Des. Codes Cryptogr. (2018) 86:2091–2113
https://doi.org/10.1007/s10623-017-0439-0

Fourier transforms and bent functions on finite groups

Yun Fan[1] · **Bangteng Xu**[2]

Received: 4 March 2017 / Revised: 2 October 2017 / Accepted: 4 November 2017 /
Published online: 15 November 2017

Abstract Let G be a finite nonabelian group. Bent functions on G are defined by the Fourier transforms at irreducible representations of G. We introduce a dual basis $\widehat{G}$, consisting of functions on G determined by its unitary irreducible representations, that will play a role similar to the dual group of a finite abelian group. Then we define the Fourier transforms as functions on $\widehat{G}$, and obtain characterizations of a bent function by its Fourier transforms (as functions on $\widehat{G}$). For a function f from G to another finite group, we define a dual function $\widetilde{f}$ on $\widehat{G}$, and characterize the nonlinearity of f by its dual function $\widetilde{f}$. Some known results are direct consequences. Constructions of bent functions and perfect nonlinear functions are also presented.

Keywords Fourier transforms · Bent functions · Perfect nonlinear functions · Dual basis · Dual functions

Mathematics Subject Classification 43A30 · 11T71 · 20C15

1 Introduction

The notion of a Boolean bent function was first introduced by Rothaus [22] in 1976. Since then Boolean bent functions have been studied in numerous papers, and various generalizations of

Communicated by A. Pott.

The first author is supported by NSFC Grant 11271005.

✉ 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 and Statistics, Eastern Kentucky University, Richmond, KY 40475, USA

this notion have been developed. Applications of bent functions and their generalizations can be found in information theory, cryptography, coding theory, etc. Tokareva [25] presented a systematic survey of the recent development of the research in this field. Among the generalizations of Boolean bent functions, bent functions which are defined on the direct product of a finite number of identical cyclic groups and take values in this cyclic group were introduced by Chung et al. [5] and Kumar et al. [13]. As further generalizations, Logachev et al. [15] defined bent functions on finite abelian groups, and Poinsot [18] defined bent functions on finite non-abelian groups. Carlet and Ding [4] and Pott [21] studied perfect nonlinear functions between two finite abelian groups, which can be regarded as a generalization of bent functions on finite abelian groups introduced in [15]. Later, the notion of perfect nonlinear functions between two finite abelian groups in [4,21] is generalized to perfect nonlinear functions between two arbitrary finite groups by Poinsot [19]. More research on bent functions and perfect nonlinear functions on finite (abelian or non-abelian) groups can be found in other papers (cf. [24,26–28]). Other generalizations of bent functions on finite groups are also studied; for example, see [8,9,20].

Perfect nonlinear functions on finite groups can be used to construct DES-like cryptosystems that are resistant to differential attacks. An example of using the classical XOR as well as the addition in a cyclic group and the multiplication in the group of units of a finite field can be found in Lai and Massey [14]. Also see [23] for more examples of S-boxes that use addition in a cyclic group. Pott [21] mentioned that "It seems that in most applications (in particular in cryptography) people use nonlinear functions on finite fields. However, there is no technical reason why you should restrict yourselves to this case".

For arbitrary finite groups, the connections between the perfect nonlinear functions and relative difference sets are studied by Pott [21]. Let G and H be arbitrary finite groups, and $f : G \to H$ a function. Pott [21] proved that f is a perfect nonlinear function if and only if the set $R_f := \{(s, f(s)) : s \in G\} \subset G \times H$ is a semiregular $(|G|, |H|, |G|, |G|/|H|)$ relative difference set in $G \times H$ relative to $\{1_G\} \times H$, where 1_G is the identity element of G. Furthermore, the notion of a (G, H)-related difference family is introduced in [26]. It is proved in [26, Theorem 1.3] that f is perfect nonlinear if and only if $\{S_y : y \in H\}$ is a (G, H)-related difference family in G, where $S_y := f^{-1}(y)$. In particuar, if f is perfect nonlinear, then by [26, Corollary 1.4], $\{S_y : y \in f(G)\}$ is also a partitioned $(|G|, K, |G|/|H|)$ difference family in G, where $K := \{|S_y| : y \in f(G)\}$.

Let G be a finite group, and let f be a complex valued function on G. If G is abelian, then there is the dual group $\widehat{G}$ of G consisting of its (irreducible) characters. The Fourier transform $\widehat{f}$ of f is defined as a function on the dual group $\widehat{G}$, and the bentness of f is defined by its Fourier transform. That is, if the values of f on G are on the unit circle, then f is said to be a bent function if the absolute value of $\widehat{f}(\chi)$ is $\sqrt{|G|}$, for any $\chi \in \widehat{G}$. If G is nonabelian, then the Fourier transform $\widehat{f}$ of f is defined as a function on the irreducible representations of G, and the bentness of f is also defined by its Fourier transform (see Sects. 2 and 3 below for some details).

Let G be a finite nonabelian group. We introduce a dual basis of G, also denoted by $\widehat{G}$, that consists of complex valued functions on G determined by its unitary irreducible representations (see Definition 2.3 in Sect. 2). The dual basis $\widehat{G}$ will play a role similar to the dual group of a finite abelian group in our discussions. That is, for a complex valued function f on G, we will define the Fourier transform $\widehat{f}$ as a function on $\widehat{G}$ (see Definition 2.5 in Sect. 2). Although our definition of the Fourier transform (as a function on $\widehat{G}$) is equivalent to the traditional definition of the Fourier transform (as a function on the irreducible representations of G), by this new definition we are able to obtain further characterizations of bent functions on finite nonabelian groups (see Theorems 3.3 and 3.4 in Sect. 3). Furthermore, if f is a

function from G to another group H, then we define a dual function $\widetilde{f}$ of f as a function from $\widehat{G}$ to the vector space with basis $\widehat{H}$. We will characterize the nonlinearity of f by its dual function $\widetilde{f}$ (see Theorems 4.2 and 4.3 in Sect. 4). The method developed in this paper also provides conceptual proofs of some known results (see Corollaries 3.9 and 4.8).

The rest of the paper is organized as follows. In Sect. 2 we discuss properties of the Fourier transform as a function on the dual basis $\widehat{G}$. Then in Sect. 3, we study characterizations of bent functions. Characterizations of perfect nonlinear functions between two arbitrary finite groups are discussed in Sect. 4, and constructions of bent functions and perfect nonlinear functions are presented in Sect. 5.

2 Fourier transforms on finite groups

Let G be a finite group. The identity element of G is denoted by 1_G, or simply by 1 when no ambiguity can occur. Let $GL(m, \mathbb{C})$ be the group of all invertible $m \times m$ matrices over the complex numbers $\mathbb{C}$. Then a homomorphism $\Phi : G \to GL(m, \mathbb{C})$ is called a (*matrix*) *representation* of G, and m is called the *degree* of Φ. We say that a representation $\Phi : G \to GL(m, \mathbb{C})$ is *reducible* if there is $P \in GL(m, \mathbb{C})$ such that

$$P^{-1}\Phi(x)P = \begin{pmatrix} A(x) & O \\ O & C(x) \end{pmatrix}, \quad \text{for all } x \in G,$$

where $A(x)$ and $C(x)$ are square matrices, and O are zero matrices. If a representation Φ is not reducible, then we say that Φ is *irreducible*. Two representations Φ and Ψ of G are said to be *equivalent* if there is an invertible matrix P such that $\Psi(x) = P^{-1}\Phi(x)P$, for all $x \in G$. Let $\mathrm{Tr}(M)$ denote the trace of a square matrix M. Then the *character* φ of G afforded by a representation Φ is the function $\varphi : G \to \mathbb{C}$ defined by $\varphi(x) = \mathrm{Tr}(\Phi(x))$, for all $x \in G$, and φ is called an *irreducible character* if Φ is irreducible. The degree of Φ is also called the *degree* of φ, and denoted by n_φ. Two irreducible representations are equivalent if and only if they afford the same character. A representation Φ is called a *unitary* representation if $\Phi(x)$ is a unitary matrix, for any $x \in G$. Note that any irreducible representation of G is equivalent to a unitary irreducible representation (see [12, Theorem 4.17]).

The *principal* irreducible representation of G is $\Phi_1 : G \to GL(1, \mathbb{C})$, $x \mapsto 1$, and the *principal* irreducible character is φ_1 afforded by Φ_1. Any other irreducible representation (character) is called a *non-principal* irreducible representation (character). Throughout the paper, let $\mathrm{Irr}(G)$ denote the set of irreducible characters of G. For the references of the representation and character theory of finite groups, the reader is referred to [1,11,12,16].

Let $f : G \to \mathbb{C}$ be a function. Then for an irreducible representation $\Phi : G \to GL(m, \mathbb{C})$, the *Fourier transform* of f at Φ is defined as

$$\widehat{f}(\Phi) := \sum_{x \in G} f(x)\Phi(x) \in \mathrm{Mat}_m(\mathbb{C}), \tag{2.1}$$

where $\mathrm{Mat}_m(\mathbb{C})$ is the algebra of all $m \times m$ matrices over $\mathbb{C}$. The order of G is denoted by $|G|$. Let $\{\Phi_1, \Phi_2, \ldots, \Phi_k\}$ be a complete set of representatives of inequivalent irreducible representations of G, where k is the number of conjugacy classes of G. It is known that the Fourier transforms of f at $\Phi_1, \Phi_2, \ldots, \Phi_k$ determine f through the *inversion formula*

$$f(x) = \frac{1}{|G|} \sum_{i=1}^{k} n_i \,\mathrm{Tr}\left(\Phi_i(x^{-1})\widehat{f}(\Phi_i)\right), \quad \text{where } n_i \text{ is the degree of } \Phi_i. \tag{2.2}$$

For each $\psi \in \mathrm{Irr}(G)$, we fix a unitary irreducible representation Φ_ψ that affords ψ. Then for any $s \in G$, $\Phi_\psi(s)$ is an $n_\psi \times n_\psi$ unitary matrix, denoted by $\left(\phi_{ij}^{\psi}(s)\right)_{i,j}$. Thus, for any $\psi \in \mathrm{Irr}(G)$, we have n_ψ^2 functions on G defined by Φ_ψ:

$$\phi_{ij}^{\psi} : G \to \mathbb{C}, \quad s \mapsto \phi_{ij}^{\psi}(s), \quad 1 \le i, j \le n_\psi.$$

Throughout the paper, the following notation will be used.

Notation 2.1 For each $\psi \in \mathrm{Irr}(G)$, let Φ_ψ be a (fixed) unitary irreducible representation that affords ψ, and we also write

$$\Phi_\psi := \left(\phi_{ij}^{\psi}\right)_{i,j}.$$

Furthermore, let

$$\widehat{G} := \{\phi_{ij}^{\psi} : \psi \in \mathrm{Irr}(G), 1 \le i, j \le n_\psi\}.$$

The set $\mathbb{C}^G$ of complex functions on G is an $|G|$-dimensional complex space. It is also a G-module (or G-space) with the G-action defined by

$$sf : G \to \mathbb{C}, \quad t \mapsto f(s^{-1}t), \quad \text{for any } s \in G, f \in \mathbb{C}^G. \tag{2.3}$$

The complex conjugate of any $z \in \mathbb{C}$ is denoted by $\overline{z}$. For any $f \in \mathbb{C}^G$, let $\overline{f}$ be the complex conjugate of f defined by $\overline{f} : G \to \mathbb{C}, s \mapsto \overline{f(s)}$. The next lemma collects some basic facts about $\widehat{G}$. These results are known and can be found in the references mentioned above.

Lemma 2.2 *With Notation 2.1, the following hold.*

(i) $|\widehat{G}| = |G|$.

(ii) $\psi = \sum_{i=1}^{n_\psi} \phi_{ii}^{\psi}$, *for all* $\psi \in \mathrm{Irr}(G)$.

(iii) $\overline{\phi_{ij}^{\psi}}(s) = \phi_{ji}^{\psi}(s^{-1})$, *for all* $\phi_{ij}^{\psi} \in \widehat{G}$ *and* $s \in G$.

(iv) $\phi_{ij}^{\psi}(st) = \sum_{k=1}^{n_\psi} \phi_{ik}^{\psi}(s)\phi_{kj}^{\psi}(t)$, *for all* $\phi_{ij}^{\psi} \in \widehat{G}$ *and* $s, t \in G$. *In particular,*

$$s\phi_{ij}^{\psi} = \sum_{k=1}^{n_\psi} \phi_{ik}^{\psi}(s^{-1})\phi_{kj}^{\psi}, \quad \textit{for any } s \in G. \tag{2.4}$$

From (2.2) and Lemma 2.2, $\widehat{G}$ is a basis of $\mathbb{C}^G$.

Definition 2.3 With Notation 2.1, we call $\widehat{G}$ a *dual basis* of G.

The dual basis $\widehat{G}$ will play a role similar to the dual group of a finite abelian group in our treatment of Fourier transforms on finite nonabelian groups.

Note that $\mathbb{C}^G$ is a unitary space with the inner product

$$\langle f, g\rangle_G = \sum_{s\in G} f(s)\overline{g(s)}, \qquad \text{for any } f, g \in \mathbb{C}^G. \tag{2.5}$$

The next lemma is well known (cf. [16, p. 187, Theorem 2.2]). It says that $\widehat{G}$ is an orthogonal basis of $\mathbb{C}^G$.

Lemma 2.4 (Orthogonality Relations) *For any* $\phi_{ij}^{\psi}, \phi_{kl}^{\chi} \in \widehat{G}$,

$$\left\langle \phi_{ij}^{\psi}, \phi_{kl}^{\chi} \right\rangle_G = \begin{cases} \frac{|G|}{n_\psi}, & \text{if } \phi_{ij}^{\psi} = \phi_{kl}^{\chi}; \\ 0, & \text{if } \phi_{ij}^{\psi} \neq \phi_{kl}^{\chi}. \end{cases} \tag{2.6}$$

For any $f \in \mathbb{C}^G$, in the next definition we define its Fourier transform $\widehat{f}$ as a function on $\widehat{G}$. Note that this definition is equivalent to the original definition of $\widehat{f}$ in (2.1) and the inversion formula (2.2). In this paper we will regard $\widehat{f}$ as a function on irreducible representations and also on $\widehat{G}$ as well. To simplify the notation, the summation over all $\phi_{ij}^{\psi} \in \widehat{G}$ is denoted by $\sum_{(\psi,i,j)}$.

Definition 2.5 For any $f \in \mathbb{C}^G$, the *Fourier transform* $\widehat{f}$ of f on $\widehat{G}$ is defined by

$$\widehat{f}(\phi_{ij}^{\psi}) = \sum_{s \in G} f(s)\phi_{ij}^{\psi}(s), \qquad \text{for any } \phi_{ij}^{\psi} \in \widehat{G}.$$

On the other hand, for any function $\tau : \widehat{G} \to \mathbb{C}$, we define the *Fourier inversion* $\widehat{\tau} \in \mathbb{C}^G$ as follows:

$$\widehat{\tau}(s) = \frac{1}{|G|} \sum_{(\psi,i,j)} n_\psi \overline{\phi_{ij}^{\psi}}(s)\tau(\phi_{ij}^{\psi}), \qquad \text{for all } s \in G.$$

Thus, from Definition 2.5 and (2.1), we have

$$\widehat{f}(\Phi_\psi) = \left(\widehat{f}(\phi_{ij}^{\psi})\right)_{i,j}, \quad \text{for any } \psi \in \mathrm{Irr}(G). \tag{2.7}$$

Remark 2.6 Since $\widehat{G}$ is a basis of $\mathbb{C}^G$, we have $\mathbb{C}^G = \mathbb{C}\widehat{G}$. Let $\sigma : \widehat{G} \to \mathbb{C}$ be a function. Then σ can be linearly extended to a function (still denoted by σ) on $\mathbb{C}\widehat{G}$ as follows:

$$\sigma : \mathbb{C}\widehat{G} \to \mathbb{C}, \quad \sum_{(\psi,i,j)} \alpha_{ij}^{\psi}\phi_{ij}^{\psi} \mapsto \sum_{(\psi,i,j)} \alpha_{ij}^{\psi}\sigma\left(\phi_{ij}^{\psi}\right).$$

In particular, for any function $f : G \to \mathbb{C}$, its Fourier transform $\widehat{f}$, a function on $\widehat{G}$, is also a function on $\mathbb{C}\widehat{G}$ by linear extension.

The next lemma is straightforward.

Lemma 2.7 $\widehat{\widehat{f}} = f$ *for any* $f \in \mathbb{C}^G$, *and* $\widehat{\widehat{\tau}} = \tau$ *for any* $\tau \in \mathbb{C}^{\widehat{G}}$.

The next lemma discusses the relation between a function and its Fourier transform on $\widehat{G}$. It can be regarded as a reformulation of the inversion formula (2.2).

Lemma 2.8 *Let* $f \in \mathbb{C}^G$, *and* $\overline{f}$ *the complex conjugate of* f. *Then*

$$\overline{f} = \frac{1}{|G|} \sum_{(\psi,i,j)} n_\psi \overline{\widehat{f}(\phi_{ij}^{\psi})}\phi_{ij}^{\psi}.$$

Proof Since $\widehat{G}$ is a basis of $\mathbb{C}^G$, we may assume that $\overline{f} = \sum_{(\psi,i,j)} \alpha_{ij}^{\psi}\phi_{ij}^{\psi}$, where $\alpha_{ij}^{\psi} \in \mathbb{C}$. Therefore, $f = \sum_{(\psi,i,j)} \overline{\alpha_{ij}^{\psi}}\,\overline{\phi_{ij}^{\psi}}$, and hence $\widehat{f} = \sum_{(\psi,i,j)} \overline{\alpha_{ij}^{\psi}}\,\widehat{\overline{\phi_{ij}^{\psi}}}$. So by Lemma 2.4,

$$\widehat{f}(\phi_{kl}^{\chi}) = \sum_{(\psi,i,j)} \overline{\alpha_{ij}^{\psi}}\,\widehat{\overline{\phi_{ij}^{\psi}}}(\phi_{kl}^{\chi}) = \sum_{(\psi,i,j)} \overline{\alpha_{ij}^{\psi}} \left\langle \phi_{kl}^{\chi}, \phi_{ij}^{\psi} \right\rangle_G = \frac{|G|}{n_\chi}\overline{\alpha_{kl}^{\chi}}, \quad \text{for any } \phi_{kl}^{\chi} \in \widehat{G}.$$

Hence, the lemma holds. □

Remark 2.9 For any $s \in G$, we have the characteristic function $\mathbf{1}_s \in \mathbb{C}^G$ (i.e. $\mathbf{1}_s(t) = 0$ if $t \neq s$ and $\mathbf{1}_s(s) = 1$), whose Fourier transform is $\widehat{\mathbf{1}}_s(\phi_{ij}^{\psi}) = \phi_{ij}^{\psi}(s)$, for any $\phi_{ij}^{\psi} \in \widehat{G}$. For any function $\sigma : \widehat{G} \to \mathbb{C}$, it is straightforward to check that $\sigma = \sum_{s\in G} \widehat{\sigma}(s)\widehat{\mathbf{1}}_s$. So the Fourier transform and the Fourier inversion can be regarded as transformations between $\widehat{G}$ and $\{\widehat{\mathbf{1}}_s : s \in G\}$.

Let V be a vector space of dimension $|G|$ with a basis $B := \{e_t\}_{t\in G}$ indexed by the elements of G. Then any $s \in G$ induces a linear transformation (an isomorphism) $\Omega_s : V \to V$, $e_t \mapsto e_{st}$, for any $t \in G$.

Definition 2.10 With the notation in the above paragraph, the (left) *regular* representation of G is

$$\Omega : G \to GL(|G|, \mathbb{C}), \quad s \mapsto \mathrm{Mat}_B(\Omega_s),$$

where $\mathrm{Mat}_B(\Omega_s)$ is the matrix of Ω_s with respect to the basis B.

The *regular* character ρ of G is the character afforded by the (left) regular representation of G. It is known that $\rho = \sum_{\psi\in \mathrm{Irr}(G)} n_\psi \psi$ (see [12, Lemma 2.11]), $\rho(1_G) = |G|$, and $\rho(s) = 0$ for any $s \in G\backslash\{1_G\}$ (see [12, Lemma 2.10]). Let I_n be the $n \times n$ identity matrix for any positive integer n. For any $g \in \mathbb{C}^G$, since $\widehat{G}$ is a basis of $\mathbb{C}^G$, and $\rho = \sum_{(\psi,i)} n_\psi \phi_{ii}^{\psi}$, the following are equivalent by Lemma 2.8 and (2.7):

(i) $g(s) = 0$ for any $s \in G\backslash\{1_G\}$;
(ii) $g = \frac{g(1)}{|G|}\rho$ (or $\overline{g} = \frac{\overline{g}(1)}{|G|}\rho$);
(iii) $\widehat{g}(\Phi_\psi) = g(1)I_{n_\psi}$, for any $\psi \in \mathrm{Irr}(G)$.

More generally, we have the next result.

Lemma 2.11 (Cf. [27, Lemma 2.1]) *Let $f \in \mathbb{C}^G$ and $\lambda \in \mathbb{C}$. Then the following are equivalent.*

(i) For any $s \in G\backslash\{1_G\}$, $f(s) = \lambda$.
(ii) For any non-principal irreducible character ψ of G, $\widehat{f}(\Phi_\psi) = (f(1) - \lambda)I_{n_\psi}$.

Proof Let $g = f - \lambda\psi_1$, where ψ_1 is the principal irreducible character of G. Note that for any non-principal irreducible character ψ of G, $\sum_{x\in G} \Phi_\psi(x) = O$ (the zero matrix, cf. [12, Problem 2.1]). Hence,

$$\widehat{g}(\Phi_\psi) = \widehat{f}(\Phi_\psi), \quad \text{for any non-principal irreducible character } \psi \text{ of } G. \tag{2.8}$$

Assume (i). Then $g = \frac{g(1)}{|G|}\rho$, and hence for any $\psi \in \mathrm{Irr}(G)$, $\widehat{g}(\Phi_\psi) = g(1)I_{n_\psi}$ by the remark before the lemma. So (ii) holds by (2.8).

Assume (ii). Then by Lemma 2.8 and (2.8),

$$\begin{aligned}\overline{g} &= \frac{1}{|G|}\sum_{(\psi,i,j)} n_\psi \overline{\widehat{g}(\phi_{ij}^{\psi})}\phi_{ij}^{\psi} = \frac{1}{|G|}\overline{\widehat{g}(\psi_1)}\psi_1 + \frac{1}{|G|}\sum_{(\psi,i),\psi\neq\psi_1} n_\psi \left(\overline{f(1)} - \overline{\lambda}\right)\phi_{ii}^{\psi} \\ &= \frac{\overline{g}(1)}{|G|}\rho + \frac{1}{|G|}\left(\overline{\widehat{g}(\psi_1)} - \overline{g}(1)\right)\psi_1.\end{aligned}$$

Thus, $\overline{g}(1) = \frac{\overline{g}(1)}{|G|}\rho(1) + \frac{1}{|G|}\left(\overline{\widehat{g}(\psi_1)} - \overline{g}(1)\right)\psi_1(1)$, and hence $\overline{\widehat{g}(\psi_1))} - \overline{g}(1) = 0$. So $\overline{g} = \frac{\overline{g}(1)}{|G|}\rho$, and (i) holds. □

The next corollary will be needed later.

Corollary 2.12 *The following hold:*

(i) A function $f \in \mathbb{C}^G$ is constant on G if and only if for any non-principal irreducible character ψ of G, $\widehat{f}(\Phi_\psi) = O$, the zero matrix.
(ii) For any $\sum_{s\in G} \alpha_s s \in \mathbb{C}G$, α_s are equal for all $s \in G$ if and only if for any non-principal irreducible character ψ of G, $\Phi_\psi\left(\sum_{s\in G} \alpha_s s\right) = O$, the zero matrix.

Proof (i) follows directly from Lemma 2.11, with $f(1) = \lambda$.
(ii) Let $f : G \to \mathbb{C}, s \mapsto \alpha_s$. Then $\widehat{f}(\Phi_\psi) = \Phi_\psi\left(\sum_{s\in G} \alpha_s s\right)$. So (ii) follows from (i). □

The set $\mathbb{C}^{\widehat{G}}$ of complex functions on $\widehat{G}$ is also a unitary complex space with the inner product:

$$\langle \xi, \eta\rangle_{\widehat{G}} = \sum_{(\psi,i,j)} n_\psi \xi(\phi_{ij}^\psi)\overline{\eta}(\phi_{ij}^\psi), \qquad \text{for any } \xi, \eta \in \mathbb{C}^{\widehat{G}}, \tag{2.9}$$

where $\overline{\eta} : \widehat{G} \to \mathbb{C}$ is the complex conjugate of η defined by $\overline{\eta}(\phi_{ij}^\psi) = \overline{\eta(\phi_{ij}^\psi)}$, for any $\phi_{ij}^\psi \in \widehat{G}$.

Lemma 2.13 *For any $f, g \in \mathbb{C}^G$,*

$$\left\langle \widehat{f}, \widehat{g}\right\rangle_{\widehat{G}} = |G|\langle f, g\rangle_G.$$

Proof It follows from (2.9), (2.5), Definition 2.5, and Lemma 2.2(iii, iv) that

$$\begin{aligned}
\left\langle \widehat{f}, \widehat{g}\right\rangle_{\widehat{G}} &= \sum_{(\psi,i,j)} n_\psi \widehat{f}(\phi_{ij}^\psi)\overline{\widehat{g}(\phi_{ij}^\psi)} = \sum_{(\psi,i,j)} \sum_{s,t\in G} n_\psi f(s)\phi_{ij}^\psi(s)\overline{g(t)}\,\overline{\phi_{ij}^\psi(t)} \\
&= \sum_{s,t\in G} f(s)\overline{g(t)} \sum_{(\psi,i,j)} n_\psi \phi_{ij}^\psi(s)\phi_{ji}^\psi(t^{-1}) \\
&= \sum_{s,t\in G} f(s)\overline{g(t)}\rho(st^{-1}), \quad \text{where } \rho \text{ is the regular character of } G, \\
&= |G|\langle f, g\rangle_G.
\end{aligned}$$

So the lemma holds. □

3 Bent functions

In this section we study characterizations of bent functions by their Fourier transforms on the dual basis $\widehat{G}$. The main results are Theorems 3.3 and 3.4 below.

In the following we always assume that G is an arbitrary finite group, $\Phi_\psi = \left(\phi_{ij}^\psi\right)_{i,j}$ is a unitary irreducible representation of G that affords ψ, for any $\psi \in \mathrm{Irr}(G)$, and $\widehat{G} := \{\phi_{ij}^\psi : \psi \in \mathrm{Irr}(G), 1 \le i, j \le n_\psi\}$ is a dual basis of G. For any matrix M, let M^* denote the conjugate transpose of M. Let $T := \{z \in \mathbb{C} : |z| = 1\}$ be the unit circle in $\mathbb{C}$.

Definition 3.1 (*Cf.* [18, *Definition 9*]) A function $f : G \to T$ is called a *bent function* if

$$\widehat{f}(\Phi_\psi)\left[\widehat{f}(\Phi_\psi)\right]^* = |G| I_{n_\psi}, \quad \text{for any } \psi \in \mathrm{Irr}(G).$$

A function $g \in \mathbb{C}^G$ is said to be *balanced* on G if $\sum_{x\in G} g(x) = 0$.

Let $f : G \to \mathbb{C}$ be a function, and $a \in G$. Then the *derivative* of f in the direction a, $d_a f$, is defined by

$$d_a f : G \to \mathbb{C}, \quad x \mapsto f(ax)\overline{f(x)}.$$

Poinsot [18, Theorem 3] characterizes a bent function by its derivatives (see Corollary 3.9 below).

Let $\sigma : \widehat{G} \to \mathbb{C}$ be a function. Then σ is also a function on $\mathbb{C}\widehat{G}$ by linear extension. We can define the derivative of σ in a similar way. That is, for any $a \in G$, the *derivative* of σ in the direction a, $d_a\sigma$, is defined by

$$d_a\sigma : \widehat{G} \to \mathbb{C}, \quad \phi_{ij}^{\psi} \mapsto \sigma(a\phi_{ij}^{\psi})\overline{\sigma(\phi_{ij}^{\psi})}.$$

Recall that the G-action on $\widehat{G}$ is given by (2.4); i.e. $a\phi_{ij}^{\psi} = \sum_{k=1}^{n_\psi} \phi_{ik}^{\psi}(a^{-1})\phi_{kj}^{\psi}$, for any $a \in G$ and $\phi_{ij}^{\psi} \in \widehat{G}$.

Definition 3.2 A function $\sigma : \widehat{G} \to \mathbb{C}$ is said to be *balanced* on $\widehat{G}$ if

$$\sum_{(\psi,i,j)} n_\psi \sigma(\phi_{ij}^{\psi}) = 0.$$

The next theorem is our first main result of this section. It characterizes a bent function f by the derivatives of its Fourier transform $\widehat{f}$.

Theorem 3.3 *Let $f : G \to T$ be a function. Then the following are equivalent.*

(i) f is a bent function.
(ii) For any $a \in G\backslash\{1_G\}$, $d_a\widehat{f}$ is balanced on $\widehat{G}$. That is,

$$\sum_{(\psi,i,j)} n_\psi \widehat{f}(a\phi_{ij}^{\psi})\,\overline{\widehat{f}(\phi_{ij}^{\psi})} = 0, \quad \text{for any } a \in G\backslash\{1_G\}.$$

The *kernel* of $\psi \in \mathrm{Irr}(G)$ is $\ker\psi := \{s \in G : \psi(s) = n_\psi\}$. It is well known that $\ker\psi$ is a normal subgroup of G. To simply the notation, for a normal subgroup N of G, let

$$N^{\perp} := \{\psi : \psi \in \mathrm{Irr}(G) \text{ and } \ker\psi \supseteq N\}. \tag{3.1}$$

Such a notation is used for subgroups of an abelian group in the literature (cf. [15], etc.), with slightly different definitions.

In the case that $f \in \mathbb{C}^G$ is not bent, the conditions under which the set $\{a \in G : d_a f$ is balanced on $G\}$ contains $Q\backslash\{1_G\}$ for some subgroup Q of G (when G is abelian) have been studied in the literature (cf. [15], etc.). Our second main result of this section characterizes functions f that have balanced derivatives $d_a f$ for a $(\neq 1_G)$ in a normal subgroup. Note that Theorem 3.4 below is not a generalization of the results of Logachev et al. (cf. [15, Theorems 4 and 5]).

Theorem 3.4 *Let $f : G \to T$ be a function, and N $(\neq \{1_G\})$ a normal subgroup of G. Then the following are equivalent.*

(i) For any $a \in N\backslash\{1_G\}$, $d_a f$ is balanced on G, i.e. $\sum_{s\in G}(d_a f)(s) = 0$.
(ii) For any $a \in N\backslash\{1_G\}$, $d_a\widehat{f}$ is balanced on $\widehat{G}$, i.e. $\sum_{(\psi,i,j)} n_\psi (d_a\widehat{f})(\phi_{ij}^{\psi}) = 0$.

(iii) For any $a \in N\backslash\{1_G\}$,

$$\sum_{(\psi,i,j),\psi\notin N^\perp} n_\psi\big(d_a\widehat{f}\big)(\phi_{ij}^\psi) = -\frac{|G|^2}{|N|}.$$

The rest of this section is devoted to the proofs of Theorems 3.3 and 3.4. Let us start with the following definition.

Definition 3.5 Let $f \in \mathbb{C}^G$. If $f = \sum_{(\psi,i,j)} \alpha_{ij}^\psi \phi_{ij}^\psi$, where $\alpha_{ij}^\psi \in \mathbb{C}$, then for any $\psi \in \mathrm{Irr}(G)$, $f_\psi := \sum_{i,j=1}^{n_\psi} \alpha_{ij}^\psi \phi_{ij}^\psi$ is called the ψ-*component* of f, and the $n_\psi \times n_\psi$ matrix $M(f)_\psi := \big(\alpha_{ij}^\psi\big)_{i,j}$ is called the ψ-*matrix* of f.

For a matrix $M = (\alpha_{ij})_{i,j}$, let $\overline{M} = (\overline{\alpha_{ij}})_{i,j}$. Then for any $f \in \mathbb{C}^G$, it follows from Lemma 2.8 and (2.7) that

$$M\big(\overline{f}\big)_\psi = \frac{n_\psi}{|G|}\overline{\widehat{f}(\Phi_\psi)}, \quad \text{for any } \psi \in \mathrm{Irr}(G). \tag{3.2}$$

Hence, the following are equivalent by the remark before Lemma 2.11: (i) $f(s) = 0$ for any $s \in G\backslash\{1_G\}$; (ii) $M(f)_\psi = f(1)\frac{n_\psi}{|G|} I_{n_\psi}$, for any $\psi \in \mathrm{Irr}(G)$; and (iii) $\widehat{f}(\Phi_\psi) = f(1) I_{n_\psi}$, for any $\psi \in \mathrm{Irr}(G)$.

The convolutions of functions on G play an important role in the study of bent functions when G is abelian. For any two functions $\sigma, \tau \in \mathbb{C}^G$, the *convolution* of σ and τ, $\sigma * \tau$, is defined by

$$\sigma * \tau : G \to \mathbb{C}, \quad a \mapsto \sum_{s\in G} \sigma(s)\tau(s^{-1}a). \tag{3.3}$$

If G is abelian and $\tau \in \widehat{G}$, then $\tau(s^{-1}) = \overline{\tau(s)}$ for any $s \in G$. But if G is nonabelian, then for any $\phi_{ij}^\psi \in \widehat{G}$ and $s \in G$, $\phi_{ij}^\psi(s^{-1}) \neq \overline{\phi_{ij}^\psi(s)}$ in general (see Lemma 2.2(iii)). So for nonabelian finite groups, we need a modified convolution.

Definition 3.6 Let $f, g \in \mathbb{C}^G$. Then the *quasi-convolution* of f and g, $f \circledast g$, is defined by

$$f \circledast g : G \to \mathbb{C}, \quad a \mapsto \sum_{x\in G} f(ax)\overline{g(x)}.$$

Lemma 3.7 *Let* $f, g \in \mathbb{C}^G$. *Then the following hold.*

(i) For any $\psi \in \mathrm{Irr}(G)$, $M(f \circledast g)_\psi = \frac{|G|}{n_\psi} M(f)_\psi \big[M(g)_\psi\big]^*$.
(ii) For any $\psi, \chi \in \mathrm{Irr}(G)$, $(f \circledast g)_\psi = f_\psi \circledast g_\psi$, *and* $f_\psi \circledast g_\chi = 0$ *if* $\psi \neq \chi$.

Proof (i) Assume that $f = \sum_{(\psi,i,j)} \alpha_{ij}^{\psi}\phi_{ij}^{\psi}$, and $g = \sum_{(\chi,k,l)} \beta_{kl}^{\chi}\phi_{kl}^{\chi}$. Then for any $a \in G$, it follows from Lemma 2.2(iv) and Lemma 2.4 that

$$\begin{aligned}(f\circledast g)(a) &= \sum_{x\in G}\sum_{(\psi,i,j)} \alpha_{ij}^{\psi}\phi_{ij}^{\psi}(ax)\sum_{(\chi,k,l)}\overline{\beta_{kl}^{\chi}}\,\overline{\phi_{kl}^{\chi}(x)}\\ &= \sum_{(\psi,i,j)}\sum_{(\chi,k,l)} \alpha_{ij}^{\psi}\overline{\beta_{kl}^{\chi}}\sum_{x\in G}\sum_{m=1}^{n_\psi}\phi_{im}^{\psi}(a)\phi_{mj}^{\psi}(x)\overline{\phi_{kl}^{\chi}(x)}\\ &= \sum_{(\psi,i,j)}\sum_{(\chi,k,l)} \alpha_{ij}^{\psi}\overline{\beta_{kl}^{\chi}}\sum_{m=1}^{n_\psi}\phi_{im}^{\psi}(a)\left\langle\phi_{mj}^{\psi},\phi_{kl}^{\chi}\right\rangle_G\\ &= \sum_{(\psi,i,j)}\sum_{k=1}^{n_\psi}\frac{|G|}{n_\psi}\alpha_{ij}^{\psi}\overline{\beta_{kj}^{\psi}}\phi_{ik}^{\psi}(a) \;=\; \sum_{(\psi,i,k)}\frac{|G|}{n_\psi}\sum_{j=1}^{n_\psi}\alpha_{ij}^{\psi}\overline{\beta_{kj}^{\psi}}\phi_{ik}^{\psi}(a).\end{aligned}$$

So (i) holds.

(ii) follows directly from (i) and its proof. □

The next lemma characterizes a function with balanced derivatives in terms of its ψ-matrices, for all $\psi \in \mathrm{Irr}(G)$.

Lemma 3.8 *Let $f : G \to \mathbb{C}$ be a function. Then the following are equivalent.*

(i) For any $a \in G\backslash\{1_G\}$, $d_a f$ is balanced.
(ii) $f\circledast f = \frac{\beta}{|G|}\rho$, where $\beta = \sum_{x\in G}|f(x)|^2$, and ρ is the regular character.
(iii) For any $\psi \in \mathrm{Irr}(G)$,

$$M(f)_\psi\big[M(f)_\psi\big]^* = \frac{n_\psi^2}{|G|^2}\beta I_{n_\psi}, \quad \textit{where } \beta \textit{ is the same as in (ii).}$$

Proof Since for any $a \in G$, $\sum_{x\in G} d_a f(x) = \sum_{x\in G} f(ax)\overline{f(x)} = (f\circledast f)(a)$, (i) and (ii) are equivalent. From the remark after Definition 3.5, (ii) holds if and only if for any $\psi \in \mathrm{Irr}(G)$, $M(f\circledast f)_\psi = \frac{n_\psi}{|G|}\beta I_{n_\psi}$. Hence, (ii) and (iii) are equivalent by Lemma 3.7. □

Since for a function $f : G \to T$, $f\circledast f = \rho$ if and only if $\overline{f}\circledast\overline{f} = \rho$, as a direct consequence of Lemma 3.8 and (3.2), we have the next result.

Corollary 3.9 (Cf. [18, Theorem 3]) *A function $f : G \to T$ is bent if and only if for any $a \in G\backslash\{1_G\}$, $d_a f$ is balanced.*

Remark 3.10 Theorem 3.3 can also be obtained as a consequence of Theorem 3.4 (with $N = G$) and Corollary 3.9. But our approach to the proof of Theorem 3.3 yields Corollary 3.9 as a direct consequence, and provides a clear explanation why Theorem 3.3 and Corollary 3.9 are true.

Similar to Definition 3.6, we can define the quasi-convolution of two functions on the dual basis $\widehat{G}$ as a function on G.

Definition 3.11 Let σ, τ be functions on the dual basis $\widehat{G}$. Then the *quasi-convolution* of σ and τ, $\sigma\circledast\tau$, is a function on G defined by

$$\sigma\circledast\tau : G \to \mathbb{C}, \quad a \mapsto \sum_{(\psi,i,j)} n_\psi\sigma(a\phi_{ij}^{\psi})\,\overline{\tau(\phi_{ij}^{\psi})}.$$

Therefore, for any $\sigma, \tau \in \mathbb{C}^{\widehat{G}}$,

$$(\sigma \circledast \tau)(1_G) = \langle \sigma, \tau \rangle_{\widehat{G}} \quad \text{and} \quad \sum_{(\psi,i,j)} n_\psi \, d_a \sigma(\phi_{ij}^\psi) = (\sigma \circledast \sigma)(a), \quad \text{for any } a \in G. \tag{3.4}$$

For any function $\sigma : \widehat{G} \to \mathbb{C}$ and any $\psi \in \mathrm{Irr}(G)$, let $\sigma(\Phi_\psi)$ be the $n_\psi \times n_\psi$ matrix $\big(\sigma(\phi_{ij}^\psi)\big)_{i,j}$, and let $\overline{\sigma(\Phi_\psi)}$ be the conjugate of $\sigma(\Phi_\psi)$, i.e. $\overline{\sigma(\Phi_\psi)} := \Big(\overline{\sigma(\phi_{ij}^\psi)}\Big)_{i,j}$. The transpose of a matrix M is denoted by $M^\top$.

Lemma 3.12 *For any functions σ and τ on $\widehat{G}$ and any $\psi \in \mathrm{Irr}(G)$, the ψ-matrix of $\overline{\sigma \circledast \tau}$ is*

$$M\big(\overline{\sigma \circledast \tau}\big)_\psi = n_\psi \, \overline{\sigma(\Phi_\psi)} \, \tau(\Phi_\psi)^\top.$$

Proof Since for any $a \in G$ and $\phi_{ij}^\psi \in \widehat{G}$, $a\phi_{ij}^\psi = \sum_{k=1}^{n_\psi} \phi_{ik}^\psi(a^{-1})\phi_{kj}^\psi$ by (2.4), it follows that

$$\begin{aligned}\sum_{(\psi,i,j)} n_\psi \sigma(a\phi_{ij}^\psi)\,\overline{\tau(\phi_{ij}^\psi)} &= \sum_{(\psi,i,j)} n_\psi \sum_{k=1}^{n_\psi} \phi_{ik}^\psi(a^{-1})\sigma(\phi_{kj}^\psi)\,\overline{\tau(\phi_{ij}^\psi)} \\ &= \sum_{\psi \in \mathrm{Irr}(G)} n_\psi \sum_{k,i=1}^{n_\psi} \left(\sum_{j=1}^{n_\psi} \sigma(\phi_{kj}^\psi)\,\overline{\tau(\phi_{ij}^\psi)} \right) \overline{\phi_{ki}^\psi(a)}.\end{aligned}$$

Let β_{ki}^ψ be the (k,i)-entry of $\sigma(\Phi_\psi)\big[\tau(\Phi_\psi)\big]^*$. Then $\beta_{ki}^\psi = \sum_{j=1}^{n_\psi} \sigma(\phi_{kj}^\psi)\,\overline{\tau(\phi_{ij}^\psi)}$. Hence,

$$(\sigma \circledast \tau)(a) = \sum_{(\psi,k,i)} n_\psi \beta_{ki}^\psi \overline{\phi_{ki}^\psi(a)}, \quad \text{for any } a \in G.$$

So the lemma holds. □

Now we are ready to prove Theorem 3.3.

Proof of Theorem 3.3 Since $\langle \widehat{f}, \widehat{f} \rangle_{\widehat{G}} = |G|\langle f, f \rangle_G = |G|^2$ by Lemma 2.13, it follows from (3.4) that

$$\text{(ii) holds} \quad \Leftrightarrow \quad \widehat{f} \circledast \widehat{f} = |G|\rho \quad \Leftrightarrow \quad \overline{\widehat{f} \circledast \widehat{f}} = |G|\rho,$$

where ρ is the regular character. But by Lemma 3.12,

$$\begin{aligned}\overline{\widehat{f} \circledast \widehat{f}} = |G|\rho &\Leftrightarrow M\Big(\overline{\widehat{f} \circledast \widehat{f}}\Big)_\psi = n_\psi |G| I_{n_\psi}, \quad \text{for any } \psi \in \mathrm{Irr}(G) \\ &\Leftrightarrow \overline{\widehat{f}(\Phi_\psi)}\big[\widehat{f}(\Phi_\psi)\big]^\top = |G| I_{n_\psi}, \quad \text{for any } \psi \in \mathrm{Irr}(G).\end{aligned}$$

Since $\overline{\widehat{f}(\Phi_\psi)}\big[\widehat{f}(\Phi_\psi)\big]^\top = |G| I_{n_\psi}$ if and only if $\widehat{f}(\Phi_\psi)\big[\widehat{f}(\Phi_\psi)\big]^* = |G| I_{n_\psi}$, the theorem holds. □

In order to prove Theorem 3.4, we need the next two lemmas. Lemma 3.13 is also needed for the proof of Theorem 4.3 in Sect. 4.

Lemma 3.13 *Let N be a normal subgroup of G. Then the following hold.*

(i) For any $s \in G$,

$$\sum_{(\psi,i),\,\psi \in N^\perp} n_\psi \phi_{ii}^\psi(s) = \begin{cases} |G/N|, & \text{if } s \in N; \\ 0, & \text{if } s \notin N. \end{cases} \tag{3.5}$$

(ii) For any $a \in N\backslash\{1_G\}$ and $b \in G$,

$$\sum_{(\psi,i),\psi\notin N^\perp} n_\psi \phi_{ii}^\psi(a^{-1}b) = \begin{cases} |G| - |G/N|, & \text{if } b = a; \\ -|G/N|, & \text{if } b \in N\backslash\{a\}; \\ 0, & \text{otherwise.} \end{cases} \tag{3.6}$$

Proof (i) For any $\psi \in \mathrm{Irr}(G)$ such that $\ker\psi \supseteq N$, Φ_ψ is also an irreducible representation of the quotient group G/N with $\Phi_\psi(sN) = \Phi_\psi(s)$, for any $s \in G$, and ψ is also an irreducible character of G/N with $\psi(sN) = \psi(s)$, for any $s \in G$. Furthermore, $\mathrm{Irr}(G/N) = \{\psi : \psi \in \mathrm{Irr}(G) \text{ and } \ker\psi \supseteq N\}$, i.e. $\mathrm{Irr}(G/N) = N^\perp$. Hence, $\sum_{\psi\in N^\perp}\sum_{1\le i\le n_\psi} n_\psi\phi_{ii}^\psi$ is the regular character of G/N, and (i) holds.

(ii) Since

$$\begin{aligned}\sum_{(\psi,i),\psi\notin N^\perp} n_\psi \phi_{ii}^\psi(a^{-1}b) &= \sum_{(\psi,i)} n_\psi \phi_{ii}^\psi(a^{-1}b) - \sum_{(\psi,i),\psi\in N^\perp} n_\psi \phi_{ii}^\psi(a^{-1}b) \\ &= \rho(a^{-1}b) - \sum_{(\psi,i),\psi\in N^\perp} n_\psi \phi_{ii}^\psi(a^{-1}b),\end{aligned}$$

where ρ is the regular character of G, (ii) follows directly from (3.5). □

Lemma 3.14 *Let $f \in \mathbb{C}^G$. Then for any $a \in G$,*

$$\sum_{(\psi,i,j)} n_\psi \left(d_a\widehat{f}\right)(\phi_{ij}^\psi) = |G| \sum_{t\in G} (d_a f)(t).$$

Proof For any $a, s \in G$ and $\phi_{ij}^\psi \in \widehat{G}$, $\left(a\phi_{ij}^\psi\right)(s) = \phi_{ij}^\psi(a^{-1}s)$ by (2.3). Thus,

$$\begin{aligned}\sum_{j=1}^{n_\psi} \left(d_a\widehat{f}\right)(\phi_{ij}^\psi) &= \sum_{j=1}^{n_\psi} \widehat{f}(a\phi_{ij}^\psi)\overline{\widehat{f}(\phi_{ij}^\psi)} = \sum_{j=1}^{n_\psi}\sum_{s,t\in G} f(s)\left(a\phi_{ij}^\psi\right)(s)\,\overline{f(t)}\,\overline{\phi_{ij}^\psi(t)} \\ &= \sum_{s,t\in G}\sum_{j=1}^{n_\psi} \phi_{ij}^\psi(a^{-1}s)\overline{\phi_{ij}^\psi(t)}\, f(s)\overline{f(t)} \\ &= \sum_{s,t\in G} \phi_{ii}^\psi(a^{-1}st^{-1}) f(s)\overline{f(t)}. \quad \text{(by Lemma 2.2(iii, iv))} \\ &= \sum_{b,t\in G} \phi_{ii}^\psi(a^{-1}b) f(bt)\overline{f(t)}. \quad (\text{where } b = st^{-1})\end{aligned}$$

That is,

$$\sum_{j=1}^{n_\psi} \left(d_a\widehat{f}\right)(\phi_{ij}^\psi) = \sum_{b,t\in G} \phi_{ii}^\psi(a^{-1}b) f(bt)\overline{f(t)}. \tag{3.7}$$

Hence,

$$\begin{aligned}\sum_{(\psi,i,j)} n_\psi \left(d_a\widehat{f}\right)(\phi_{ij}^\psi) &= \sum_{(\psi,i)}\sum_{b,t\in G} n_\psi \phi_{ii}^\psi(a^{-1}b) f(bt)\overline{f(t)} \\ &= \sum_{b,t\in G} \rho(a^{-1}b) f(bt)\overline{f(t)} \quad (\text{where } \rho \text{ is the regular character of G}) \\ &= |G| \sum_{t\in G} f(at)\overline{f(t)}.\end{aligned}$$

So the lemma holds. □

Now we are ready to prove Theorem 3.4.

Proof of Theorem 3.4 The equivalence of (i) and (ii) follows directly from Lemma 3.14. In the following we prove that (ii) implies (iii) and that (iii) implies (i).

Assume (ii). Then for any $a \in N\backslash\{1_G\}$,

$$\begin{aligned}
&\sum_{(\psi,i,j),\psi\notin N^\perp} n_\psi\big(d_a\widehat{f}\big)(\phi_{ij}^\psi)\\
&= \sum_{(\psi,i,j)} n_\psi\big(d_a\widehat{f}\big)(\phi_{ij}^\psi) - \sum_{(\psi,i,j),\psi\in N^\perp} n_\psi\big(d_a\widehat{f}\big)(\phi_{ij}^\psi)\\
&= 0 - \sum_{(\psi,i),\psi\in N^\perp}\sum_{b,t\in G} n_\psi\phi_{ii}^\psi(a^{-1}b)f(bt)\overline{f(t)} \quad \text{(by (ii) and (3.7))}\\
&= -|G/N|\sum_{b\in N,t\in G} f(bt)\overline{f(t)} \quad \text{(by (3.5), because } a\in N)\\
&= -\frac{|G|}{|N|}\sum_{t\in G} f(t)\overline{f(t)} \quad \text{(from the equivalence of (i) and (ii))}\\
&= -\frac{|G|^2}{|N|}.
\end{aligned}$$

This proves that (ii) implies (iii).

Now assume (iii). For any $a \in N\backslash\{1_G\}$,

$$\begin{aligned}
&\sum_{(\psi,i,j),\psi\notin N^\perp} n_\psi\big(d_a\widehat{f}\big)(\phi_{ij}^\psi)\\
&= \sum_{(\psi,i),\psi\notin N^\perp}\sum_{b,t\in G} n_\psi\phi_{ii}^\psi(a^{-1}b)f(bt)\overline{f(t)} \quad \text{(by (3.7))}\\
&= (|G|-|G/N|)\sum_{t\in G} f(at)\overline{f(t)} - |G/N|\sum_{b\in N\backslash\{a\}}\sum_{t\in G} f(bt)\overline{f(t)} \quad \text{(by (3.6))}\\
&= |G|\sum_{t\in G} f(at)\overline{f(t)} - |G/N|\sum_{b\in N}\sum_{t\in G} f(bt)\overline{f(t)}\\
&= |G|\sum_{t\in G} f(at)\overline{f(t)} - |G/N|\sum_{\substack{b\in N\\ b\neq 1_G}}\sum_{t\in G} f(bt)\overline{f(t)} - \frac{|G|^2}{|N|}.
\end{aligned}$$

Thus, (iii) implies that

$$|G|\sum_{t\in G} f(at)\overline{f(t)} - |G/N|\sum_{\substack{b\in N\\ b\neq 1_G}}\sum_{t\in G} f(bt)\overline{f(t)} = 0, \quad \text{for any } a\in N\backslash\{1_G\}.$$

That is,

$$|N|\sum_{t\in G} f(at)\overline{f(t)} = \sum_{\substack{b\in N\\ b\neq 1_G}}\sum_{t\in G} f(bt)\overline{f(t)}, \quad \text{for any } a\in N\backslash\{1_G\}.$$

The above equality says that $\sum_{t\in G} f(at)\overline{f(t)}$ are equal for all $a \in N\backslash\{1_G\}$, and hence

$$|N|\sum_{t\in G} f(at)\overline{f(t)} = (|N|-1)\sum_{t\in G} f(at)\overline{f(t)}, \quad \text{for all } a \in N\backslash\{1_G\}.$$

So we must have that $\sum_{t\in G} f(at)\overline{f(t)} = 0$, for all $a \in N\backslash\{1_G\}$. This proves that (iii) implies (i). □

4 Perfect nonlinear functions

In this section we always assume that G and H are arbitrary finite groups, and study characterizations of perfect nonlinear functions from G to H. Our main results are Theorems 4.2, 4.3, and 4.7.

Let $f : G \to H$ be a function. For any $h \in H$, let $f^{-1}(h) := \{s \in G : f(s) = h\}$ be the inverse image of h under f. If $|H|$ divides $|G|$, and for any $h \in H$, $|f^{-1}(h)| = |G|/|H|$, then we say that f is *evenly-balanced* (cf [26]). An evenly-balanced function is also called a *balanced* function in the literature (cf. [4,19]).

The (*left*) *derivative* of a function $f : G \to H$ in direction $a \in G$ is defined by (cf. [19])

$$D_a f : G \to H, \quad x \mapsto f(ax)f(x)^{-1}.$$

Definition 4.1 (*Cf.* [19, *Definition 1.1*]) Let G, H be finite groups. Then a function $f : G \to H$ is said to be *perfect nonlinear* if for any $a \in G\backslash\{1_G\}$, $D_a f$ is evenly-balanced.

For any two functions $\sigma, \tau \in \mathbb{C}^G$, the *convolution* of σ and τ, $\sigma * \tau$, is defined by (3.3). It is clear that for any $a \in G$, $(\sigma * \tau)(a) = \sum_{s\in G} \sigma(as)\tau(s^{-1})$. For any $\sigma \in \mathbb{C}^G$, we define a function $\overline{\sigma}^{(-)} \in \mathbb{C}^G$ by

$$\overline{\sigma}^{(-)} : G \to \mathbb{C}, \quad a \mapsto \overline{\sigma(a^{-1})}.$$

Since $\{\mathbf{1}_s : s \in G\}$ is a basis of $\mathbb{C}^G$, where $\mathbf{1}_s$ is the characteristic function (i.e. $\mathbf{1}_s(t) = 0$ if $t \neq s$ and $\mathbf{1}_s(s) = 1$), for any function $f : G \to H$, we can define the *dual* function $\widetilde{f}$ of f as follows:

$$\widetilde{f} : \mathbb{C}^G \to \mathbb{C}^H, \quad \sum_{s\in G} \alpha_s \mathbf{1}_s \mapsto \sum_{s\in G} \alpha_s \mathbf{1}_{f(s)}.$$

In particular, $\widetilde{f}$ is also a function on $\widehat{G}$.

The next theorem characterizes a perfect nonlinear function in terms of its dual function and the dual basis $\widehat{G}$.

Theorem 4.2 *Let G, H be finite groups, and $f : G \to H$ a function. Then the following are equivalent.*

(i) f is a perfect nonlinear function.
(ii) For any $a \in G\backslash\{1_G\}$,

$$\sum_{(\psi,i,j)} n_\psi \left(\widetilde{f}(a\phi_{ij}^{\psi}) * \overline{\left[\widetilde{f}(\phi_{ij}^{\psi})\right]}^{(-)}\right) = \frac{|G|^2}{|H|}\zeta_1,$$

where ζ_1 is the principal irreducible character of H.

Let $f : G \to H$ be a function. In the case that f is not perfect nonlinear, the set $\{a \in G | D_a f : G \to H \text{ is evenly-balanced}\}$ describes how close f is to being perfect nonlinear. Let N be a normal subgroup of G. The next theorem discusses the sufficient and necessary conditions under which $D_a f : G \to H$ is evenly-balanced for any $a \in N \backslash \{1_G\}$. Recall that $N^\perp := \{\psi : \psi \in \mathrm{Irr}(G) \text{ and } \ker \psi \supseteq N\}$ (see (3.1)).

Theorem 4.3 *Let G, H be finite groups, $f : G \to H$ a function, and N ($\neq \{1_G\}$) a normal subgroup of G. Let ρ_H and ζ_1 be the regular character and principal irreducible character of H, respectively. Then the following are equivalent.*

(i) For any $a \in N \backslash \{1_G\}$, $D_a f : G \to H$ is evenly-balanced.
(ii) For any $a \in N \backslash \{1_G\}$,

$$\sum_{(\psi,i,j)} n_\psi \left(\widetilde{f}(a\phi_{ij}^\psi) * \overline{\left[\widetilde{f}(\phi_{ij}^\psi)\right]}^{(-)} \right) = \frac{|G|^2}{|H|}\zeta_1.$$

(iii) For any $a \in N \backslash \{1_G\}$,

$$\sum_{(\psi,i,j),\psi \notin N^\perp} n_\psi \left(\widetilde{f}(a\phi_{ij}^\psi) * \overline{\left[\widetilde{f}(\phi_{ij}^\psi)\right]}^{(-)} \right) = \frac{|G|^2}{|H| \cdot |N|}(\zeta_1 - \rho_H).$$

Note that Theorem 4.2 is a special case of Theorem 4.3 with $N = G$. So we only need to prove Theorem 4.3. We need the next two lemmas first.

Lemma 4.4 *Let G, H be finite groups, and $f : G \to H$ a function. Then f is evenly-balanced if and only if*

$$\sum_{s \in G} \mathbf{1}_{f(s)} = \frac{|G|}{|H|}\zeta_1, \quad \text{where } \zeta_1 \text{ is the principal irreducible character of } H.$$

Proof If f is evenly-balanced, then in the group algebra $\mathbb{C}H$,

$$\sum_{s \in G} f(s) = \frac{|G|}{|H|} \sum_{h \in H} h. \tag{4.1}$$

On the other hand, if (4.1) holds, then for any $h \in H$, by comparing the coefficients of h in both sides of (4.1), we see that $|H|$ divides $|G|$, and $|f^{-1}(h)| = |G|/|H|$. Thus, f is evenly-balanced if and only if (4.1) holds. Since $\{\mathbf{1}_h : h \in H\}$ is a basis of $\mathbb{C}^H$, it follows that (4.1) holds if and only if

$$\sum_{s \in G} \mathbf{1}_{f(s)} = \frac{|G|}{|H|} \sum_{h \in H} \mathbf{1}_h = \frac{|G|}{|H|}\zeta_1.$$

So the lemma holds. □

Lemma 4.5 *Let G, H be finite groups, $a \in G \backslash \{1_G\}$, and $f : G \to H$ a function. Then $D_a f$ is evenly-balanced if and only if*

$$\sum_{(\psi,i,j)} n_\psi \left(\widetilde{f}(a\phi_{ij}^\psi) * \overline{\left[\widetilde{f}(\phi_{ij}^\psi)\right]}^{(-)} \right) = \frac{|G|^2}{|H|}\zeta_1,$$

where ζ_1 is the principal irreducible character of H.

Proof Since $\phi_{ij}^{\psi} = \sum_{s\in G} \phi_{ij}^{\psi}(s)\mathbf{1}_s$, and $\overline{(\mathbf{1}_{f(s)})}^{(-)} = \mathbf{1}_{f(s)^{-1}}$, we see that

$$\widetilde{f}(\phi_{ij}^{\psi}) = \sum_{s\in G} \phi_{ij}^{\psi}(s)\mathbf{1}_{f(s)} \quad \text{and} \quad \overline{\left[\widetilde{f}(\phi_{ij}^{\psi})\right]}^{(-)} = \sum_{s\in G} \overline{\phi_{ij}^{\psi}(s)}\mathbf{1}_{f(s)^{-1}}, \quad \text{for any } \phi_{ij}^{\psi} \in \widehat{G}.$$

Furthermore, it follows from $a\phi_{ij}^{\psi} = \sum_{k=1}^{n_\psi} \phi_{ik}^{\psi}(a^{-1})\phi_{kj}^{\psi}$ that

$$\widetilde{f}(a\phi_{ij}^{\psi}) = \sum_{k=1}^{n_\psi} \phi_{ik}^{\psi}(a^{-1})\widetilde{f}(\phi_{kj}^{\psi}) = \sum_{k=1}^{n_\psi}\sum_{t\in G} \phi_{ik}^{\psi}(a^{-1})\phi_{kj}^{\psi}(t)\mathbf{1}_{f(t)}.$$

Since $\mathbf{1}_{f(t)} * \mathbf{1}_{f(s)^{-1}} = \mathbf{1}_{f(t)f(s)^{-1}}$, Lemma 2.2(iii, iv) yields that

$$\begin{aligned}\sum_{j=1}^{n_\psi}\left(\widetilde{f}(a\phi_{ij}^{\psi}) * \overline{\left[\widetilde{f}(\phi_{ij}^{\psi})\right]}^{(-)}\right) &= \sum_{s,t\in G}\sum_{j,k=1}^{n_\psi} \phi_{ik}^{\psi}(a^{-1})\phi_{kj}^{\psi}(t)\overline{\phi_{ij}^{\psi}(s)}\left(\mathbf{1}_{f(t)} * \mathbf{1}_{f(s)^{-1}}\right)\\ &= \sum_{s,t\in G} \phi_{ii}^{\psi}(a^{-1}ts^{-1})\mathbf{1}_{f(t)f(s)^{-1}}\\ &= \sum_{b,s\in G} \phi_{ii}^{\psi}(a^{-1}b)\mathbf{1}_{f(bs)f(s)^{-1}}. \quad (\text{where } b = ts^{-1})\end{aligned}$$

That is,

$$\sum_{j=1}^{n_\psi}\left(\widetilde{f}(a\phi_{ij}^{\psi}) * \overline{\left[\widetilde{f}(\phi_{ij}^{\psi})\right]}^{(-)}\right) = \sum_{b,s\in G} \phi_{ii}^{\psi}(a^{-1}b)\mathbf{1}_{f(bs)f(s)^{-1}}. \tag{4.2}$$

Therefore,

$$\begin{aligned}\sum_{(\psi,i,j)} n_\psi\left(\widetilde{f}(a\phi_{ij}^{\psi}) * \overline{\left[\widetilde{f}(\phi_{ij}^{\psi})\right]}^{(-)}\right) &= \sum_{b,s\in G}\sum_{(\psi,i)} n_\psi\phi_{ii}^{\psi}(a^{-1}b)\mathbf{1}_{f(bs)f(s)^{-1}}\\ &= |G|\sum_{s\in G}\mathbf{1}_{f(as)f(s)^{-1}}.\end{aligned}$$

Hence, the lemma holds by Lemma 4.4. □

Now we are ready to prove Theorem 4.3.

Proof of Theorem 4.3 The equivalence of (i) and (ii) follows directly from Lemma 4.5. In the following we prove that (ii) implies (iii) and that (iii) implies (i).

Assume (ii). Then

$$\begin{aligned}&\sum_{(\psi,i,j),\psi\notin N^\perp} n_\psi\left(\widetilde{f}(a\phi_{ij}^{\psi}) * \overline{\left[\widetilde{f}(\phi_{ij}^{\psi})\right]}^{(-)}\right)\\ &= \sum_{(\psi,i,j)} n_\psi\left(\widetilde{f}(a\phi_{ij}^{\psi}) * \overline{\left[\widetilde{f}(\phi_{ij}^{\psi})\right]}^{(-)}\right) - \sum_{(\psi,i,j),\psi\in N^\perp} n_\psi\left(\widetilde{f}(a\phi_{ij}^{\psi}) * \overline{\left[\widetilde{f}(\phi_{ij}^{\psi})\right]}^{(-)}\right)\\ &= \frac{|G|^2}{|H|}\zeta_1 - \sum_{b,s\in G}\sum_{(\psi,i),\psi\in N^\perp} n_\psi\phi_{ii}^{\psi}(a^{-1}b)\mathbf{1}_{f(bs)f(s)^{-1}} \quad (\text{by (ii) and (4.2)})\\ &= \frac{|G|^2}{|H|}\zeta_1 - |G/N|\sum_{b\in N}\sum_{s\in G}\mathbf{1}_{f(bs)f(s)^{-1}}, \quad (\text{by (3.5)})\end{aligned}$$

Since (i) and (ii) are equivalent, i.e. $D_b f : G \to H$ is evenly-balanced for any $b \in N\backslash\{1_G\}$, by Lemma 4.4 we see that

$$\sum_{b\in N}\sum_{s\in G}\mathbf{1}_{f(bs)f(s)^{-1}} = \frac{|G|}{|H|}\rho_H + (|N|-1)\frac{|G|}{|H|}\zeta_1.$$

Thus, (iii) holds.

Now assume (iii). Note that

$$\begin{aligned}
&\sum_{(\psi,i,j),\psi\notin N^\perp} n_\psi\left(\widetilde{f}(a\phi_{ij}^{\psi}) * \overline{\left[\widetilde{f}(\phi_{ij}^{\psi})\right]}^{(-)}\right)\\
&= \sum_{b,s\in G}\sum_{(\psi,i),\psi\notin N^\perp} n_\psi \phi_{ii}^{\psi}(a^{-1}b)\mathbf{1}_{f(bs)f(s)^{-1}} \quad \text{(by (4.2))}\\
&= (|G|-|G/N|)\sum_{s\in G}\mathbf{1}_{f(as)f(s)^{-1}} - |G/N|\sum_{b\in N\backslash\{a\}}\sum_{s\in G}\mathbf{1}_{f(bs)f(s)^{-1}}, \quad \text{(by (3.6))}\\
&= |G|\sum_{s\in G}\mathbf{1}_{f(as)f(s)^{-1}} - |G/N|\sum_{b\in N}\sum_{s\in G}\mathbf{1}_{f(bs)f(s)^{-1}}.
\end{aligned}$$

So (iii) implies that for any $a \in N\backslash\{1_G\}$,

$$|G|\sum_{s\in G}\mathbf{1}_{f(as)f(s)^{-1}} - |G/N|\sum_{\substack{b\in N\\ b\neq 1_G}}\sum_{s\in G}\mathbf{1}_{f(bs)f(s)^{-1}} = \frac{|G|^2}{|N|\cdot|H|}\zeta_1. \tag{4.3}$$

The above equality implies that $\sum_{s\in G}\mathbf{1}_{f(as)f(s)^{-1}}$ are equal for all $a \in N\backslash\{1_G\}$, and hence

$$\big(|G|-|G/N|(|N|-1)\big)\sum_{s\in G}\mathbf{1}_{f(as)f(s)^{-1}} = \frac{|G|^2}{|N|\cdot|H|}\zeta_1, \quad \text{for any } a\in N\backslash\{1_G\}.$$

Hence,

$$\sum_{s\in G}\mathbf{1}_{f(as)f(s)^{-1}} = \frac{|G|}{|H|}\zeta_1, \quad \text{for any } a\in N\backslash\{1_G\}.$$

Thus, $D_a f$ is evenly-balanced for any $a \in N\backslash\{1_G\}$ by Lemma 4.4, and (i) holds. □

For each $\zeta \in \mathrm{Irr}(H)$, let us fix a unitary irreducible representation $\Lambda_\zeta := \big(\lambda_{ij}^{\zeta}\big)_{i,j}$ of H. Let $\widehat{H} := \{\lambda_{ij}^{\zeta} : \zeta \in \mathrm{Irr}(H), 1 \le i,j \le n_\zeta\}$ be a dual basis of H, and let $\mathrm{Irr}(H)^\sharp := \mathrm{Irr}(H)\backslash\{\zeta_1\}$, where ζ_1 is the principal irreducible character of H. For any function $f : G \to H$ and any $\lambda_{ij}^{\zeta} \in \widehat{H}$, we define a function f_{ij}^{ζ} on G as follows:

$$f_{ij}^{\zeta} : G \to \mathbb{C}, \quad a \mapsto \sum_{s\in G}\big(\lambda_{ij}^{\zeta}\circ D_a f\big)(s).$$

f_{ij}^{ζ} is called an *autocorrelation* function of f in [19].

Lemma 4.6 *Let G, H be finite groups, and $f : G \to H$ a function. Then for any $\zeta \in \mathrm{Irr}(H)$,*

$$f_{ij}^{\zeta} = \sum_{k=1}^{n_\zeta}\big[(\lambda_{ik}^{\zeta}\circ f)\circledast(\lambda_{jk}^{\zeta}\circ f)\big].$$

Proof For any $a \in G$, Lemma 2.2(iii, iv) implies that

$$f_{ij}^{\zeta}(a) = \sum_{s\in G} \lambda_{ij}^{\zeta}\big(f(as)f(s)^{-1}\big) = \sum_{k=1}^{n_\zeta}\sum_{s\in G} \lambda_{ik}^{\zeta}(f(as))\overline{\lambda_{jk}(f(s))}$$
$$= \sum_{k=1}^{n_\zeta}\big[(\lambda_{ik}^{\zeta}\circ f)\circledast(\lambda_{jk}^{\zeta}\circ f)\big](a).$$

So the lemma holds. □

The next theorem characterizes a perfect nonlinear function $f : G \to H$ in terms of f_{ij}^{ζ}. Let δ_{ij} be the Kronecker delta.

Theorem 4.7 *Let G, H be finite groups, and $f : G \to H$ a function. Then the following are equivalent.*

(i) f is a perfect nonlinear function.
(ii) For any $\zeta \in \mathrm{Irr}(H)^\sharp$, $f_{ij}^{\zeta} = \delta_{ij}\rho$, where ρ is the regular character of G.
(iii) For any $\zeta \in \mathrm{Irr}(H)^\sharp$,

$$\sum_{k=1}^{n_\zeta} M\big(\lambda_{ik}^{\zeta}\circ f\big)_\psi\Big[M\big(\lambda_{jk}^{\zeta}\circ f\big)_\psi\Big]^* = \delta_{ij}\frac{n_\psi^2}{|G|}I_{n_\psi}, \quad \text{for any } \psi \in \mathrm{Irr}(G).$$

Proof Let $g : G \to H$ be a function. Then by (4.1), g is evenly-balanced if and only if $\sum_{s\in G} g(s) = (|G|/|H|)\sum_{h\in H} h$. Hence by Corollary 2.12(ii), g is evenly-balanced if and only if for any $\zeta \in \mathrm{Irr}(H)^\sharp$, the function $\lambda_{ij}^{\zeta}\circ g : G \to \mathbb{C}$ is balanced. Therefore,

$$f \text{ is perfect nonlinear} \Leftrightarrow \lambda_{ij}^{\zeta}\circ D_a f \text{ is balanced, for any } a \in G\backslash\{1_G\} \text{ and } \zeta \in \mathrm{Irr}(H)^\sharp,$$
$$\Leftrightarrow f_{ij}^{\zeta}(a) = 0, \quad \text{for any } a \in G\backslash\{1_G\} \text{ and } \zeta \in \mathrm{Irr}(H)^\sharp.$$

But for any $\zeta \in \mathrm{Irr}(H)^\sharp$,

$$f_{ij}^{\zeta}(1_G) = \sum_{s\in G}\lambda_{ij}^{\zeta}\big(f(s)f(s)^{-1}\big) = |G|\lambda_{ij}^{\zeta}(1_H) = \delta_{ij}|G|.$$

So f is perfect nonlinear if and only if $f_{ij}^{\zeta} = \delta_{ij}\rho$, for any $\zeta \in \mathrm{Irr}(H)^\sharp$, and the equivalence of (i) and (ii) holds.

For any $\zeta \in \mathrm{Irr}(H)$, $f_{ij}^{\zeta} = \sum_{k=1}^{n_\zeta}\big[(\lambda_{ik}^{\zeta}\circ f)\circledast(\lambda_{jk}^{\zeta}\circ f)\big]$ by Lemma 4.6. Therefore, for any $\psi \in \mathrm{Irr}(G)$, Lemma 3.7(i) implies that

$$M(f_{ij}^{\zeta})_\psi = \frac{|G|}{n_\psi}\sum_{k=1}^{n_\zeta} M\big(\lambda_{ik}^{\zeta}\circ f\big)_\psi\Big[M\big(\lambda_{jk}^{\zeta}\circ f\big)_\psi\Big]^*.$$

Note that $f_{ij}^{\zeta} = \delta_{ij}\rho$ if and only if $M(f_{ij}^{\zeta})_\psi = \delta_{ij}n_\psi I_{n_\psi}$, for any $\psi \in \mathrm{Irr}(G)$. So the equivalence of (ii) and (iii) holds. □

Since $f_{ij}^{\zeta} = \delta_{ij}\rho$ if and only if $\overline{f_{ij}^{\zeta}} = \delta_{ij}\rho$, as a direct consequence of Theorem 4.7 and (3.2), we have the following corollary. Our approach also provides a conceptual proof of Corollary 4.8.

Corollary 4.8 (Cf. [19, Theorem 4]) *Let G, H be finite groups, and $f : G \to H$ a function. Then f is perfect nonlinear if and only if for any $\psi \in \mathrm{Irr}(G)$,*

$$\sum_{k=1}^{n_\zeta} \widehat{\left(\lambda_{ik}^{\zeta} \circ f\right)}(\Phi_\psi) \left[\widehat{\left(\lambda_{jk}^{\zeta} \circ f\right)}(\Phi_\psi)\right]^* = \delta_{ij}|G|I_{n_\psi}, \quad \text{for any } \zeta \in \mathrm{Irr}(H)^\sharp.$$

5 Constructions of bent functions

Let N, H be finite groups, and let $\mu : H \to \mathrm{Aut}(N), h \mapsto \mu_h$ be a group homomorphism, where $\mathrm{Aut}(N)$ is the automorphism group of N. Let $N \rtimes_\mu H$ be the semidirect product of N and H with respect to μ. That is, as a set, $N \rtimes_\mu H$ is the Cartesian product $N \times H$, and the multiplication of elements in $N \rtimes_\mu H$ is defined by

$$(a_1, h_1) * (a_2, h_2) := (a_1\mu_{h_1}(a_2), h_1h_2), \quad \text{for any } (a_1, h_1), (a_2, h_2) \in N \rtimes_\mu H.$$

Note that the identity element of $N \rtimes_\mu H$ is $(1_N, 1_H)$. Recall that T is the unit circle in the complex numbers.

Proposition 5.1 *With the notation in the above paragraph, let $f : N \to T$ and $g : H \to T$ be bent functions. Then the following hold.*

(i) $f \times g : N \rtimes_\mu H \to T, (a, h) \mapsto f(a)g(h)$ is a bent function.
(ii) $f \times_\mu g : N \rtimes_\mu H \to T, (a, h) \mapsto f\big(\mu_{h^{-1}}(a)\big)g(h)$ is a bent function.

Proof (i) Let $(a, h) \in N \rtimes_\mu H \backslash \{(1_N, 1_H)\}$. Then

$$\begin{aligned}
&\sum_{(b,k)\in N\rtimes_\mu H} (f \times g)\big((a, h) * (b, k)\big)\overline{(f \times g)\big((b, k)\big)} \\
&= \sum_{(b,k)\in N\rtimes_\mu H} f(a\mu_h(b))g(hk)\overline{f(b)g(k)} \\
&= \sum_{b\in N} f(a\mu_h(b))\overline{f(b)} \sum_{k\in H} g(hk)\overline{g(k)}.
\end{aligned}$$

If $h \neq 1_H$, then $\sum_{k\in H} g(hk)\overline{g(k)} = 0$ (because g is bent). If $h = 1_H$, then μ_h is the identity map on N, and $a \neq 1_N$. Thus, $\sum_{b\in N} f(a\mu_h(b))\overline{f(b)} = \sum_{b\in N} f(ab)\overline{f(b)} = 0$. So (i) holds.

(ii) Let $(a, h) \in N \rtimes_\mu H \backslash \{(1_N, 1_H)\}$. Then

$$\begin{aligned}
&\sum_{(b,k)\in N\rtimes_\mu H} (f \times_\mu g)\big((a, h) * (b, k)\big)\overline{(f \times_\mu g)\big((b, k)\big)} \\
&= \sum_{(b,k)\in N\rtimes_\mu H} f\big(\mu_{(hk)^{-1}}(a\mu_h(b))\big)g(hk)\overline{f\big(\mu_{k^{-1}}(b)\big)}\,\overline{g(k)} \\
&= \sum_{k\in H}\sum_{b\in N} f\big(\mu_{k^{-1}h^{-1}}(a)\mu_{k^{-1}}(b)\big)\overline{f\big(\mu_{k^{-1}}(b)\big)}g(hk)\overline{g(k)}. \quad \text{(because } \mu_{(hk)^{-1}}\mu_h = \mu_{k^{-1}}\text{)}
\end{aligned}$$

If $a \neq 1_N$, then $\mu_{k^{-1}h^{-1}}(a) \neq 1_N$, and hence f a bent function implies that

$$\sum_{b\in N} f\big(\mu_{k^{-1}h^{-1}}(a)\mu_{k^{-1}}(b)\big)\overline{f\big(\mu_{k^{-1}}(b)\big)} = \sum_{b'\in N} f\big(\mu_{k^{-1}h^{-1}}(a)b'\big)\overline{f(b')} = 0,$$

for all $k \in H$, where $b' = \mu_{k^{-1}}(b)$.

If $a = 1_N$, then $h \neq 1_H$, and $f\big(\mu_{k^{-1}h^{-1}}(a)\mu_{k^{-1}}(b)\big)\overline{f\big(\mu_{k^{-1}}(b)\big)} = 1$ for all $b \in N$. Hence,

$$\sum_{k\in H}\sum_{b\in N} f\big(\mu_{k^{-1}h^{-1}}(a)\mu_{k^{-1}}(b)\big)\overline{f\big(\mu_{k^{-1}}(b)\big)}g(hk)\overline{g(k)} = |N|\sum_{k\in H} g(hk)\overline{g(k)} = 0.$$

So (ii) holds. □

If the homomorphism $\mu : H \to \mathrm{Aut}(N)$ is trivial, i.e. μ_h is the identity map on N for any $h \in H$, then the semidirect product $N \rtimes_\mu H$ is the direct product of N and H. So Proposition 5.1(i) is also true for direct products of finite groups.

Note that many nonabelian finite groups are (isomorphic to) semidirect products of finite abelian groups. So we can obtain bent functions on many nonabelian finite groups by applying Proposition 5.1. Also the same nonabelian finite group can be the semidirect products of different (non-isomorphic) finite (abelian) groups. So by Proposition 5.1, we can construct different bent functions on the same group.

Similarly for perfect nonlinear functions, we have the following result.

Proposition 5.2 *With the notation in the paragraph before Proposition 5.1, let Q be a finite group, and let $f : N \to Q$ and $g : H \to Q$ be perfect nonlinear functions. Then the following hold.*

(i) $f \times g : N \rtimes_\mu H \to Q, (a, h) \mapsto f(a)g(h)$ is a perfect nonlinear function.
(ii) $f \times_\mu g : N \rtimes_\mu H \to Q, (a, h) \mapsto f\big(\mu_{h^{-1}}(a)\big)g(h)$ is a perfect nonlinear function.

Proof (i) Let $(a, h) \in N \rtimes_\mu H \backslash \{(1_N, 1_H)\}$. Then

$$\sum_{(b,k)\in N\rtimes_\mu H} (f \times g)\big((a, h) * (b, k)\big)\big[(f \times g)\big((b, k)\big)\big]^{-1}$$
$$= \sum_{b\in N}\left[f(a\mu_h(b))\Big(\sum_{k\in H} g(hk)g(k)^{-1}\Big)f(b)^{-1}\right].$$

If $h \neq 1_H$, then $\sum_{k\in H} g(hk)g(k)^{-1} = \frac{|H|}{|Q|}\sum_{x\in Q} x$ (because g is perfect nonlinear). Hence,

$$f(a\mu_h(b))\Big(\sum_{k\in H} g(hk)g(k)^{-1}\Big)f(b)^{-1} = \frac{|H|}{|Q|}\sum_{x\in Q} x, \quad \text{for any } b \in N.$$

Therefore,

$$\sum_{(b,k)\in N\rtimes_\mu H} (f \times g)\big((a, h) * (b, k)\big)\big[(f \times g)\big((b, k)\big)\big]^{-1} = \frac{|N|\cdot|H|}{|Q|}\sum_{x\in Q} x. \tag{5.1}$$

If $h = 1_H$, then μ_h is the identity map on N, and $a \neq 1_N$. Thus, $\sum_{b\in N} f(a\mu_h(b))f(b)^{-1} = \sum_{b\in N} f(ab)f(b)^{-1} = \frac{|N|}{|Q|}\sum_{x\in Q} x$, and (5.1) is also true. So (i) holds.

The proof of (ii) is similar. □

With the assumption in Proposition 5.2, it follows from [21, Theorem 1] that the set $R_f := \{(a, f(a)) : a \in N\} \subset N \times Q$ is a semiregular $(|N|, |Q|, |N|, |N|/|Q|)$ relative difference set in $N \times Q$ relative to $\{1_N\} \times Q$, and $R_g := \{(h, g(h)) : h \in H\} \subset H \times Q$ is a semiregular $(|H|, |Q|, |H|, |H|/|Q|)$ relative difference set in $H \times Q$ relative to $\{1_H\} \times Q$. From Proposition 5.2(i),

$$R_{f\times g} := \{\big((a, h), (f \times g)(a, h)\big) : (a, h) \in N \rtimes_\mu H\} \subset (N \rtimes_\mu H) \times Q$$

is a semiregular $(|N \rtimes_\mu H|, |Q|, |N \rtimes_\mu H|, |N \rtimes_\mu H|/|Q|)$ relative difference set in $(N \rtimes_\mu H) \times Q$ relative to $\{(1_N, 1_H)\} \times Q$. Let $G_1 := N \times Q, G_2 := H \times Q$, and $G := (N \rtimes_\mu H) \times Q$. Then we can regard G as $G_1 G_2$, and $R_{f \times g}$ as $R_f R_g$. So Proposition 5.2(i) also follows from [10, Theorem 4].

Let G be a finite group. Let N be a normal subgroup of G, $\{b_i : 1 \le i \le m\}$ a complete set of representatives of (left) cosets of N in G, and $\varepsilon : \{b_i : 1 \le i \le m\} \to T$ a function. Furthermore, let $\theta = (\theta_1, \ldots, \theta_m)$ and $\pi = (\pi_1, \ldots, \pi_m)$, where $\theta_i, 1 \le i \le m$, are automorphisms (not necessarily all distinct) of N, and $\pi_i : N \to T, 1 \le i \le m$, are group homomorphisms (not necessarily all distinct). The existence of θ_i and π_i is clear. For example, θ_i can be the map

$$\theta_i : N \to N, \quad x \mapsto b_i^{-1} x b_i,$$

and π_i can be any linear irreducible character of N.

Proposition 5.3 *With the notation in the above paragraph, let $f : N \to T$ be a bent function on N. Let*

$$f_{\varepsilon,\pi,\theta} : G \to T, \quad b_i x \mapsto \varepsilon(b_i)\pi_i(x) f(\theta_i(x)), \qquad \text{for any } x \in N, 1 \le i \le m.$$

Then for any $a \in N \backslash \{1_G\}$, $d_a(f_{\varepsilon,\pi,\theta})$ is balanced on G.

Proof Let $a \in N \backslash \{1_G\}$. Then for any $x \in N$, $ab_i x = b_i(b_i^{-1} a b_i x) \in b_i N$ for all b_i. Hence,

$$\begin{aligned}
\sum_{y \in G} d_a(f_{\varepsilon,\pi,\theta})(y) &= \sum_{i=1}^{m} \sum_{x \in N} f_{\varepsilon,\pi,\theta}(ab_i x)\overline{f_{\varepsilon,\pi,\theta}(b_i x)} \\
&= \sum_{i=1}^{m} \sum_{x \in N} \varepsilon(b_i)\pi_i(b_i^{-1} a b_i x) f(\theta_i(b_i^{-1} a b_i x))\overline{\varepsilon(b_i)\pi_i(x) f(\theta_i(x))} \\
&= \sum_{i=1}^{m} \sum_{x \in N} \pi_i(b_i^{-1} a b_i) f(\theta_i(b_i^{-1} a b_i)\theta_i(x))\overline{f(\theta_i(x))}.
\end{aligned}$$

Since f is a bent function on $N, \theta_i \in \mathrm{Aut}(N)$, and $a \ne 1_G$, we see that $\theta_i(b_i^{-1} a b_i) \in N \backslash \{1_G\}$, and hence

$$\sum_{x \in N} f(\theta_i(b_i^{-1} a b_i)\theta_i(x))\overline{f(\theta_i(x))} = 0, 1 \le i \le m.$$

So the proposition holds. □

For perfect nonlinear functions, we have the following result.

Proposition 5.4 *With the notation in the paragraph before Proposition 5.3, let H be a finite group, and $f : N \to H$ a perfect nonlinear function. Let*

$$f_\theta : G \to H, \quad b_i x \mapsto f(\theta_i(x)), \qquad \text{for any } x \in N, 1 \le i \le m.$$

Then for any $a \in N \backslash \{1_G\}$, $D_a(f_\theta) : G \to H$ is evenly-balanced.

Proof Let $a \in N\backslash\{1_G\}$. Then for any $x \in N$, $ab_i x = b_i(b_i^{-1}ab_i x) \in b_i N$ for all b_i. Hence,

$$\begin{aligned}\sum_{y\in G} D_a(f_\theta)(y) &= \sum_{i=1}^{m}\sum_{x\in N} f_\theta(ab_i x) f_\theta(b_i x)^{-1}\\ &= \sum_{i=1}^{m}\sum_{x\in N} f(\theta_i(b_i^{-1}ab_i x)) f(\theta_i(x))^{-1}\\ &= \sum_{i=1}^{m}\sum_{x\in N} f(\theta_i(b_i^{-1}ab_i)\theta_i(x)) f(\theta_i(x))^{-1}.\end{aligned}$$

Since f is perfect nonlinear on N, $\theta_i \in \mathrm{Aut}(N)$, and $a \neq 1_G$, we see that $\theta_i(b_i^{-1}ab_i) \in N\backslash\{1_G\}$, and hence

$$\sum_{x\in N} f(\theta_i(b_i^{-1}ab_i)\theta_i(x)) f(\theta_i(x))^{-1} = \frac{|N|}{|H|}\sum_{z\in H} z,\ 1 \le i \le m.$$

So the proposition holds. □

Davis and Poinset [7] studied perfect nonlinear functions and difference sets on group actions (called *G-perfect nonlinear functions* and *G-difference sets*, respectively). Similar to [7, Theorem 3.3] (also see [9, Corollary 2.11]), we have the next result.

Proposition 5.5 *Let G be an arbitrary finite group, and $H := \{0, 1\}$ an additive group of order 2. Let $f : G \to H$ be a function, and $S_i := f^{-1}(i)$, $i = 0, 1$. Then f is perfect nonlinear if and only if 4 divides $|G|$ and S_0 is a $(|G|, |S_0|, |S_0| - |G|/4)$ difference set in G.*

The above proposition can be obtained as a consequence of [7, Theorem 3.3] (or [9, Corollary 2.11]). Here we include a proof for the convenience of the reader. For a nonempty subset C of G, let $C^+ := \sum_{s\in C} s$ and $C^{(-)} := \sum_{s\in C} s^{-1}$. For any $\sum_{s\in G}\gamma_s s$ in the group algebra $\mathbb{C}G$, let $\left(\sum_{s\in G}\gamma_s s\right)^{(-)} := \sum_{s\in G}\gamma_s s^{-1}$.

Proof of Proposition 5.5 By [26, Theorem 1.3], f is perfect nonlinear if and only if $\{S_0, S_1\}$ is a (G, H)-related difference family, i.e. $S_0^+ S_1^{(-)} + S_1^+ S_0^{(-)} = \frac{|G|}{|H|}\left(G\backslash\{1_G\}\right)^+$. Since $S_0 \cap S_1 = \emptyset$ and $S_0 \cup S_1 = G$, we see that $S_0^+ S_1^{(-)} = S_0^+\left(G^+ - S_0^{(-)}\right) = |S_0|G^+ - S_0^+ S_0^{(-)}$, and $S_1^+ S_0^{(-)} = \left(S_0^+ S_1^{(-)}\right)^{(-)} = S_0^+ S_1^{(-)}$. Thus,

$$\begin{aligned}f \text{ is perfect nonlinear} &\Leftrightarrow |S_0|G^+ - S_0^+ S_0^{(-)} = \frac{|G|}{4}\left(G^+ - 1_G\right)\\ &\Leftrightarrow S_0^+ S_0^{(-)} = |S_0|\cdot 1_G + \left(|S_0| - \frac{|G|}{4}\right)(G^+ - 1_G).\end{aligned}$$

Hence, the proposition holds. □

Acknowledgements The authors would like to thank the referees; their useful comments have improved the paper.

References

1. Alperin J.L., Bell R.B.: Groups and Representations, GTM 162. Springer, New York (1997).
2. Arasu K.T., Ding C., Helleseth T., Kumar P.V., Martinsen H.: Almost difference sets and their sequences with optimal autocorrelations. IEEE Trans. Inform. Theory **47**(7), 2934–2943 (2001).

3. Beth T., Jungnickel D., Lenz H.: Design Theory, 2nd edn. Cambridge University Press, Cambridge (1999).
4. Carlet C., Ding C.: Highly nonlinear mappings. J. Complex. **20**, 205–244 (2004).
5. Chung H., Kumar P.V.: A new general construction of generalized bent functions. IEEE Trans. Inform. Theory **35**, 206–209 (1989).
6. Dillon J.F.: Elementary Hadamard Difference Sets. Ph.D. Thesis, University of Maryland (1974).
7. Davis J.A., Poinsot L.: G-perfect nonlinear functions. Des. Codes Cryptogr. **46**, 83–96 (2008).
8. Fan Y., Xu B.: Fourier transforms and bent functions on faithful actions of finite abelian groups. Des. Codes Cryptogr. **82**, 543–558 (2017).
9. Fan Y., Xu B.: Nonlinear functions and difference sets on group actions. Des. Codes Cryptogr. **85**, 319–341 (2017).
10. Galati J.C., LeBel A.C.: Relative difference sets in semidirect products with an amalgamated subgroup. J. Comb. Des. **13**, 211–221 (2005).
11. Huppert B.: Character Theory of Finite Groups. Walter de Gruyter & Co., Berlin (1998).
12. Isaacs M.: Character Theory of Finite Groups, vol. 69. Pure and Applied MathematicsAcademic Press Inc., New York (1976).
13. Kumar P.V., Scholtz R.A., Welch L.R.: Generalized bent functions and their properties. J. Comb. Theory Ser. A **40**, 90–107 (1985).
14. Lai X., Massey J.L.: A proposal for a new block encryption standard. In: Advances in Cryptology-Eurocrypt'90. Lecture Notes in Computer Science, Vol. 473, pp. 389–404. Springer (1991).
15. Logachev O.A., Salnikov A.A., Yashchenko V.V.: Bent functions over a finite abelian group. Discret. Math. Appl. **7**, 547–564 (1997).
16. Nagao H., Tsushima Y.: Representations of Finite Groups. Academic Press Inc., Boston (1989).
17. Poinsot L., Harari S.: Group actions based perfect nonlinearity. GESTS Int. Trans. Comput. Sci. Eng. **12**, 1–14 (2005).
18. Poinsot L.: Bent functions on a finite nonabelian group. J. Discret. Math. Sci. Cryptogr. **9**, 349–364 (2006).
19. Poinsot L.: Non abelian bent functions. Cryptogr. Commun. **4**, 1–23 (2012).
20. Poinsot L., Pott A.: Non-Boolean almost perfect nonlinear functions on non-abelian groups. Int. J. Found. Comput. Sci. **22**, 1351–1367 (2011).
21. 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).
22. Rothaus O.S.: On bent functions. J. Comb. Theory Ser. A **20**, 300–305 (1976).
23. Shorin V.V., Jelezniakov V.V., Gabidulin E.M.: Linear and differential cryptanalysis of Russian GOST. In: Augot D., Carlet C. (eds.) Workshop on Coding and Cryptography, pp. 467–476 (2001).
24. Solodovnikov V.I.: Bent functions from a finite abelian group to a finite abelian group. Diskret. Mat. **14**, 99–113 (2002).
25. Tokareva N.: Generalizations of bent functions: a survey of publications. J. Appl. Ind. Math. **5**, 110–129 (2011).
26. Xu B.: Multidimensional Fourier transforms and nonlinear functions on finite groups. Linear Algebr. Appl. **452**, 89–105 (2014).
27. Xu B.: Bentness and nonlinearity of functions on finite groups. Des. Codes Cryptogr. **76**, 409–430 (2015).
28. Xu B.: Dual bent functions on finite groups and C-algebras. J. Pure Appl. Algebr. **220**, 1055–1073 (2016).