design theory.* Math. Surveys. Monogr. 175, American Mathematical Society, Providence, RI (2011).

[4] G. Hughes, *Non-splitting abelian* $(4t, 2, 4t, 2t)$ *relative difference sets and Hadamard cocycles.* Europ. J. Combin. 21 (2000), no. 3, 323–331.

[5] J. Jedwab, *Generalized perfect arrays and Menon difference sets.* Des. Codes Cryptogr. 2 (1992), no. 1, 19–68.

[6] S. Mesnager, F. Özbudak, and A. Sınak, *Characterizations of partially bent and plateaued functions over finite fields.* Arithmetic of Finite Fields, 224–241, Lecture Notes in Comput. Sci., vol. 11321, Springer, Cham, 2018.

[7] S. Mesnager, C. Tang, and Y. Qi, *Generalized plateaued functions and admissible (plateaued) functions.* IEEE Trans. Inf. Theory 63 (2017), no. 10, 6139–6148.

[8] B. Schmidt, *On* (p^a, p^b, p^a, p^{a-b})*-relative difference sets.* J. Algebraic Combin. 6 (1997), 279–297.

[9] B. Schmidt, *A survey of group invariant Butson matrices and their relation to generalized bent functions and various other objects.* Radon Ser. Comput. Appl. Math. 23 (2019), 241–251.

[10] J. Wang, *The linear kernel of Boolean functions and partially bent functions.* Systems Sci. Math. Sci. 10 (1997), no. 1, 6–11.

[11] X. Wang, and J. Zhou, *Generalized partially bent functions.* In: Future Generation Communication and Networking (FGCN 2007). vol. 1, pp. 16–21, IEEE (2007).