Citation:
LeBel, A and Horadam, K 2008, 'Direct sums of balanced functions, perfect nonlinear functions, and orthogonal cocycles', Journal of Combinatorial Designs, vol. 16, no. 3, pp. 173-181

Direct sums of balanced functions, perfect nonlinear functions and orthogonal cocycles*

Alain LeBel and K. J. Horadam

Abstract

Determining if a direct sum of functions inherits nonlinearity properties from its direct summands is a subtle problem. Here, we correct a statement by Nyberg on inheritance of balance and we use a connection between balanced derivatives and orthogonal cocycles to generalise Nyberg's result to orthogonal cocycles. We obtain a new search criterion for PN functions and orthogonal cocycles mapping to non-cyclic abelian groups and use it to find all the orthogonal cocycles over $\mathbb{Z}_2^t,\ 2 \leq t \leq 4$. We conjecture that any orthogonal cocycle over $\mathbb{Z}_2^t, t \geq 2$, must be multiplicative.
Keywords: perfect nonlinear function, balanced function, orthogonal cocycle, relative difference set, generalized Hadamard matrix, exponential sum

1 Introduction

We assume throughout that G and C are finite groups of orders v and w, respectively, and that C is abelian of exponent m, *additively* written as a direct product $C = C_1 \times \cdots \times C_n,\ n \geq 1$.

A function $f : G \to C$ is *balanced* if $w|v$ and

$$\forall\, c \in C,\ |\{g \in G : f(g) = c\}| = v/w. \tag{1}$$

For instance, any epimorphism is balanced. The composition of two balanced functions is balanced. In particular, let $\pi_j : C \twoheadrightarrow C_j$ be the j^{th} projection epimorphism. If f is balanced, the compositions $f_j = \pi_j \circ f : G \twoheadrightarrow C_j,\ 1 \leq j \leq n$,

*The final version of this preprint is published in *J. Combin. Designs* 16: 173–181, 2008.

are all balanced. The converse is not true. In this paper we investigate conditions under which balance for f is inherited from balanced projections $f_j,\ 1 \leq j \leq n$.

Every $f : G \to C$ can be written as a direct sum[1] $f = (f_1, \ldots, f_n)$ of the projections f_j, with $(f_1, \ldots, f_n)(g) = (f_1(g), \ldots, f_n(g)),\ g \in G$. Nyberg [10, p. 381] states that for any integers $m, t, n \geq 1$, $t \geq n$, a function $f = (f_1, \ldots, f_n) : \mathbb{Z}_m^t \to \mathbb{Z}_m^n$ is balanced if and only if, for every $\mathbf{c} = (c_1, \ldots, c_n) \neq \mathbf{0} \in \mathbb{Z}_m^n$, the "inner product" $\mathbf{c} \cdot f : \mathbb{Z}_m^t \to \mathbb{Z}_m$ is balanced, where

$$(\mathbf{c} \cdot f)(\mathbf{x}) = \mathbf{c} \cdot f(\mathbf{x}) = \left(\sum_{j=1}^{n} c_j\ f_j \right)(\mathbf{x}) = \sum_{j=1}^{n} c_j\ (f_j(\mathbf{x})),\ \ \forall\, \mathbf{x} \in \mathbb{Z}_m^t. \qquad (2)$$

Whilst this is true when m is a prime p, it is not true for composite m, even for a prime power $m = p^k$, if $k > 1$ (see Corollary 2.3.2). For instance, the identity map $\mathbb{Z}_4 \to \mathbb{Z}_4$ is balanced, but the map $\mathbb{Z}_4 \to \mathbb{Z}_4$ defined by $x \mapsto 2x$ is not balanced — it is not even surjective.

The paper is organised as follows. In Section 2, the character group of C is used to derive an exponential sum generalisation (Theorem 2.2) of the balanced linear combination condition in (2), which exactly characterises when $f : G \to C$ inherits balance from the functions f_j, for *any* G and abelian C. The balanced linear combination condition applies *only* when C is elementary abelian (Corollary 2.3). In Section 3, we translate the perfect nonlinear (PN) property (i.e. f has balanced derivatives) to an orthogonality property for a class of 2-dimensional functions called cocycles. Then we characterise exactly when direct sums of cocycles inherit orthogonality (Theorem 3.3).

Theorem 3.3 provides us with a new search criterion for finding PN functions and orthogonal cocycles for *any* G and abelian C. In Section 4 the characterisation is used to find all orthogonal cocycles from $\mathbb{Z}_2^t$ to $\mathbb{Z}_2^n$ for $1 \leq n \leq t \leq 4$. For $n \geq 2$, these are all multiplicative. We conjecture this is true for all t.

Balanced functions and orthogonal cocycles are used in the search for highly nonlinear functions such as bent, PN and APN functions. In cryptography, highly nonlinear functions are used to construct keystream generators, S-box functions, components of hash algorithms and authentication codes; in sequence design, functions with low autocorrelation are used in CDMA communications systems; and in coding theory they describe good error-correcting codes. Orthogonal cocycles are also equivalent to central semiregular relative difference sets and therefore to generalised Hadamard matrices (see [11]).

[1]The direct sum is so-called to avoid confusion with the *direct product* $f_1 \times \cdots \times f_n : G_1 \times \cdots \times G_n \to C$ of functions $f_j : G_j \to C$.

2 Balance and the Fourier Transform

Recall that an irreducible *character* of an additively written finite abelian group C of exponent m is any group homomorphism from C to the multiplicatively written cyclic group $D = \langle\omega\rangle \subset \mathbb{C}$ of all complex m^{th} roots of unity, where $\omega = e^{2i\pi/m}$. The group $\widehat{C} = \mathrm{Hom}(C, D)$ of all such characters of C under multiplication is isomorphic to C. For any choice of isomorphism $\chi : C \to \widehat{C}$, we denote the image of $c \in C$ by χ_c. The identity χ_0 is the trivial homomorphism. The characters of C may therefore be expressed as exponential functions $\chi_c(d) = \omega^{K(c,d)}$ where $K : C \times C \to \mathbb{Z}_m$ is some biadditive function.

Given a choice of isomorphism χ, the *Fourier Transform (FT)* of a complex-valued function $\varphi : C \to \mathbb{C}$ is the function $\widehat{\varphi} : C \to \mathbb{C}$ given by

$$\widehat{\varphi}(c) = \sum_{c' \in C} \varphi(c')\chi_c(c'),\ c \in C. \tag{3}$$

The balance property for a function $f : G \twoheadrightarrow C$ may be reformulated in terms of its composition with the characters of C, using the FT.

Proposition 2.1 *Let C be abelian. Then $f : G \to C$ is balanced if and only if, for every $c \neq 0 \in C$,*

$$\sum_{g \in G} (\chi_c \circ f)(g) = 0.$$

Proof. (c.f. [3, Proposition 14] for G abelian.) Set $N_c = \{g \in G : f(g) = c\},\ c \in C$. Thus for any $b \in C$, $\sum_{g\in G}(\chi_b \circ f)(g) = \sum_{c\in C} |N_c|\chi_b(c)$. If f is balanced, $|N_c| = v/w$ is constant, so for $b \neq 0 \in C$, $\sum_{g\in G}(\chi_b \circ f)(g) = v/w \sum_{c\in C} \chi_b(c) = 0$. Conversely, if $\sum_{g\in G}(\chi_b \circ f)(g) = 0$ for all $b \neq 0 \in C$ then the function $N : C \to \mathbb{C}$ given by $N(c) = |N_c| \in \mathbb{Z}$ has FT $\widehat{N}(b) = \sum_{c\in C} N(c)\chi_b(c) = 0$ for all $b \neq 0 \in C$. Therefore, applying the inverse FT, $N(c) = w^{-1} \sum_{b\in C} \widehat{N}(b)\overline{\chi_b(c)}$ = $w^{-1}\widehat{N}(0)\overline{\chi_0(c)} = \widehat{N}(0)/w$, a constant for all $c \in C$, and f is balanced. □

When $C = C_1 \times \cdots \times C_n$ and C_j has exponent m_j, where $m_j | m$, select $\omega_j = \omega^{m/m_j} = e^{2i\pi/m_j}$ as the m_j^{th} root of unity used to define the character group $\widehat{C_j}$. Given an isomorphism $\chi_j : C_j \to \widehat{C_j},\ j = 1, \ldots, n$, there are biadditive functions $K_j : C_j \times C_j \to \mathbb{Z}_{m_j}$ such that $(\chi_j)_{c_j}(d_j) = \omega_j^{K_j(c_j,d_j)}$ for all $c_j,\ d_j \in C_j$. Then the isomorphism $\chi : C \to \widehat{C}$ must be given, for all $\mathbf{c} = (c_1, c_2, \ldots, c_n)$ and

$\mathbf{d} = (d_1, d_2, \ldots, d_n)$ in C, by

$$\chi_{\mathbf{c}}(\mathbf{d}) = \prod_{j=1}^{n} (\chi_j)_{c_j}(d_j) = \omega^{K(\mathbf{c},\mathbf{d})}, \;\; where \;\; K(\mathbf{c},\mathbf{d}) = \sum_{j=1}^{n} K_j(c_j, d_j) m/m_j. \tag{4}$$

Combining (4) with Proposition 2.1 we have the following result.

Theorem 2.2 *Let $C = C_1 \times \cdots \times C_n$, where C_j has exponent m_j. With the notation above, $f : G \to C$ is balanced if and only if, in $\mathbb{C}$, for every $\mathbf{c} \neq \mathbf{0} \in C$,*

$$\sum_{g \in G} \omega^{K(\mathbf{c}, f(g))} = 0, \;\; where \;\; K(\mathbf{c}, f(g)) = \sum_{j=1}^{n} K_j(c_j, f_j(g)) m/m_j. \qquad \square$$

Note that C may be isomorphic to several different direct products. This variation can be useful in other applications, such as the weighted Galois Ring trace [6], but here we restrict to factorisations in which the direct factors are all cyclic.

When $C = \mathbb{Z}_w$ is itself cyclic (so $m = w$) and $c \in \mathbb{Z}_w$, we choose χ to be $\chi_c(1) = \omega^c$, so $\chi_c(d) = \omega^{cd}$, $d \in \mathbb{Z}_w$ and $K(c, d) = cd$. Under the isomorphism $D \cong \mathbb{Z}_w$ given by $\omega \mapsto 1$, χ_c is multiplication by c. When $C = C_1 \times \cdots \times C_n$ and $C_j = \mathbb{Z}_{m_j}$, then by (4), for all $\mathbf{c} = (c_1, c_2, \ldots, c_n)$, $\mathbf{d} = (d_1, d_2, \ldots, d_n) \in C$, we have

$$\chi_{\mathbf{c}}(\mathbf{d}) = \omega^{\mathbf{c} * \mathbf{d}}, \;\; where \;\; \mathbf{c} * \mathbf{d} = \sum_{j=1}^{n} c_j d_j m/m_j. \tag{5}$$

In particular, when $m_j = m$ for all $1 \leq j \leq n$, $\mathbf{c} * \mathbf{d} = \mathbf{c} \cdot \mathbf{d} = \sum_{j=1}^{n} c_j d_j$.

Corollary 2.3 *Let $C = \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n}$ have order w and exponent m and let $\omega = e^{2i\pi/m}$.*

1. *$f : G \to C$ is balanced if and only if, in $\mathbb{C}$, for every $\mathbf{c} \neq \mathbf{0} \in C$, $\sum_{g \in G} \omega^{\mathbf{c} * f(g)} = 0$.*
2. *Let $C = \mathbb{Z}_m^n$ and $f : G \to \mathbb{Z}_m^n$. If $\mathbf{c} \cdot f$ is balanced for every $\mathbf{c} \neq \mathbf{0} \in C$, f is balanced. If f is balanced, $\mathbf{c} \cdot f$ is balanced for every $\mathbf{c} \neq \mathbf{0} \in C$ only if $m = p$ is prime.*

Proof. 2. If $\mathbf{c} \cdot f$ is balanced, $\mathbf{c} \neq \mathbf{0}$, then $\sum_{g \in G} \omega^{\mathbf{c} \cdot f(g)} = v/m \, (\sum_{i=0}^{m-1} \omega^i) = 0$. The mapping $K_{\mathbf{c}} : C \to \mathbb{Z}_m$ defined by $K_{\mathbf{c}}(\mathbf{d}) = \mathbf{c} \cdot \mathbf{d}$ is an epimorphism for every $\mathbf{c} \neq \mathbf{0}$ if and only if m is prime. Therefore, if f is balanced, the composite $K_{\mathbf{c}} \circ f = \mathbf{c} \cdot f$ is balanced for every $\mathbf{c} \neq \mathbf{0}$, only if m is prime. $\square$

When $m = p$ and $G = \mathbb{Z}_p^t$ in Corollary 2.3.2, we recover Nyberg's linear combination condition (2). It is clear that the condition fails for composite m.

3 Direct sums of PN functions and orthogonal cocycles

The (left) *derivative* of a function $\phi : G \to C$ *in direction* g is the function $(\Delta\phi)_g : G \to C$ defined by $(\Delta\phi)_g(h) = \phi(gh) - \phi(h)$. The function ϕ is *perfect nonlinear (PN)* if $(\Delta\phi)_g$ is balanced for every $g \neq 1 \in G$.

When ϕ is PN and $w = v$, it is a *planar* function, and it is conjectured that v must be a prime power. When G is abelian, this conjecture is known to hold [1]. When $G = C$ is cyclic, v must be odd and square-free (see [8]) so v must be an odd prime. Nyberg's original PN functions [10, Def. 3.1] have $G = \mathbb{Z}_m^t$ and $C = \mathbb{Z}_m^n$, $n \leq t$. When $n = t$, examples of such PN functions exist when m is an odd prime p but they cannot exist when $m = 2$, since

$$(\Delta\phi)_g(h) = \phi(g + h) + \phi(h) = (\Delta\phi)_g(g + h) \tag{6}$$

and $(\Delta\phi)_g$ is at best an APN (two-to-one) function.

There is a natural differential operator ∂ which maps 1D functions ϕ to 2D functions $\partial\phi$ called coboundaries, which are the simplest form of 2D cocycles.

Given a function $\phi : G \to C$, define $\partial\phi : G \times G \to C$ to be

$$\partial\phi(g, h) = \phi(gh) - \phi(g) - \phi(h),\ g, h \in G. \tag{7}$$

A function $\partial\phi$ satisfying (7) is called a *coboundary*. The function ϕ is *normalised* if $\phi(1) = 0$, and then $\partial\phi(1, g) = \partial\phi(g, 1) = 0,\ g \in G$. The coboundaries $\partial\phi$ are the simplest members of a set of 2D functions which are known as *cocycles*. A (2-dimensional) *cocycle* is a mapping $\psi : G \times G \to C$ satisfying

$$\psi(g, h) + \psi(gh, k) \ = \ \psi(g, hk) + \psi(h, k),\ \ \forall\, g, h, k \in G. \tag{8}$$

This implies $\psi(g, 1) \ = \ \psi(1, h) \ = \ \psi(1, 1),\ \forall g, h \in G$, and we assume, as is standard, that ψ is *normalised*; that is, $\psi(1, 1) = 0$. For fixed G and C, the set of cocycles forms an abelian group $Z^2(G, C)$ under pointwise addition and the coboundaries form a subgroup $B^2(G, C)$.

Clearly,

$$\phi \text{ is PN} \Leftrightarrow \forall\, g \neq 1 \in G,\ c \in C, \quad |\{h \in G : \partial\phi(g,h) = c\}| = v/w. \qquad (9)$$

The condition on coboundaries $\partial\phi$ in (9) which translates perfect nonlinearity of ϕ is called *orthogonality*. It extends to cocycles without difficulty [11]: a cocycle $\psi \in Z^2(G,C)$ is orthogonal if $|\{h \in G : \psi(g,h) = c\}| = v/w$ $\forall\, g \neq 1 \in G,\ c \in C$. By (1), the following definition is equivalent.

Definition 3.1 *For $\psi \in Z^2(G,C)$ define $\psi_g : G \to C$ for each $g \in G$ to be*

$$\psi_g(h) = \psi(g,h), \ \ \forall\, h \in G.$$

We say $\psi \in Z^2(G,C)$ is orthogonal *if ψ_g is balanced for all $g \neq 1 \in G$.*

If $C = C_1 \times C_2$, $\psi \in Z^2(G,C_1)$ and $\varphi \in Z^2(G,C_2)$, then $(\psi,\varphi) \in Z^2(G,C)$. Conversely, every cocycle $\psi \in Z^2(G,C)$, $C = C_1 \times \ldots \times C_n$, is a direct sum of cocycles $\psi_j = \pi_j \circ \psi \in Z^2(G,C_j)$, $1 \leq j \leq n$.

If $\psi \in Z^2(G,C)$ is orthogonal and $\gamma : C \twoheadrightarrow D$ is an epimorphism of abelian groups then $\gamma \circ \psi \in Z^2(G,D)$ is orthogonal. Hence each of the cocycles ψ_j is orthogonal. However, the converse does not hold. For instance if ψ_j is orthogonal, the cocycle $(\psi_j,\psi_j) : G \times G \to C_j \times C_j$ is not even surjective. Thus an orthogonal cocycle cannot have any repeated direct factors. We record some straightforward consequences when ψ is orthogonal.

Proposition 3.2 *Assume $\psi = (\psi_1,\ldots,\psi_n) \in Z^2(G, C_1 \times \ldots \times C_n)$, $n \geq 2$, is orthogonal. Then each $\psi_j \in Z^2(G,C_j)$ is orthogonal. Further,*

1. *If $i \neq j$ but there is an isomorphism $\alpha : C_i \cong C_j$, then $\alpha \circ \psi_i \neq \psi_j$.*
2. *If $C_j = \mathbb{Z}_r$ and $k \in \mathbb{Z}_r$, then the scalar multiple $k\psi_j$ is orthogonal if and only if $(k,r) = 1$.*
3. *If p is prime and $C_j = \mathbb{Z}_p$, $1 \leq j \leq n$, then every nontrivial $\mathbb{Z}_p$-linear combination $\sum_{j=1}^n c_j\psi_j$ is an orthogonal cocycle in $Z^2(G,\mathbb{Z}_p)$.*

Proof. 1. Suppose that $\alpha \circ \psi_i = \psi_j$. Let γ be the epimorphism $\gamma : C_1 \times \cdots \times C_n \to C_j \times C_j$ which sends factors C_k, for $k \neq i,j$, to the identity, is the identity on C_j and is α on C_i. Then $\gamma \circ \psi = (\psi_j,\psi_j)$ is orthogonal, a contradiction. 2. This follows from the surjectivity or otherwise of $\mathbb{Z}_r \to k\mathbb{Z}_r$. 3. Every nontrivial

$\mathbb{Z}_p$-linear combination $\sum_{j=1}^{n} c_j\psi_j$ is a composition $c \circ (\psi_1, \ldots, \psi_n)$ of ψ with the epimorphism $c : \mathbb{Z}_p^n \to \mathbb{Z}_p$, where c takes the j^{th} unit vector of $\mathbb{Z}_p^n$ to c_j, with at least one $c_j \neq 0$ and, vice versa, every epimorphism is of this form. □

Now we can show that orthogonality of a cocycle $\psi = (\psi_1, \ldots, \psi_n)$ is an exponential sum property of nontrivial weighted linear combination cocycles formed from its direct summands ψ_j.

Theorem 3.3 *Let G be a group of order v, let $C = \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n}$, $m_j \geq 2$, $1 \leq j \leq n$, be an abelian group of exponent m and order w, where $w|v$ and let $\omega = e^{2i\pi/m}$. Let $\psi = (\psi_1, \ldots, \psi_n) \in Z^2(G, C)$ and for every $\mathbf{c} = (c_1, \ldots, c_n) \in C$, define $\mathbf{c} * \psi \in Z^2(G, \mathbb{Z}_m)$ to be*

$$(\mathbf{c} * \psi)(g, h) = \sum_{j=1}^{n} c_j \, \psi_j(g, h) \, m/m_j, \quad g, h \in G.$$

1. *Then ψ is orthogonal if and only if, for each $\mathbf{c} \neq \mathbf{0} \in C$, the cocycle $\mathbf{c} * \psi$ satisfies*
$$\sum_{g \in G} \omega^{(\mathbf{c}*\psi)_d(g)} = 0, \quad \forall \, d \neq 1 \in G. \tag{10}$$

2. *If $\psi = \partial\phi = (\partial\phi_1, \ldots, \partial\phi_n) \in B^2(G, C)$ then $\phi : G \to C$ is PN if and only if, for each $\mathbf{c} \neq \mathbf{0} \in C$,*
$$\sum_{g \in G} \omega^{\mathbf{c}*(\Delta\phi)_d(g)} = 0, \quad \forall \, d \neq 1 \in G. \tag{11}$$

Proof. By Definition 3.1 and Corollary 2.3, ψ is orthogonal if and only if, for each $d \neq 1 \in G$,

$$\sum_{g \in G} \omega^{\mathbf{c}*\psi_d(g)} = 0, \quad \forall \, \mathbf{c} \neq 0 \in C$$

and the result follows since $\mathbf{c} * \psi_d(g) = (\mathbf{c} * \psi)(d, g) = (\mathbf{c} * \psi)_d(g)$. If $\psi = \partial\phi$ then $\sum_{g \in G} \omega^{(\mathbf{c}*\psi)_d(g)} = \omega^{-\mathbf{c}*\phi(d)} \sum_{g \in G} \omega^{\mathbf{c}*(\Delta\phi)_d(g)}$ and this sum is 0 if and only if $\sum_{g \in G} \omega^{\mathbf{c}*(\Delta\phi)_d(g)} = 0$. □

Theorem 3.3.2 generalises [3, Theorem 16]: if G is abelian then $\phi : G \to C$ is PN if and only if, for every $c \neq 0 \in C$, $\chi_c \circ \phi$ is bent.

In the simple special case that C is an elementary abelian group, condition (10) is equivalent to the inner product cocycle $\mathbf{c} \cdot \psi$ being orthogonal.

Theorem 3.4 *Let G be a group of order v and p a prime such that $p^n|v$. Let $\psi = (\psi_1, \ldots, \psi_n)$ in $Z^2(G, \mathbb{Z}_p^n)$, where $\psi_j \in Z^2(G, \mathbb{Z}_p)$, $1 \leq j \leq n$. Then ψ is orthogonal if and only if each non-trivial $\mathbb{Z}_p$–linear combination of cocycles $\sum_{j=1}^n c_j\psi_j$ in $Z^2(G, \mathbb{Z}_p)$ is orthogonal.*

Proof. Proposition 3.2.3 gives one direction. For the other, if, for every $\mathbf{c} \neq \mathbf{0} \in \mathbb{Z}_p^n$, the cocycle $\mathbf{c} \cdot \psi = \sum_{j=1}^n c_j\psi_j$ is orthogonal then by Definition 3.1 for every $\mathbf{c} \neq \mathbf{0} \in \mathbb{Z}_p^n$, $\mathbf{c} \cdot \psi_d \ (= (\mathbf{c} \cdot \psi)_d \ )$ is balanced $\forall\, d \neq 1 \in G$. By Corollary 2.3.2, ψ_d is balanced $\forall\, d \neq 1 \in G$ and so ψ is orthogonal by Definition 3.1. □

A cocycle is *multiplicative* if it is a homomorphism when restricted to either coordinate (and hence, by (8), to both coordinates).

For a multiplicative $\psi \in Z^2(G, \mathbb{Z}_p^n)$, Theorem 3.4 is already known (c.f. MacDonald [9]), in terms of the matrix representations of the bilinear forms ψ_j, since necessarily G is abelian and $G \cong \mathbb{Z}_p^t$.

Corollary 3.5 *Let $t \geq n$, let $\psi = (\psi_1, \ldots, \psi_n)$ in $Z^2(\mathbb{Z}_p^t, \mathbb{Z}_p^n)$ be multiplicative, and represent the bilinear form ψ_j by matrix M_j, $1 \leq j \leq n$. Then ψ is orthogonal if and only if every non-trivial $\mathbb{Z}_p$–linear combination of the M_j is non-singular; that is, if and only if, for any $(c_1, c_2, \ldots, c_n) \neq 0 \in \mathbb{Z}_p^n$, $\sum_{j=1}^n c_j M_j \in GL(t, p)$.*

By the results above, we have a new search criterion for PN functions and orthogonal cocycles, and therefore also for central relative difference sets and G-cocyclic generalised Hadamard matrices with entries in C.

First, by Proposition 3.2 it is necessary to find n distinct orthogonal cocycles $\psi_j : G \times G \to \mathbb{Z}_{m_j}$, $1 \leq j \leq n$. Then the direct sum $\psi = (\psi_1, \ldots, \psi_n) : G \times G \to C = \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n}$ may be tested for orthogonality using (10). If all the cocycles are coboundaries $\psi_j = \partial\phi_j$, this is a test for constructing a PN function $\phi = (\phi_1, \ldots, \phi_n)$ from n PN direct summands ϕ_j.

4 Computations for elementary abelian 2-groups

The direct sum criterion is applied to elementary abelian 2-groups $G = \mathbb{Z}_2^t$, $C = \mathbb{Z}_2^n$, as the smallest cases for which exhaustive search quickly exceeds our computational resources. Of course, none of the orthogonal cocycles found when $t = n$ can be coboundaries, since by (6) and (7), no $(\partial\phi)_g$, for $g \in G$, can be one-to-one. The results in [7] reported here were computed using MAGMA [2].

t	1	2	3	4	5
x	1	6	168	$20,160$	$9,999,360$
o	1	6	168	$26,880$	$\approx 7.34 \times 10^7$
x/o	1	1	1	0.75	≈ 0.136
z	2	16	1024	$2^{21} \approx 2.1 \times 10^6$	$2^{41} \approx 2.2 \times 10^{12}$
o/z	0.5	0.375	≈ 0.164	$\approx 1.28 \times 10^{-2}$	$\approx 3.34 \times 10^{-5}$

Table 1: Number x of multiplicative orthogonal cocycles versus number o of orthogonal cocycles and total number z of cocycles in $Z^2(\mathbb{Z}_2^t, \mathbb{Z}_2)$

For $G = \mathbb{Z}_2^t$, $t \leq 4$, Table 1 lists the number $x = |GL(t, 2)|$ of multiplicative orthogonal cocycles in $Z^2(\mathbb{Z}_2^t, \mathbb{Z}_2)$ and the total number o of orthogonal cocycles found by exhaustive checking. For $t = 5$, o is estimated by Monte Carlo sampling. The total number of cocycles $z = 2^{2^t - 1 + t(t-1)/2} = |Z^2(\mathbb{Z}_2^t, \mathbb{Z}_2)|$ is included for comparison purposes. When t is even and $n < t$, some of the orthogonal cocycles will be orthogonal coboundaries, corresponding to the binary PN (that is, bent) functions.

From Table 1, all orthogonal cocycles in $Z^2(\mathbb{Z}_2^t, \mathbb{Z}_2)$ with $1 \leq t \leq 3$ are multiplicative. Hence all orthogonal cocycles in $Z^2(\mathbb{Z}_2^t, \mathbb{Z}_2^n)$ with $1 < n \leq t \leq 3$ are multiplicative, otherwise projection onto one factor would give a contradiction.

Theorem 3.4 was applied in [7] to find all the orthogonal cocycles in $Z^2(\mathbb{Z}_2^t, \mathbb{Z}_2^n)$ with $1 < n \leq t \leq 4$, using the orthogonal cocycles in $Z^2(\mathbb{Z}_2^t, \mathbb{Z}_2)$ found in the computation of Table 1. Direct exhaustive search for these is beyond our computational resources.

For example, the direct sums of every pair of orthogonal cocycles in $Z^2(\mathbb{Z}_2^4, \mathbb{Z}_2)$ have been tested. There are $22,575,840$ cocycles $\mathbb{Z}_2^4 \times \mathbb{Z}_2^4 \to \mathbb{Z}_2^2$ formed from the direct sum of two non-multiplicative orthogonal cocycles and $135,475,200$ formed from the direct sum of a multiplicative orthogonal cocycle and a non-multiplicative orthogonal cocycle. None of these direct sums is orthogonal. Thus, there are no non-multiplicative orthogonal cocycles in $Z^2(\mathbb{Z}_2^4, \mathbb{Z}_2^2)$. This implies (by projection, again) all orthogonal cocycles in $Z^2(\mathbb{Z}_2^4, \mathbb{Z}_2^3)$ and $Z^2(\mathbb{Z}_2^4, \mathbb{Z}_2^4)$ are multiplicative.

Lemma 4.1 *When $2 \leq n \leq t \leq 4$, all orthogonal cocycles in $Z^2(\mathbb{Z}_2^t, \mathbb{Z}_2^n)$ are multiplicative.*

All the orthogonal cocycles when $t = n$ are then computed by applying Theorem 3.4 to direct sums of distinct multiplicative orthogonal cocycles.

Lemma 4.2 *(Compare with Table 1) The total number o of orthogonal cocycles in $Z^2(\mathbb{Z}_2^n, \mathbb{Z}_2^n)$, $1 \leq n \leq 4$, is tabulated. In each case, they are all multiplicative.*

n	1	2	3	4
o	1	12	$96,768$	$2,160,666,869,760$
		[5]		$\approx 2.2 \times 10^{12}$

We conjecture that for $n > 1$, any orthogonal cocycles on elementary abelian 2-groups must be multiplicative.

Conjecture 4.3 *For $2 \leq n \leq t < \infty$, any orthogonal cocycle in $Z^2(\mathbb{Z}_2^t, \mathbb{Z}_2^n)$ is multiplicative.*

For odd primes, this is not true, even for $G = \mathbb{Z}_3^4$. When $p = 3$, the Coulter-Matthews PN function [4] determines an orthogonal coboundary in $Z^2(\mathbb{Z}_3^{2k}, \mathbb{Z}_3^{2k})$ which is not multiplicative.

Acknowledgements. Theorem 3.4 (with a different proof, see [7, Theorem 6.2]) and the results in Section 4 form part of the PhD thesis [7] of the first author, taken under the supervision of the second author.

The authors thank the anonymous referee for very helpful comments which improved the clarity and streamlined the exposition.

References

[1] A. Blokhuis, D. Jungnickel and B. Schmidt, Proof of the prime power conjecture for projective planes of order n with abelian collineation groups of order n^2, *Proc. Amer. Math. Soc.* 130 (2002) 1473–1476.

[2] W. Bosma, J. Cannon and C. Playoust, The MAGMA algebra system I: the user language, *J. Symbol. Comp.* 24 (1997) 235–265.

[3] C. Carlet and C. Ding, Highly nonlinear mappings, *J. Complexity* 20 (2004) 205–244.

[4] R. S. Coulter and R. W. Matthews, Planar functions and planes of Lenz-Barlotti Class II, *Des., Codes Cryptogr.* 10 (1997) 167–184.

[5] K. J. Horadam, Equivalence classes of central semiregular relative difference sets, *J. Combin. Des.* 8 (2000) 330–346.

[6] K. J. Horadam and A. Rao, Fourier Transforms from a weighted trace map, *Proc. 2006 ISIT*, IEEE (2006) 1080-1084.

[7] A. LeBel, Shift actions on 2-cocycles, Ph. D. Thesis, RMIT University, Melbourne, Australia, 2005.

[8] K. H. Leung, S. L. Ma and V. Tan, Planar functions from $\mathbb{Z}_n$ to $\mathbb{Z}_n$, *J. Algebra*, 224 (2000) 427–436.

[9] I. D. MacDonald, Some p-groups of Frobenius and extra-special type, *Israel J. Math.* 40 (1981) 350–364.

[10] K. Nyberg, Perfect nonlinear S-boxes, in: EUROCRYPT-91, LNCS 547, Springer, New York, 1991, 378–385.

[11] A. A. I. Perera and K. J. Horadam, Cocyclic generalised Hadamard matrices and central relative difference sets, *Des., Codes Cryptogr.* 15 (1998) 187–200.

Key Words and Phrases: Perfect nonlinear function, balanced function, orthogonal cocycle, relative difference set, generalised Hadamard matrix, exponential sum.

2000 AMS Classification: Primary 94A60, 94A55; Secondary 20J06

Affiliation of authors: Mathematical Sciences, SMGS, RMIT University, Melbourne, AUSTRALIA
Email addresses: Alain.LeBel@bigpond.com, Kathy.Horadam@rmit.edu.au

Preferred Mailing Address of Contact Author:

Prof. K. J. Horadam
Mathematical Sciences, SMGS
RMIT University - City Campus
GPO Box 2476V
Melbourne, VIC 3001
AUSTRALIA

Telephone +61 3 9925 2283
Fax +61 3 9925 2454
Email Kathy.Horadam@rmit.edu.au