Des. Codes Cryptogr. (2017) 82:543–558
DOI 10.1007/s10623-016-0177-8

Fourier transforms and bent functions on faithful actions of finite abelian groups

Yun Fan[1] · **Bangteng Xu**[2]

Received: 18 June 2015 / Revised: 1 October 2015 / Accepted: 6 January 2016 /
Published online: 23 January 2016

Abstract Let G be a finite abelian group acting faithfully on a finite set X. The G-bentness and G-perfect nonlinearity of functions on X are studied by Poinsot and co-authors (Discret Appl Math 157:1848–1857, 2009; GESTS Int Trans Comput Sci Eng 12:1–14, 2005) via Fourier transforms of functions on G. In this paper we introduce the so-called G-dual set $\widehat{X}$ of X, which plays the role similar to the dual group $\widehat{G}$ of G, and develop a Fourier analysis on X, a generalization of the Fourier analysis on the group G. Then we characterize the bentness and perfect nonlinearity of functions on X by their own Fourier transforms on $\widehat{X}$. Furthermore, we prove that the bentness of a function on X can be determined by its distance from the set of G-linear functions. As direct consequences, many known results in Logachev et al. (Discret Math Appl 7:547–564, 1997), Carlet and Ding (J Complex 20:205–244, 2004), Poinsot (2009), Poinsot et al. (2005) and some new results about bent functions on G are obtained. In order to explain the theory developed in this paper clearly, examples are also presented.

Keywords Group actions · G-linear functions · G-dual sets · Fourier transforms on G-sets · Bent functions · Perfect nonlinear functions

Mathematics Subject Classification 43A25 · 11T71 · 20C99

Communicated by A. Pott.

✉ Bangteng Xu
bangteng.xu@eku.edu

Yun Fan
yfan@mail.ccnu.edu.cn

[1] School of Mathematics and Statistics, Central China Normal University, Wuhan 430079, China

[2] Department of Mathematics & Statistics, Eastern Kentucky University, Richmond, KY 40475, USA

1 Introduction

Bent functions, perfect nonlinear functions, and their generalizations have been studied in many papers. The notion of a Boolean bent function was introduced by Rothaus [10]. More than a decade ago, Logachev et al. [4] generalized this concept to bent functions on finite abelian groups. As a further generalization, Poinsot [5] studied bent functions on finite non-abelian groups. Recently, a closely related notion, perfect nonlinear functions between finite abelian groups as well as between arbitrary finite groups, has been studied in quite a few papers; for example, see [2,8,9,12–15]. These functions have numerous applications in cryptography, coding theory, and other fields. A critical tool in these studies is the Fourier analysis on finite groups.

Let G and H be finite abelian groups, and let $f : G \to H$ be a function. The perfect nonlinearity of f is defined via its derivatives $f'_\alpha : G \to H$, $x \mapsto f(\alpha x)f(x)^{-1}$, for all non-identity $\alpha \in G$, and characterized by the bentness of the complex functions $\xi \circ f$, for all non-trivial irreducible characters ξ of H. Fourier transforms of complex functions on the group G play a key role. Poinsot et al. [6,7] generalized the perfect nonlinearity to a function $g : X \to H$, where X is a finite set with an action of G on it (such X is called a *G-set*). The derivatives of g are defined by $g'_\alpha : X \to H$, $x \mapsto f(\alpha x)f(x)^{-1}$, for any $\alpha \in G$. By introducing functions $g_x : G \to H, \alpha \mapsto g(\alpha x)$, for all $x \in X$, and using the Fourier transforms of g_x, Poinsot et al. [6,7] obtained the characterizations of the perfect nonlinearity of g (see Corollaries 4.12 and 5.4 below).

Our concern in this research is how to establish the Fourier analysis on a finite G-set X, as a generalization of the classical Fourier analysis on the finite abelian group G, and use it as a tool to study the bentness and perfect nonlinearity of functions on X.

The set of functions from the G-set X to the complex field $\mathbb{C}$, denoted by $\mathbb{C}^X$, is a $\mathbb{C}G$-module, where $\mathbb{C}G$ is the group algebra of G over $\mathbb{C}$. $\mathbb{C}^X$ is also a unitary space with the usual Hermitian inner product. The canonical decomposition of $\mathbb{C}^X$ is the orthogonal direct sum of the ψ-components $(\mathbb{C}^X)_\psi$, where ψ are irreducible characters of G. Using this decomposition we obtain an orthogonal basis $\widehat{X}$ of $\mathbb{C}^X$ which consists of G-linear functions and is closed under complex conjugation (see Theorem 2.3 below). Such a basis $\widehat{X}$, called a G-dual set of X, plays a role in $\mathbb{C}^X$ similar to the dual group of G, $\widehat{G}$, in $\mathbb{C}^G$. We define the Fourier transform $\widehat{f}$ of $f \in \mathbb{C}^X$ as a function on $\widehat{X}$ (see Definition 3.1 below), and define the bentness of f in terms of $\widehat{f}(\lambda)$ for all $\lambda \in \widehat{X}$ (see Definition 4.1 below).

Then using the Fourier analysis on the G-set X, we study the characterizations of bent functions on X. We will prove that (Theorem 4.6) a function $f : X \to T$, where T is the unit circle in $\mathbb{C}$, is bent if and only if the derivatives of f in all nontrivial directions are balanced. Furthermore, we will prove that (Theorem 4.9) a function $f \in T^X$ is bent if and only if the distance from f to the set of G-linear functions, denoted by $(\mathbb{C}^X)_G$, reaches the best possible upper bound of the distance between $(\mathbb{C}^X)_G$ and any function in T^X. This result gives another geometric interpretation of the importance of bent functions in cryptography. The perfect nonlinearity of functions from X to a finite abelian group H is also characterized in terms of Fourier transforms of functions on X (Theorem 5.2 below). As expected, many known results in [2,4,6,7] and some new results about bentness and nonlinearity of functions on finite abelian groups are obtained as immediate consequences. To explain the theory established in this paper, several examples are also included.

The rest of the paper is organized as follows. In Sect. 2 we present the classical decomposition of the $\mathbb{C}G$-module $\mathbb{C}^X$, and prove the existence of the G-dual set $\widehat{X}$ of X. Then in Sect. 3 we introduce the Fourier transforms of functions in $\mathbb{C}^X$, and investigate their basic

properties. Section 4 is devoted to the study of the characterizations of bent functions on X. Finally, perfect nonlinear functions are discussed in Sect. 5, and explanatory examples are presented in Sect. 6.

2 G-dual sets of G-sets

Throughout the paper, let G be a finite abelian group, and let X be a finite G-set. That is, there is a map $G \times X \to X$, $(a, x) \mapsto ax$, such that $a(bx) = (ab)x$ and $1x = x$ for all $x \in X$ and $a, b \in G$, where 1 is the identity of G. Let $\mathbb{C}$ be the complex field. The complex conjugate of any $z \in \mathbb{C}$ is denoted by $\overline{z}$. Let $\mathbb{C}^X$ be the set of functions from X to $\mathbb{C}$. Then $\mathbb{C}^X$ is a vector space over $\mathbb{C}$. Let $\mathrm{GL}(\mathbb{C}^X)$ be the group of automorphisms of $\mathbb{C}^X$; that is, the elements of $\mathrm{GL}(\mathbb{C}^X)$ are bijective linear transformations of $\mathbb{C}^X$. Define

$$\rho : G \to \mathrm{GL}(\mathbb{C}^X), \quad a \mapsto \rho(a),$$

where $\rho(a)$ is defined by

$$\big(\rho(a)(f)\big)(x) := f(a^{-1}x), \quad \text{for any } f \in \mathbb{C}^X, \quad x \in X.$$

Then ρ is a group homomorphism; that is, ρ is a linear representation of G on $\mathbb{C}^X$. Let $\mathbb{C}G$ be the group algebra of G over $\mathbb{C}$. Then $\mathbb{C}^X$ is a $\mathbb{C}G$-module, with the G-action defined by

$$(\alpha f)(x) = f(\alpha^{-1}x), \quad \forall\, f \in \mathbb{C}^X \ \ \forall\, \alpha \in G \ \ \forall\, x \in X. \tag{2.1}$$

We also call $\mathbb{C}^X$ a complex G-space. Let $\widehat{G}$ be the dual group of G. For any irreducible character $\psi \in \widehat{G}$, let $(\mathbb{C}^X))_\psi$ be the sum of irreducible submodules of $\mathbb{C}^X$ that afford ψ. Since G is abelian, any irreducible character of G is also an irreducible representation of G. Hence by [11, Theorem 8, p. 21], ρ induces the canonical decomposition of $\mathbb{C}^X$ as follows:

$$\mathbb{C}^X = \bigoplus_{\psi \in \widehat{G}} (\mathbb{C}^X))_\psi,$$

and the projection $P_\psi : \mathbb{C}^X \to (\mathbb{C}^X))_\psi$ is given by

$$P_\psi(f) := \frac{1}{|G|} \sum_{a \in G} \overline{\psi(a)} \rho(a)(f), \quad \text{for any } f \in \mathbb{C}^X. \tag{2.2}$$

Therefore,

$$f = \sum_{\psi \in \widehat{G}} P_\psi(f), \quad \text{for any } f \in \mathbb{C}^X.$$

Furthermore, $f \in (\mathbb{C}^X))_\psi$ if and only if $f = P_\psi(f)$. If $f = P_\psi(f)$, then for any $a \in G$ and $x \in X$,

$$\begin{aligned} f(a^{-1}x) = P_\psi(f)(a^{-1}x) \ &= \ \frac{1}{|G|} \sum_{b \in G} \psi(b^{-1}) f(b^{-1}a^{-1}x) \\ &= \psi(a) \frac{1}{|G|} \sum_{b \in G} \psi(b^{-1}a^{-1}) f(b^{-1}a^{-1}x) \ = \ \psi(a) P_\psi(f)(x) \\ &= \psi(a) f(x). \end{aligned}$$

On the other hand, if for any $a \in G$ and $x \in X$, $f(a^{-1}x) = \psi(a) f(x)$, then $f = P_\psi(f)$. Thus,

$$(\mathbb{C}^X))_\psi = \{f \in \mathbb{C}^X \mid f(a^{-1}x) = \psi(a)f(x), \forall a \in G, \forall x \in X\}. \tag{2.3}$$

$(\mathbb{C}^X))_\psi$ is called the *ψ-component* of $\mathbb{C}^X$.

Definition 2.1 For any $\psi \in \widehat{G}$, functions in $(\mathbb{C}^X))_\psi$ are said to be *ψ-linear*. A function $f \in \mathbb{C}^X$ is said to be *G-linear* if it is ψ-linear for some $\psi \in \widehat{G}$.

The complex conjugate of a function $f \in \mathbb{C}^X$ is $\overline{f}$ defined by $\overline{f}(x) = \overline{f(x)}$, $x \in X$. It is well known that $\mathbb{C}^X$ is a unitary space with the usual Hermitian inner product: $\langle f, g\rangle = \sum_{x\in X} f(x)\overline{g}(x)$ for $f, g \in \mathbb{C}^X$. Note that

$$\langle af, g\rangle = \langle f, a^{-1}g\rangle, \quad \text{for any } a \in G,\ f, g \in \mathbb{C}^X. \tag{2.4}$$

Hence, for distinct $\psi, \varphi \in \widehat{G}$, $(\mathbb{C}^X))_\psi$ and $(\mathbb{C}^X))_\varphi$ are orthogonal. The length (or norm) $|f|$ of any $f \in \mathbb{C}^X$ is $|f| = \sqrt{\langle f, f\rangle}$. We say that a basis $u_1, \ldots, u_n$ of $\mathbb{C}^X$ is an *ℓ-normal orthogonal basis* (where ℓ is a positive real number) if $\langle u_i, u_j\rangle = \delta_{ij}\ell$, where δ_{ij} is the Kronecker delta.

Definition 2.2 A basis $\widehat{X}$ of the unitary G-space $\mathbb{C}^X$ is called a G-dual set *of* X if the following conditions are satisfied:

(i) any $\lambda \in \widehat{X}$ is G-linear;
(ii) $\widehat{X}$ is an $|X|$-normal orthogonal basis; and
(iii) $\widehat{X}$ is closed under complex conjugation, i.e. $\overline{\lambda} \in \widehat{X}$ for all $\lambda \in \widehat{X}$.

Theorem 2.3 *For any G-set X, there exists a G-dual set $\widehat{X}$.*

Proof Let $|X| = n$. Since $\overline{\psi} \in \widehat{G}$ for any $\psi \in \widehat{G}$, it follows from (2.3) that for any $f \in (\mathbb{C}^X)_\psi$, $\overline{f} \in (\mathbb{C}^X)_{\overline{\psi}}$. That is, $\overline{(\mathbb{C}^X)}_\psi = (\mathbb{C}^X)_{\overline{\psi}}$, where $\overline{(\mathbb{C}^X)}_\psi = \left\{\overline{f} \,\middle|\, f \in (\mathbb{C}^X)_\psi\right\}$. For any $\psi \in \widehat{G}$, it is known that there is an n-normal orthogonal basis $(\widehat{X})_\psi$ for the ψ-component $(\mathbb{C}^X)_\psi$ of $\mathbb{C}^X$. Hence, $\overline{(\widehat{X})}_\psi = \left\{\overline{\lambda} \,\middle|\, \lambda \in (\widehat{X})_\psi\right\}$ is also an n-normal orthogonal basis of the $\overline{\psi}$-component $(\mathbb{C}^X)_{\overline{\psi}}$. Thus, if $\psi \neq \overline{\psi}$, then $(\widehat{X})_\psi \cup \overline{(\widehat{X})}_\psi$ is an n-normal orthogonal basis of $(\mathbb{C}^X)_\psi \oplus (\mathbb{C}^X)_{\overline{\psi}}$ which is closed under complex conjugation.

In the following we prove that if $\psi = \overline{\psi}$, then there is an n-normal orthogonal basis $(\widehat{X})_\psi$ of $(\mathbb{C}^X)_\psi$ such that for any $\lambda \in (\widehat{X})_\psi$, $\lambda = \overline{\lambda}$. Let $f \in (\mathbb{C}^X)_\psi$ such that $f \neq 0$. Then at least one of $f + \overline{f}$ and $\sqrt{-1}(f - \overline{f})$ is not zero. Thus, $\overline{(\mathbb{C}^X)}_\psi = (\mathbb{C}^X)_\psi$ implies that there is a $\lambda_1 \in (\mathbb{C}^X)_\psi$ such that $\lambda_1 \neq 0$, and $\lambda_1 = \overline{\lambda}_1$. We may also assume that $\langle\lambda_1, \lambda_1\rangle = n$. Note that $(\mathbb{C}^X)_\psi = \mathbb{C}\lambda_1 \oplus (\mathbb{C}\lambda_1)^\perp$. Also for any $f \in (\mathbb{C}\lambda_1)^\perp$, it follows from $\lambda_1 = \overline{\lambda}_1$ that $\overline{f} \in (\mathbb{C}\lambda_1)^\perp$. Hence, if $(\mathbb{C}\lambda_1)^\perp \neq \{0\}$, then as above, there is $\lambda_2 \in (\mathbb{C}\lambda_1)^\perp$ such that $\lambda_2 = \overline{\lambda}_2$, $\langle\lambda_2, \lambda_2\rangle = n$, and $(\mathbb{C}\lambda_1)^\perp = \mathbb{C}\lambda_2 \oplus (\mathbb{C}\lambda_1 \oplus \mathbb{C}\lambda_2)^\perp$. Continuing this process, we see that $\lambda_1, \lambda_2, \ldots$ form an n-normal orthogonal basis of $(\mathbb{C}^X)_\psi$ which is closed under complex conjugation.

Therefore, the orthogonal direct sum $\mathbb{C}^X = \bigoplus_{\psi\in\widehat{G}}(\mathbb{C}^X)_\psi$ implies that the union $\widehat{X}$ of the n-normal orthogonal bases of the G-linear components of $\mathbb{C}^X$ chosen in the above two paragraphs is an n-normal orthogonal basis of $(\mathbb{C}^X)_\psi$ which is closed under complex conjugation. □

Remark 2.4 (i) If $\widehat{X}$ is a G-dual set of X, then $\widehat{Y} = \{\varepsilon\lambda \mid \lambda \in \widehat{X},\ \varepsilon \in T\}$ is also a G-dual set of X, where T is the unit circle in $\mathbb{C}$. We call $\widehat{Y}$ a rescaling of $\widehat{X}$ by T.

(ii) If X is a transitive G-set, then every non-zero G-linear component $(\mathbb{C}^X)_\psi$ of $\mathbb{C}^X$ is 1-dimensional, and hence $(\widehat{X})_\psi$ consists of exactly one function of length $\sqrt{n}$. Thus, X has a unique G-dual set $\widehat{X}$ up to rescaling by T. In particular, if $X = G$ is the regular

G-set, then X has a unique G-dual set up to rescaling by T. Usually, the dual group $\widehat{G}$ is chosen as $\widehat{X}$.

(iii) However, if the number of the G-orbits of X is greater that 1, then the G-dual set $\widehat{X}$ is not unique up to rescaling by T. The proof of Theorem 2.3 provides a way to chose a G-dual set. Later we will show another way to obtain a G-dual set (see Example 6.4 below).

From now on, for the G-set X we fix a G-dual set $\widehat{X}$ as follows. For any $\psi \in \widehat{G}$, let $(\widehat{X})_\psi$ be an n-normal orthogonal basis of $(\mathbb{C}^X)_\psi$ such that $\overline{(\widehat{X})_\psi} = (\widehat{X})_{\overline{\psi}}$, and let $\widehat{X} = \bigcup_{\psi\in\widehat{G}}(\widehat{X})_\psi$. So $(\mathbb{C}^X)_\psi = \bigoplus_{\lambda\in(\widehat{X})_\psi} \mathbb{C}\lambda$ for any $\psi \in \widehat{G}$. Note that some $(\widehat{X})_\psi$ may be empty (correspondingly, some component $(\mathbb{C}^X)_\psi$ may be zero).

Let $\widehat{X} = \{\lambda_1, \ldots, \lambda_n\}$ and $X = \{x_1, \ldots, x_n\}$. Then we have an $n \times n$ matrix $\Lambda = \big(\lambda_i(x_j)\big)_{1\le i,j\le n}$. The n-normal orthogonality of $\widehat{X}$ implies that $\Lambda \cdot \overline{\Lambda}^T = nI$, where I is the identity matrix and $\overline{\Lambda}^T$ is the conjugate transpose of Λ. Hence we also have $\overline{\Lambda}^T \cdot \Lambda = nI$. Thus, we have the following

Lemma 2.5 (Orthogonality Relations) *The following hold:*

$$\sum_{x\in X} \lambda(x)\overline{\mu}(x) = \begin{cases} n, & \lambda = \mu; \\ 0, & \lambda \ne \mu; \end{cases} \quad \forall\ \lambda, \quad \mu \in \widehat{X}. \tag{2.5}$$

$$\sum_{\lambda\in\widehat{X}} \lambda(x)\overline{\lambda}(y) = \begin{cases} n, & x = y; \\ 0, & x \ne y; \end{cases} \quad \forall\ x, \quad y \in X. \tag{2.6}$$

3 Fourier transforms of functions on G-sets

Given a G-set X, in this section we discuss the Fourier transform of $f \in \mathbb{C}^X$ on a G-dual set $\widehat{X}$. We will need to consider the space $\mathbb{C}^{\widehat{X}}$ of complex functions on $\widehat{X}$, which is also a unitary space with the usual inner product $\langle g, h\rangle = \sum_{\lambda\in\widehat{X}} g(\lambda)\bar{h}(\lambda),\ \forall\ g, h \in \mathbb{C}^{\widehat{X}}$.

For any $\sigma \in \mathbb{C}^G$, the Fourier transform $\widehat{\sigma}$ of σ at any $\psi \in \widehat{G}$ is $\widehat{\sigma}(\psi) = \sum_{\alpha\in G} \sigma(\alpha)\psi(\alpha)$. The next definition generalizes this notion to the functions on G-sets. In the following we always assume that $|X| = n$.

Definition 3.1 For any $f \in \mathbb{C}^X$, the *Fourier transform* of f, $\widehat{f} \in \mathbb{C}^{\widehat{X}}$, is defined as:

$$\widehat{f}(\lambda) = \sum_{x\in X} f(x)\lambda(x), \quad \forall\ \lambda \in \widehat{X}.$$

For any $g \in \mathbb{C}^{\widehat{X}}$, the *Fourier inversion* of g, $\widehat{g} \in \mathbb{C}^X$, is defined as:

$$\widehat{g}(x) = \frac{1}{n} \sum_{\lambda\in\widehat{X}} g(\lambda)\overline{\lambda}(x), \quad \forall\ x \in X.$$

Remark 3.2 (i) For $x \in X$ we have the characteristic function $\mathbf{1}_x$ (i.e. $\mathbf{1}_x(y) = 0$ if $y \ne x$, and $\mathbf{1}_x(x) = 1$), whose Fourier transform is $\widehat{\mathbf{1}}_x(\lambda) = \lambda(x)$, for any $\lambda \in \widehat{X}$. We can rewrite the definitions of $\widehat{f}$ and $\widehat{g}$ in Definition 3.1 as follows:

$$\widehat{f}(\lambda) = \langle f, \overline{\lambda}\rangle, \ \ \forall\ f \in \mathbb{C}^X, \forall\ \lambda \in \widehat{X} \quad \text{and} \quad \widehat{g}(x) = \frac{1}{n}\langle g, \widehat{\mathbf{1}}_x\rangle, \ \ \forall\ g \in \mathbb{C}^{\widehat{X}}, \forall\ x \in X.$$

(ii) Since $\widehat{X}$ is an n-normal orthogonal basis of $\mathbb{C}^X$, and $\{\widehat{\mathbf{1}}_x \mid x \in X\}$ is an n-normal orthogonal basis of $\mathbb{C}^{\widehat{X}}$, it is straightforward to check that

$$f = \frac{1}{n}\sum_{\lambda\in\widehat{X}} \widehat{f}(\overline{\lambda})\lambda, \ \forall\ f \in \mathbb{C}^X \quad \text{and} \quad g = \sum_{x\in X} \widehat{g}(x)\widehat{\mathbf{1}}_x, \ \forall\ g \in \mathbb{C}^{\widehat{X}}. \tag{3.1}$$

That is, the Fourier transform and the Fourier inversion are just transformations between bases $\widehat{X}$ and $\{\widehat{\mathbf{1}}_x \mid x \in X\}$.

(iii) It is also straightforward to check that

$$\widehat{\widehat{f}} = f, \ \forall\ f \in \mathbb{C}^X \quad \text{and} \quad \widehat{\widehat{g}} = g, \ \forall\ g \in \mathbb{C}^{\widehat{X}}. \tag{3.2}$$

To simplify the notation, for any $f \in \mathbb{C}^X$ and $\psi \in \widehat{G}$, let $f_\psi := P_\psi(f)$ defined in (2.2).

Lemma 3.3 *For any $f \in \mathbb{C}^X$ and $\psi \in \widehat{G}$, the following hold.*

(i) *For any $\varphi \in \widehat{G}$ and $\lambda \in (\widehat{X})_\varphi$, $\widehat{f_\psi}(\lambda) = \delta_{\psi\overline{\varphi}}\widehat{f}(\lambda)$.*

(ii) *For any $\psi \in \widehat{G}$,*

$$f_\psi = \frac{1}{n}\sum_{\lambda\in(\widehat{X})_\psi} \widehat{f}(\overline{\lambda})\lambda.$$

(iii) $|\widehat{f_\psi}|^2 = \sum_{\lambda\in(\widehat{X})_\psi} |\widehat{f}(\overline{\lambda})|^2$.

Proof Note that by (2.2) and (2.3),

$$\begin{aligned}\widehat{f_\psi}(\lambda) &= \sum_{x\in X} f_\psi(x)\lambda(x) \ = \ \frac{1}{|G|}\sum_{x\in X}\sum_{a\in G} \overline{\psi(a)} f(a^{-1}x)\lambda(x)\\ &= \frac{1}{|G|}\sum_{y\in X}\sum_{a\in G} \overline{\psi(a)} f(y)\lambda(ay) \ = \ \frac{1}{|G|}\sum_{y\in X}\sum_{a\in G} \overline{\psi(a)} f(y)\overline{\varphi(a)}\lambda(y)\\ &= \delta_{\psi\overline{\varphi}}\widehat{f}(\lambda).\end{aligned}$$

So (i) holds. Now (ii) follows directly from (i) and (3.1), and (iii) follows directly from (i) and the definition of the length $|\widehat{f_\psi}|$. □

Lemma 3.4 $\langle \widehat{f}, \widehat{g}\rangle = n\langle f, g\rangle$, *for all* $f, g \in \mathbb{C}^X$.

Proof By (3.1) and the orthogonality of $\widehat{X}$, we get that

$$\begin{aligned}\langle f, g\rangle &= \left\langle \frac{1}{n}\sum_{\lambda\in\widehat{X}} \widehat{f}(\overline{\lambda})\lambda, \ \frac{1}{n}\sum_{\mu\in\widehat{X}} \widehat{g}(\overline{\mu})\mu \right\rangle \ = \ \frac{1}{n^2}\sum_{\lambda,\mu\in\widehat{X}} \hat{f}(\overline{\lambda})\overline{\hat{g}}(\overline{\mu})\cdot\langle\lambda,\mu\rangle\\ &= \frac{1}{n}\sum_{\lambda\in\widehat{X}} \hat{f}(\overline{\lambda})\overline{\hat{g}}(\overline{\lambda}) \ = \ \frac{1}{n}\langle \widehat{f}, \widehat{g}\rangle.\end{aligned}$$

□

The next corollary is immediate from Lemma 3.4. Recall that T is the unit circle in $\mathbb{C}$.

Corollary 3.5 *If $f \in T^X$, then $\langle f, f\rangle = n$ and $\langle \widehat{f}, \widehat{f}\rangle = n^2$.*

Corollary 3.6 *Let $f, g \in \mathbb{C}^X$ and $\alpha \in G$. Then*

$$\langle \alpha^{-1}f, g\rangle = \frac{1}{n}\sum_{\psi\in\widehat{G}} \psi(\alpha)\sum_{\lambda\in(\widehat{X})_\psi} \widehat{f}(\lambda)\overline{\widehat{g}}(\lambda).$$

Proof By Eq. (2.4) and Lemma 3.4, we have that

$$\langle \alpha^{-1} f, g\rangle = \langle f, \alpha g\rangle = \frac{1}{n}\langle \widehat{f}, \widehat{\alpha g}\rangle = \frac{1}{n}\sum_{\lambda\in\widehat{X}} \widehat{f}(\lambda)\overline{\widehat{\alpha g}}(\lambda) = \frac{1}{n}\sum_{\psi\in\widehat{G}}\sum_{\lambda\in(\widehat{X})_\psi} \widehat{f}(\lambda)\overline{\widehat{\alpha g}}(\lambda).$$

For each $\lambda \in (\widehat{X})_\psi$ we have $\lambda(\alpha x) = \overline{\psi}(\alpha)\lambda(x)$ by (2.3). So

$$\begin{aligned}\sum_{\lambda\in(\widehat{X})_\psi} \widehat{f}(\lambda)\overline{\widehat{\alpha g}}(\lambda) &= \sum_{\lambda\in(\widehat{X})_\psi} \widehat{f}(\lambda)\sum_{x\in X}\overline{(\alpha g)(x)\lambda(x)} = \sum_{\lambda\in(\widehat{X})_\psi} \widehat{f}(\lambda)\sum_{x\in X}\overline{g(\alpha^{-1}x)\lambda(\alpha\alpha^{-1}x)}\\ &= \psi(\alpha)\sum_{\lambda\in(\widehat{X})_\psi} \widehat{f}(\lambda)\sum_{y\in X}\overline{g(y)}\,\overline{\lambda}(y) = \psi(\alpha)\sum_{\lambda\in(\widehat{X})_\psi} \widehat{f}(\lambda)\overline{\widehat{g}}(\lambda).\end{aligned}$$

So the corollary holds. □

4 Bent functions on G-sets

Let T^X be the set of all T-valued functions on the G-set X, where T is the unit circle in $\mathbb{C}$. In this section we define the bentness of functions in T^X, and study its characterizations. In the following we assume that $|X| = n$ and $|G| = m$.

Definition 4.1 A function $f \in T^X$ is called a *bent function* on the G-set X if

$$\sum_{\lambda\in(\widehat{X})_\psi} \left|\widehat{f}(\lambda)\right|^2 = \frac{|X|^2}{|G|}, \quad \text{for all } \psi \in \widehat{G}.$$

If $X = G$ is the regular G-set, then $\widehat{X} = \widehat{G}$ and $(\widehat{G})_\psi = \{\psi\}$ for any $\psi \in \widehat{G}$. By the above definition, a function $f \in T^G$ is bent if $|\widehat{f}(\psi)|^2 = |G|$ for any $\psi \in \widehat{G}$. This is just the classical definition of bent functions on G (cf. [4]).

The bentness of functions on G-sets are also defined in [6, Definition 6], and called *G-bent functions*. But the definition in [6] is different; it uses the Fourier transforms of functions on G. However, we will show that the definition in [6] is equivalent to Definition 4.1 (see Corollary 4.12 below).

Although the bent function is defined by the use of $\lambda \in \widehat{X}$, the next lemma says that the bentness of a function on X is independent of the choice of $\widehat{X}$.

Lemma 4.2 *For a function $f : X \to T$, the following are equivalent.*

(i) *f is a bent function.*
(ii) *For any $\psi, \varphi \in \widehat{G}$, $|\widehat{f_\psi}| = |\widehat{f_\varphi}|$.*
(iii) *For any $\psi, \varphi \in \widehat{G}$, $|f_\psi| = |f_\varphi|$.*

Proof By Lemma 3.3(iii), (i) implies (ii). Assume (ii). From Lemma 3.3 and Corollary 3.5 we see that

$$\sum_{\psi\in\widehat{G}} |\widehat{f_\psi}|^2 = \sum_{\psi\in\widehat{G}}\sum_{\lambda\in(\widehat{X})_{\overline{\psi}}} |\widehat{f}(\lambda)|^2 = \langle \widehat{f}, \widehat{f}\rangle = n^2.$$

Hence, for any $\psi \in \widehat{G}$, $\sum_{\lambda\in(\widehat{X})_\psi} \left|\widehat{f}(\lambda)\right|^2 = |\widehat{f_{\overline{\psi}}}|^2 = n^2/m$, and (i) holds.

(ii) and (iii) are equivalent by Lemma 3.4. □

The support of $f \in \mathbb{C}^X$ in X is $\mathrm{Supp}(f) := \{x \in X \mid f(x) \neq 0\}$. Then $f \neq 0$ if and only if $\mathrm{Supp}(f) \neq \emptyset$. A nonempty subset Y of X is G-invariant if $ay \in Y$ for any $a \in G$ and $y \in Y$.

Definition 4.3 If $f \in \mathbb{C}^X$ is a non-zero function and $\mathrm{Supp}(f)$ is G-invariant, then f is said to be *differentiable*. For any differentiable function $f \in \mathbb{C}^X$ we define a function f'_α on $\mathrm{Supp}(f)$ as follows:

$$f'_\alpha(x) = f(\alpha x) f(x)^{-1}, \quad \forall\, x \in \mathrm{Supp}(f).$$

f'_α is called the *derivative* of f in direction α.

Any function $f \in T^X$ is differentiable and $f'_\alpha \in T^X$. Also any non-zero G-linear function is differentiable. The following lemma is a geometric explanation of the G-linearity of a function by its derivatives.

Lemma 4.4 *Let $f \in \mathbb{C}^X$ be differentiable. Then f'_α is a constant function on* $\mathrm{Supp}(f)$ *for any $\alpha \in G$ if and only if f is G-linear.*

Proof It is clear that if f is ψ-linear for some $\psi \in \widehat{G}$, then for any $\alpha \in G$, $f'_\alpha(x) = \overline{\psi}(\alpha)$ for $x \in \mathrm{Supp}(f)$, and f'_α is a constant function. Now assume that for any $\alpha \in G$, $f'_\alpha(x) = \psi_f(\alpha)$, for all $x \in \mathrm{Supp}(f)$. Then for any $\alpha, \beta \in G$, it is straightforward to check that $\psi_f(\alpha\beta) = \psi_f(\alpha)\psi_f(\beta)$. So ψ_f is an irreducible character of G, and f is $\overline{\psi}_f$-linear. □

Functions far away from G-linear functions on X are more useful and interesting in cryptography. So by Lemma 4.4 we want to investigate those functions whose derivatives in all nontrivial directions are far away from constant functions. As for the functions on finite groups, a function $h : X \to T$ is said to be *balanced* if $\sum_{x\in X} h(x) = 0$.

Definition 4.5 A function $f : X \to T$ is said to have *totally balanced derivatives* if

$$\sum_{x\in X} f'_\alpha(x) = 0, \quad \forall\ \alpha \in G\backslash\{1_G\}.$$

We are ready to present the characterizations of bent functions on G-sets.

Theorem 4.6 *A function $f \in T^X$ is bent if and only if f has totally balanced derivatives.*

Proof Since f is T-valued, $\sum_{x\in X} f'_\alpha(x) = \sum_{x\in X} f(\alpha x)\overline{f}(x) = \langle \alpha^{-1} f, f\rangle$. By Corollary 3.6 we have that

$$\sum_{x\in X} f'_\alpha(x) = \frac{1}{n}\sum_{\psi\in\widehat{G}} \psi(\alpha) \sum_{\lambda\in(\widehat{X})_\psi} \widehat{f}(\lambda)\overline{\widehat{f}}(\lambda) = \frac{1}{n}\sum_{\psi\in\widehat{G}} \Big(\sum_{\lambda\in(\widehat{X})_\psi} |\widehat{f}(\lambda)|^2 \Big)\psi(\alpha).$$

Since $\overline{(\widehat{X})_\psi} = (\widehat{X})_{\overline{\psi}}$, Lemma 3.3(iii) implies that

$$\sum_{x\in X} f'_\alpha(x) = \frac{1}{n}\sum_{\psi\in\widehat{G}} |\widehat{f_{\overline{\psi}}}|^2 \psi(\alpha). \tag{4.1}$$

If f has totally balanced derivatives, i.e. $\sum_{x\in X} f'_\alpha(x) = 0$ for all $\alpha \in G\backslash\{1_G\}$, then Eq. (4.1) implies that the function $\sum_{\psi\in\widehat{G}} |\widehat{f_{\overline{\psi}}}|^2\psi$ on G takes zero on $G\backslash\{1_G\}$, and hence it must be a multiple of the regular character $\rho = \sum_{\psi\in\widehat{G}} \psi$ of G. Thus, for any $\psi, \varphi \in \widehat{G}$ we have $|\widehat{f_\psi}|^2 = |\widehat{f_\varphi}|^2$, and f is bent by Lemma 4.2.

Conversely, if f is bent, i.e. $|\widehat{f_\psi}|^2 = \frac{n^2}{m}$ for all $\psi \in \widehat{G}$, then by Eq. (4.1) we have

$$\sum_{x\in X} f'_\alpha(x) = \frac{1}{n}\sum_{\psi\in\widehat{G}} \frac{n^2}{m}\psi(\alpha) = \frac{n}{m}\sum_{\psi\in\widehat{G}} \psi(\alpha) = 0, \quad \text{for all } \alpha \in G\backslash\{1_G\}.$$

That is, f has totally balanced derivatives. □

Let $f \in T^X$. From Corollary 3.6 and the proof of Theorem 4.6, the following are equivalent: (i) f is bent; (ii) for any $\alpha \in G\backslash\{1_G\}$, $\langle \alpha f, f\rangle = 0$; (iii) for any $\alpha \in G\backslash\{1_G\}$, $\langle \widehat{f}, \widehat{\alpha f}\rangle = 0$.

Corollary 4.7 *If there is a $\psi \in \widehat{G}$ such that $(\mathbb{C}^X)_\psi = 0$ (i.e. $(\widehat{X})_\psi = \emptyset$), then there exists no bent function $f \in T^X$.*

Proof For any $f \in T^X$, $(\widehat{X})_\psi = \emptyset$ implies that $|\widehat{f_\psi}| = 0$. □

Remark 4.8 The above corollary says that the condition "$(\mathbb{C}^X)_\psi \neq 0$ for all $\psi \in \widehat{G}$" is a necessary condition for the existence of bent functions.

If the G-action on X is not faithful, i.e. the kernel K of the action is nontrivial, then there must be an irreducible character ψ of G which takes nontrivial values on K, and hence $(\mathbb{C}^X)_\psi = 0$. So by the above corollary, there exists no bent functions on X.

However, even if the G-action on X is faithful, there may still exist some $\psi \in \widehat{G}$ such that $(\mathbb{C}^X)_\psi = 0$, and hence the bent functions on X do not exist. See Example 6.3 below for such an example.

The distance of $f, g \in \mathbb{C}^X$ is $d(f, g) := |f - g|$, and the distance between two subsets $S_1, S_2 \subseteq \mathbb{C}^X$ is

$$\mathrm{d}(S_1, S_2) := \min\big\{\mathrm{d}(f_1, f_2) \,\big|\, f_1 \in S_1,\ f_2 \in S_2\big\}. \tag{4.2}$$

Our next characterization of a bent function is given by its distance from the set $(\mathbb{C}^X)_G$ of G-linear functions. The next theorem says that $\sqrt{(m-1)n/m}$ is the best possible upper bound of the distance from any T-valued function to $(\mathbb{C}^X)_G$, and the upper bound is attained if and only if the function is bent.

Theorem 4.9 *Let $f \in T^X$. Then the following hold.*

(i) $d\big(f, (\mathbb{C}^X)_G\big) \le \sqrt{\frac{(m-1)n}{m}}$.

(ii) *f is bent if and only if* $d\big(f, (\mathbb{C}^X)_G\big) = \sqrt{\frac{(m-1)n}{m}}$.

Proof Recall that for any $f \in \mathbb{C}^X$, $f = \sum_{\psi\in\widehat{G}} f_\psi$. For any G-linear function g, there is a $\varphi \in \widehat{G}$ such that g is φ-linear. So $g = g_\varphi \in (\mathbb{C}^X)_\varphi$, and $g_\psi = 0$ for any $\psi \in \widehat{G} \setminus \{\varphi\}$. Since any two distinct G-linear components are orthogonal to each other,

$$\big[\mathrm{d}(f, g)\big]^2 = |f - g|^2 = \Big|\sum_{\psi\in\widehat{G}} (f_\psi - g_\psi)\Big|^2 = |f_\varphi - g_\varphi|^2 + \sum_{\psi\neq\varphi} |f_\psi|^2 \ge \sum_{\psi\neq\varphi} |f_\psi|^2,$$

and the equality holds if and only if $g = f_\varphi$. By Corollary 3.5,

$$\sum_{\psi\in\widehat{G}} |f_\psi|^2 = \sum_{\psi\in\widehat{G}} \langle f_\psi, f_\psi\rangle = \Big\langle \sum_{\psi\in\widehat{G}} f_\psi, \sum_{\psi\in\widehat{G}} f_\psi \Big\rangle = \langle f, f\rangle = |f|^2 = n.$$

So according to the definition of the distance in Eq. (4.2), we have

$$\big[\mathrm{d}\big(f,(\mathbb{C}^X)_\varphi\big)\big]^2 = n - |f_\varphi|^2.$$

Hence the square of the distance between f and $(\mathbb{C}^X)_G$ is

$$\big[\mathrm{d}\big(f,(\mathbb{C}^X)_G\big)\big]^2 = \min_{\varphi\in\widehat{G}}\big\{n - |f_\varphi|^2\big\} = n - \max_{\varphi\in\widehat{G}}\big\{|f_\varphi|^2\big\}.$$

By the equality $\sum_{\psi\in\widehat{G}}|f_\psi|^2 = n$ again, $|\widehat{G}| = m$ implies that

$$\max_{\varphi\in\widehat{G}}\big\{|f_\varphi|^2\big\} \geq \frac{n}{m},$$

where the equality holds if and only if $|f_\psi|^2 = |f_\varphi|^2$ for all $\psi,\varphi\in\widehat{G}$. In conclusion,

$$\mathrm{d}\big(f,(\mathbb{C}^X)_G\big)^2 \leq n - \frac{n}{m} = \frac{(m-1)n}{m}, \tag{4.3}$$

and the equality in (4.3) holds if and only if $|f_\psi|^2 = |f_\varphi|^2$ for all $\psi,\varphi\in\widehat{G}$. By Lemma 4.2, the equality in (4.3) holds if and only if f is bent. □

By taking $X = G$ as the regular G-set, we have the next corollary from Theorem 4.6, Theorem 4.9 and Lemma 4.2. Note that the equivalence of (i) and (ii) in Corollary 4.10 below was proved in [4].

Corollary 4.10 *Let $f\in T^G$. Then the following are equivalent.*

(i) *f is a bent function.*
(ii) *f has totally balanced derivatives.*
(iii) *Among all functions in T^G, f has the greatest distance $\sqrt{|G|-1}$ from the set $(\mathbb{C}^G)_G$ of G-linear functions.*
(iv) *$|\langle f,\psi\rangle|$ are equal for all $\psi\in\widehat{G}$.*

Proof The equivalence of (i), (ii), and (iii) is immediate from Theorems 4.6 and 4.9. Since $\widehat{G}$ is a basis of $\mathbb{C}^G$, we may assume that $f = \sum_{\psi\in\widehat{G}} c_\psi\psi$, where $c_\psi\in\mathbb{C}$. Hence, the ψ-component of f is $f_\psi = c_\psi\psi$, for any $\psi\in\widehat{G}$. Thus,

$$|\langle f,\psi\rangle| = |\langle c_\psi\psi,\psi\rangle| = |c_\psi| = \sqrt{|\langle f_\psi, f_\psi\rangle|}, \quad \text{for any } \psi\in\widehat{G}.$$

So the equivalence of (i) and (iv) holds by Lemma 4.2. □

Lemma 4.11 *For any $f\in\mathbb{C}^X$ and $x\in X$, let $f_x\in\mathbb{C}^G$ be defined by $f_x(\alpha) = f(\alpha x)$ for all $\alpha\in G$. Then $\widehat{f_x}(\psi) = mf_{\overline{\psi}}(x)$ for all $\psi\in\widehat{G}$.*

Proof It follows from (2.2) that

$$\widehat{f_x}(\psi) = \sum_{\alpha\in G} f_x(\alpha)\psi(\alpha) = \sum_{\alpha\in G} f(\alpha x)\overline{\psi}(\alpha^{-1}) = mf_{\overline{\psi}}(x).$$

□

The next corollary is one of the main results of [6,7], where the G-bentness of $f\in T^X$ is defined by the condition (ii) of Corollary 4.12. So Corollary 4.12 implies that the G-bentness defined in [6,7] is equivalent to the bentness defined by Definition 4.1.

Corollary 4.12 (Cf. [6,7]) *Let $f \in T^X$. Then the following are equivalent.*

(i) *f has totally balanced derivatives. That is, f is a bent function by Definition 4.1.*
(ii) *$\frac{1}{n}\sum_{x\in X} |\widehat{f_x}(\psi)|^2 = m$ for all $\psi \in \widehat{G}$. That is, f is a G-bent function by* [6, Definition 6].

Proof By Lemmas 4.11 and 3.4, we have

$$\frac{1}{n}\sum_{x\in X} |\widehat{f_x}(\psi)|^2 = \frac{m^2}{n}\sum_{x\in X} |f_{\overline{\psi}}(x)|^2 = \frac{m^2}{n}\langle f_{\overline{\psi}}, f_{\overline{\psi}}\rangle = \frac{m^2}{n^2}\langle \widehat{f_{\overline{\psi}}}, \widehat{f_{\overline{\psi}}}\rangle = \frac{m^2}{n^2}|\widehat{f_{\overline{\psi}}}|^2.$$

Thus, (ii) holds if and only if $|\widehat{f_{\overline{\psi}}}|^2 = \frac{n^2}{m}$ for all $\psi \in \widehat{G}$ if and only if f has totally balanced derivatives by Theorem 4.6 and Lemma 4.2. □

Remark 4.13 For any $f, g \in \mathbb{C}^X$, the *pseudo-convolution* $f \boxtimes g$ of f and g is defined as (cf. [7])

$$f \boxtimes g : G \to \mathbb{C}, \quad \alpha \mapsto \sum_{x\in X} \overline{f(x)}g(\alpha x).$$

By Lemma 2.5 and (3.2), it is straightforward to show that

$$\widehat{(f \boxtimes g)}(\psi) = \frac{m}{n}\sum_{\lambda\in(\widehat{X})_\psi} \overline{\widehat{f}(\lambda)}\widehat{g}(\lambda), \quad \text{for any } \psi \in \widehat{G}.$$

The equivalence of (i) and (ii) of Corollary 4.12 can also be proved by the above equality.

5 Perfect nonlinear functions on G-sets

As an application of the characterizations of bent functions on G-sets, in this section we discuss the characterizations of perfect nonlinear functions from a G-set to an abelian group. Our approach here is different from that of [6,7]. Let X be a G-set as before, and let H be an abelian group whose operation is multiplication. The set of all functions from X to H is denoted by H^X. An $f \in H^X$ is said to be *evenly-balanced* (cf. [13,15]) if $|H|$ divides $|X|$ and

$$\big|\{x \in X | f(x) = h\}\big| = \frac{|X|}{|H|}, \quad \text{for any } h \in H.$$

An evenly-balanced function is also called a *balanced* or *uniformly distributed* function in literature. The *derivative* of $f \in H^X$ in direction $\alpha \in G$ is

$$f'_\alpha : X \to H, \quad x \mapsto f(\alpha x)f(x)^{-1}.$$

Definition 5.1 (cf. [7, Definition 1]) A function $f : X \to H$ is said to be *G-perfect nonlinear* if for any $\alpha \in G\backslash\{1_G\}$, the function f'_α is evenly-balanced.

Any $g \in H^X$ induces a non-negative integral function $g^\#$ on H as follows:

$$g^\# : H \to \mathbb{N} \cup \{0\}, \quad h \mapsto \big|\{x \in X \mid g(x) = h\}\big|.$$

Hence, $g^\#$ is constant on H if and only if g is evenly-balanced. Thus, a function $f : X \to H$ is G-perfect nonlinear if and only if for any $\alpha \in G\backslash\{1_G\}$, $f'^\#_\alpha$ is constant on H.

Theorem 5.2 *Let $f \in H^X$. Then following are equivalent.*

(i) *For any $\xi \in \widehat{H}\backslash\{1\}$ the composition function $\xi \circ f : X \to T$ has totally balanced derivatives.*
(ii) *For any $\xi \in \widehat{H}\backslash\{1\}$ the composition function $\xi \circ f : X \to T$ is bent.*
(iii) *The function $f : X \to H$ is G-perfect nonlinear.*

Proof It is enough to show that (i) $\Leftrightarrow$ (iii). Since $(\xi \circ f)(x) \in T$, we have $(\xi \circ f)(x)^{-1} = \overline{(\xi \circ f)(x)}$, for any $x \in X$. So

$$\begin{aligned}\sum_{x\in X}(\xi\circ f)'_\alpha(x) &= \sum_{x\in X}(\xi\circ f)(\alpha x)\overline{(\xi\circ f)(x)}\\ &= \sum_{x\in X}\xi\big(f(\alpha x)\big)\overline{\xi}\big(f(x)\big) = \sum_{x\in X}\xi\big(f(\alpha x)\big)\xi\big(f(x)^{-1}\big)\\ &= \sum_{x\in X}\xi\big(f(\alpha x)f(x)^{-1}\big) = \sum_{x\in X}\xi\big(f'_\alpha(x)\big).\end{aligned}$$

For any $h \in H$, let $X(f'_\alpha, h) = \{x \in X \mid f'_\alpha(x) = h\}$. Then X is the disjoint union $X = \bigcup_{h\in H} X(f'_\alpha, h)$, and the cardinality $|X(f'_\alpha, h)| = f'^{\#}_\alpha(h)$. So

$$\sum_{x\in X}(\xi\circ f)'_\alpha(x) = \sum_{h\in H}\sum_{x\in X(f'_\alpha,h)}\xi(h) = \sum_{h\in H} f'^{\#}_\alpha(h)\xi(h) = \widehat{f'^{\#}_\alpha}(\xi). \tag{5.1}$$

Thus, $(\xi \circ f)'_\alpha$ is balanced if and only if $\widehat{f'^{\#}_\alpha}(\xi) = 0$. Hence for any $\xi \in \widehat{H}\backslash\{1\}$, the function $(\xi \circ f)'_\alpha$ is balanced if and only if $\widehat{f'^{\#}_\alpha}$ is zero on $\widehat{H}\backslash\{1\}$ if and only if $f'^{\#}_\alpha$ is constant on H. That is, for any $\xi \in \widehat{H}\backslash\{1\}$, the function $\xi \circ f$ has totally balanced derivatives if and only if f is G-perfect nonlinear. □

Taking $X = G$ to be the regular G-set, we have the next

Corollary 5.3 (Cf. [2]) *Let G, H be abelian groups, and $f : G \to H$ a function. Then the following are equivalent.*

(i) *f is perfect nonlinear.*
(ii) *For any $\xi \in \widehat{H}\backslash\{1\}$ the composition function $\xi \circ f : G \to T$ is bent.*

Let $f \in H^X$. Then for any $x \in X$, there is a function (cf. [6,7])

$$f_x : G \to H, \quad \alpha \mapsto f(\alpha x).$$

Also for any $\xi \in \widehat{H}$, there is a function $(\xi \circ f)_x : G \to T$, $\alpha \mapsto (\xi \circ f)(\alpha x)$. Note that $(\xi \circ f)_x = \xi \circ f_x$, for any $x \in X$. The next corollary is immediate from Theorem 5.2 and Corollary 4.12.

Corollary 5.4 (cf. [6, Theorems 5 and 7]) *Let $f \in H^X$. Then the following are equivalent.*

(i) *f is G-perfect nonlinear.*
(ii) *For any $\xi \in \widehat{H}\backslash\{1\}$ and $\alpha \in G$,*

$$\frac{1}{|X|}\sum_{x\in X}\left|\widehat{(\xi\circ f_x)}(\alpha)\right|^2 = |G|.$$

6 Examples

In this section we present a few examples that explain the theory developed in the previous sections.

Example 6.1 Assume that $X = G$ is the regular G-set. As mentioned in Remark 2.4, the G-dual set $\widehat{X}$ is unique up to rescaling by T, and the typical choice of $\widehat{X}$ is just the dual group $\widehat{G}$. So the theory developed in previous sections includes the corresponding theory for finite abelian groups as a special case. For example, some well-known results in [2,4,12] as well as other properties of bent functions on finite abelian groups are given in Corollary 4.10 and Corollary 5.3 as immediate consequences.

The next theorem gives a necessary condition under which a G-set admits a bent function.

Theorem 6.2 *Let G be a finite abelian group and let X be a G-set with exactly two orbits. If X admits a bent function, then X has a regular orbit.*

Proof Toward a contradiction, assume that the orbits of X are X_1, X_2, none of which is regular. Let K_i be the kernel of the action of G on X_i, $i = 1, 2$. Then $|K_i| \geq 2$, and hence $|X_i| = |G|/|K_i| \leq |G|/2$, $i = 1, 2$. Thus $|X| = |X_1| + |X_2| \leq |G|$, and $|\widehat{X}| = |X| \leq |G|$. Let ψ_1 be the principal irreducible character of G. Then $|(\widehat{X})_{\psi_1}| = |(\widehat{X}_1)_{\psi_1}| + |(\widehat{X}_2)_{\psi_1}| = 2$. Hence, $|\widehat{X}| \leq |G|$ implies that there is $\varphi \in \widehat{G}$ such that $(\widehat{X})_\varphi = \emptyset$. So X does not admit a bent function by Corollary 4.7, a contradiction. □

The next example gives a G-set which does not admit a bent function.

Example 6.3 Let $G = \{1, \alpha, \beta, \gamma\}$ be the Klein four group. That is, G is an abelian group such that

$$\alpha^2 = \beta^2 = \gamma^2 = 1,\ \alpha\beta = \gamma,\ \beta\gamma = \alpha,\ \gamma\alpha = \beta.$$

Let $X = \{x_1, x_2, x_3, x_4\}$ be a faithful G-set with two orbits X_1 and X_2 as follows:

1. $X_1 = \{x_1, x_2\}$, 1 and α fix both points x_1 and x_2, while β and γ interchange the two points;
2. $X_2 = \{x_3, x_4\}$, 1 and β fix both points x_3 and x_4, while γ and α interchange the two points.

Since none of these two orbits is regular, X does not admit a bent function by Theorem 6.2.

The next example gives a G-set X and a bent function on X.

Example 6.4 As in Example 6.3 above, let $G = \{1, \alpha, \beta, \gamma\}$ be the Klein four group and $\widehat{G} = \{\psi_1, \psi_2, \psi_3, \psi_4\}$ given by the Table 1.

But this time we consider the G-set $X = \{x_1, x_2, x_3, x_4, x_5, x_6\}$ with three orbits:

- $X_1 = \{x_1, x_2\}$, 1 and α fix both points x_1 and x_2, while β and γ interchange the two points;
- $X_2 = \{x_3, x_4\}$, 1 and β fix both points x_3 and x_4, while γ and α interchange the two points;
- $X_3 = \{x_5, x_6\}$, 1 and γ fix both points x_5 and x_6, while α and β interchange the two points.

Table 1 Character Table of the Klein Four Group

	1	α	β	γ
ψ_1	1	1	1	1
ψ_2	1	1	-1	-1
ψ_3	1	-1	1	-1
ψ_4	1	-1	-1	1

Table 2 The G-dual set of X for Example 6.4

	x_1	x_2	x_3	x_4	x_5	x_6
$\frac{1}{\sqrt{3}}\lambda_1$	1	1	0	0	0	0
$\frac{1}{\sqrt{3}}\lambda_2$	1	-1	0	0	0	0
$\frac{1}{\sqrt{3}}\lambda_3$	0	0	1	1	0	0
$\frac{1}{\sqrt{3}}\lambda_4$	0	0	1	-1	0	0
$\frac{1}{\sqrt{3}}\lambda_5$	0	0	0	0	1	1
$\frac{1}{\sqrt{3}}\lambda_6$	0	0	0	0	1	-1

We can take $\widehat{X} = \{\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5, \lambda_6\}$ as in Table 2 (to simplify the table, we list $\frac{1}{\sqrt{3}}\lambda_i$ instead of λ_i).

We can check that the G-linear components of $\mathbb{C}^X$ are

$$(\widehat{X})_{\psi_1} = \{\lambda_1, \lambda_3, \lambda_5\},\ (\widehat{X})_{\psi_2} = \{\lambda_2\},\ (\widehat{X})_{\psi_3} = \{\lambda_4\},\ (\widehat{X})_{\psi_4} = \{\lambda_6\}.$$

Let $\omega = \frac{-1+\sqrt{-3}}{2}$ be a primitive third root of unity. Take $f \in T^X$ as follows:

$$f(x_j) = \omega^{(1+(-1)^j)/2} = \begin{cases} 1, & j = 1, 3, 5; \\ \omega, & j = 2, 4, 6. \end{cases}$$

Then

$$\sum_{x\in X_j} f'_\alpha(x) = \sum_{x\in X_j} f(\alpha x) f(x)^{-1} = \begin{cases} 1 + 1 = 2, & j = 1; \\ 1 \cdot \omega^{-1} + \omega \cdot 1 = -1, & j = 2, 3. \end{cases}$$

So $\sum\limits_{x\in X} f'_\alpha(x) = 0$. Similarly, $\sum\limits_{x\in X} f'_\beta(x) = \sum\limits_{x\in X} f'_\gamma(x) = 0$. That is, f has totally balanced derivatives.

On the other hand,

$$\begin{aligned} \langle \widehat{f}_{\psi_1}, \widehat{f}_{\psi_1} \rangle &= \sum_{\lambda\in(\widehat{X})_{\psi_1}} |\widehat{f}(\lambda)|^2 = \sum_{j=1,3,5} \Big| \sum_{x\in X} f(x)\lambda_j(x) \Big|^2 \\ &= \sum_{j=1,3,5} \big|\sqrt{3}(1+\omega)\big|^2 = 3\big|\sqrt{3}(1+\omega)\big|^2 = 9, \\ \langle \widehat{f}_{\psi_2}, \widehat{f}_{\psi_2} \rangle &= \sum_{\lambda\in(\widehat{X})_{\psi_2}} \big|\widehat{f}(\lambda)\big|^2 = \Big| \sum_{x\in X} f(x)\lambda_2(x) \Big|^2 = \big|\sqrt{3}(1-\omega)\big|^2 = 9. \end{aligned}$$

Similarly, $\langle \widehat{f_{\psi_3}}, \widehat{f_{\psi_3}} \rangle = \langle \widehat{f_{\psi_4}}, \widehat{f_{\psi_4}} \rangle = \left|\sqrt{3}(1-\omega)\right|^2 = 9$. In conclusion, we have $\langle \widehat{f_\psi}, \widehat{f_\psi} \rangle = 9, \forall\ \psi \in \widehat{G}$, and f is a bent function.

The next example gives a G-perfect nonlinear function.

Example 6.5 We continue Example 6.4 and further take $H = \{1, h, h^2\}$ with $h^3 = 1$ to be a cyclic group of order 3. Let $g : X \to H$ be as follows:

$$g(x_j) = h^{(1+(-1)^j)/2} = \begin{cases} 1, & j = 1, 3, 5; \\ h, & j = 2, 4, 6. \end{cases}$$

It is known that $\widehat{H} = \{1, \xi, \xi^2\}$, where $\xi(h^i) = \omega^i, i = 0, 1, 2$. Then the composition function $\xi \circ g : X \to \mathbb{C}$ is just the function f in Example 6.4, and hence $\xi \circ g$ is a bent function on X. Similarly we can check that $\xi^2 \circ g$ is also a bent function on X. So $g : X \to H$ is a G-perfect nonlinear function from the G-set X to the abelian group H. It is also straightforward to check that $g'^{\#}_\alpha = g'^{\#}_\beta = g'^{\#}_\gamma = 2$ are constant functions on H.

The next example discusses the constructions of new bent functions from old ones.

Example 6.6 (i) Let G be an abelian group, and let X_1 and X_2 be two disjoint G-sets. Let $f : X_1 \cup X_2 \to T$ be a function such that both $f|_{X_1}$ and $f|_{X_2}$ are bent functions. Then for any $a \in G \setminus \{1\}$, $\sum_{x \in X} f'_a(x) = \sum_{x \in X_1} f'_a(x) + \sum_{x \in X_2} f'_a(x) = 0$. So f is also a bent function by Theorem 4.6.

(ii) Let G be an abelian group, and let X_1 and X_2 be two G-sets. Let $f_i : X_i \to T, i = 1, 2$, be two functions, and let $f : X_1 \times X_2 \to T$ be a function defined by $f(x_1, x_2) := f_1(x_1) f_2(x_2)$, for any $(x_1, x_2) \in X_1 \times X_2$. Let G act on $X_1 \times X_2$ by $a(x_1, x_2) = (ax_1, ax_2)$, for any $a \in G$ and $(x_1, x_2) \in X_1 \times X_2$. Then for any $a \in G \setminus \{1\}$,

$$\sum_{(x_1,x_2) \in X_1 \times X_2} f'_a(x_1, x_2) = \Big(\sum_{x \in X_1} (f_1)'_a(x_1) \Big) \cdot \Big(\sum_{x_2 \in X_2} (f_2)'_a(x_2) \Big).$$

Thus, if one of f_1 and f_2 is bent, then f is also bent by Theorem 4.6.

(iii) Let G_i be an abelian group, and let X_i be a G_i-set, $i = 1, 2$. Then $X_1 \times X_2$ is a $(G_1 \times G_2)$-set with action $(a_1, a_2)(x_1, x_2) = (a_1 x_1, a_2 x_2)$, for any $(a_1, a_2) \in G_1 \times G_2$ and $(x_1, x_2) \in X_1 \times X_2$. Let $f_i : X_i \to T$, $i = 1, 2$, be two functions, and let $f : X_1 \times X_2 \to T$ be a function defined by $f(x_1, x_2) := f_1(x_1) f_2(x_2)$, for any $(x_1, x_2) \in X_1 \times X_2$. Then for any $(a_1, a_2) \in G_1 \times G_2 \setminus \{(1, 1)\}$,

$$\sum_{(x_1,x_2) \in X_1 \times X_2} f'_{(a_1,a_2)}(x_1, x_2) = \Big(\sum_{x \in X_1} (f_1)'_{a_1}(x_1) \Big) \cdot \Big(\sum_{x_2 \in X_2} (f_2)'_{a_2}(x_2) \Big).$$

Thus, f is a bent function if and only if both f_1 and f_2 are bent by Theorem 4.6.

Acknowledgements This work was done while the first author was visiting the second author at Eastern Kentucky University in Spring 2014; he is grateful for the hospitality. The work of the first author is supported by NSFC with Grant Number 11271005. The authors would like to thank the referees for their useful comments, especially for the suggestions of Theorem 6.2 and Example 6.6.

References

1. Alperin J.L., Bell R.B.: Groups and Representations, GTM 162. Springer, New York (1997).
2. Carlet C., Ding C.: Highly nonlinear mappings. J. Complex. **20**, 205–244 (2004).

3. Dillon J.F.: Elementary Hadamard difference sets, Ph.D. Thesis, University of Maryland (1974).
4. Logachev O.A., Salnikov A.A., Yashchenko V.V.: Bent functions over a finite abelian group. Discret. Math. Appl. **7**, 547–564 (1997).
5. Poinsot L.: Bent functions on a finite nonabelian group. J. Discret. Math. Sci. Cryptogr. **9**, 349–364 (2006).
6. Poinsot L.: A new characterization of group action-based perfect nonlinearity. Discret. Appl. Math. **157**, 1848–1857 (2009).
7. Poinsot L., Harari S.: Group actions based perfect nonlinearity. GESTS Int. Trans. Comput. Sci. Eng. **12**, 1–14 (2005).
8. Poinsot L., Pott A.: Non-boolean almost perfect nonlinear functions on non-abelian groups. Int. J. Found. Comput. Sci. **22**, 1351–1367 (2011).
9. Pott A.: Nonlinear functions in abelian groups and relative difference sets. In: Optimal Discrete Structures and Algorithms, ODSA 2000. Discret. Appl. Math. **138**, 177–193 (2004).
10. Rothaus O.S.: On bent functions. J. Comb. Theory A **20**, 300–305 (1976).
11. Serre J.-P.: Representations of Finite Groups. Springer, New York (1984).
12. Solodovnikov V.I.: Bent functions from a finite abelian group to a finite abelian group. Diskret. Mat. **14**, 99–113 (2002).
13. Xu B.: Multidimensional Fourier transforms and nonlinear functions on finite groups. Linear Algebra Appl. **450**, 89–105 (2014).
14. Xu B.: Dual bent functions on finite groups and C-algebras. J. Pure Appl. Algebra **220**, 1055–1073 (2016).
15. Xu B.: Bentness and nonlinearity of functions on finite groups. Des. Codes Cryptogr. **76**, 409–430 (2015).