Designs, Codes and Cryptography (2020) 88:755–770
https://doi.org/10.1007/s10623-019-00708-8

New nonexistence results on (m, n)-generalized bent functions

Ka Hin Leung[1] **· Qi Wang**[2]

Received: 3 August 2019 / Revised: 10 December 2019 / Accepted: 12 December 2019 /
Published online: 2 January 2020

Abstract
In this paper, we present some new nonexistence results on (m, n)-generalized bent functions, which improved recent results. More precisely, we derive new nonexistence results for general n and m odd or $m \equiv 2 \pmod 4$, and further explicitly prove nonexistence of $(m, 3)$-generalized bent functions for all integers m odd or $m \equiv 2 \pmod 4$. The main tools we utilized are certain exponents of minimal vanishing sums from applying characters to group ring equations that characterize (m, n)-generalized bent functions.

Keywords Exponent · Generalized bent function · Minimal relation · Nonexistence · Vanishing sum

Mathematics Subject Classification 11A07 · 16S34 · 05B10 · 94A15

1 Introduction

Let $m \geq 2$, n be positive integers, and $\zeta_m = e^{\frac{2\pi\sqrt{-1}}{m}}$ be a primitive complex m-th root of unity. A function $f : \mathbb{Z}_2^n \to \mathbb{Z}_m$ is called an (m, n)-*generalized bent function* (GBF) if

$$|F(y)|^2 = 2^n \tag{1}$$

Communicated by G. Kyureghyan.

K.H. Leung's research was supported by Grant R-146-000-158-112, Ministry of Education, Singapore. Q. Wang's research was supported by the National Natural Science Foundation of China under Grant 61672015.

✉ Qi Wang
wangqi@sustech.edu.cn

Ka Hin Leung
mathlkh@nus.edu.cn

1 Department of Mathematics, National University of Singapore, Kent Ridge, Singapore 119260, Republic of Singapore

2 Department of Computer Science and Engineering , Southern University of Science and Technology, Xili Nanshan District, Shenzhen 518055, Guangdong, China

for all $y \in \mathbb{Z}_2^n$, where $F(y)$ is defined as

$$F(y) := \sum_{x \in \mathbb{Z}_2^n} \zeta_m^{f(x)} (-1)^{y \cdot x}, \tag{2}$$

and $y \cdot x$ denotes the usual inner product. In particular, when $m = 2$, the generalized bent functions defined above are simply Boolean bent functions introduced by Rothaus [10], whereas the function $F : \mathbb{Z}_2^n \to \mathbb{R}$ in fact becomes the Fourier transform of the Boolean function f. In 1985, Kumar et al. [3] generalized the notion of Boolean bent function by considering bent functions from $\mathbb{Z}_m^n$ to $\mathbb{Z}_m$. For recent nonexistence results on such generalized bent functions, see Leung and Schmidt [6]. Schmidt [12] investigated generalized bent functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_m$ for their applications in CDMA communications. For the Boolean case, it is well known that bent function exists if and only if n is even, and many constructions were reported (for a survey see [1]). In the literature, there exist constructions of generalized bent function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_m$ for $m = 4, 8, 2^k$ (for example, see [9,11–14]). Very recently, Liu et al. [7] presented several nonexistence results on generalized bent functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_m$. In this paper, we continue to investigate the nonexistence of such generalized bent functions, and present more new nonexistence results. If m and n are both even or m is divisible by 4, then there exists an (m, n)-generalized bent function [7]. Therefore, we restrict attention to the following two cases:

(i) m is odd;
(ii) n is odd and $m \equiv 2 \pmod 4$.

In the following, we always assume that m is odd or $m = 2m'$ with m' odd.

The remainder of this paper is organized as follows. In Sect. 2, we introduce some basic tools and auxiliary results. In Sect. 3, we give several new nonexistence results of (m, n)-generalized bent functions, which improve the recent results in [7]. Furthermore, we show that no $(m, 3)$-GBF exists for all m odd or $m \equiv 2 \pmod 4$ in Sect. 4.

2 Basic tools and auxiliary results

In this section, we introduce some basic tools and auxiliary results, which will be used in later sections.

2.1 Group ring and character theory

It turns out that group ring and characters of abelian groups play an important role in the study of GBFs. Let G be a finite group of order v. Suppose that R is a ring, and $R[G]$ denotes the group ring of G over R. For a subset D of a group G, we may identify D with the group ring element $\sum_{g \in G} d_g g \in R[G]$, also denoted by D by abuse of notation, where $d_g \in R$ and these d_g's are called *coefficients* of D. Let 1_G denote the identity element of G and let r be an element in R. For simplicity, we write r for the group ring element $r1_G \in R[G]$. For the group ring element $D = \sum_{g \in G} d_g g \in R[G]$, its *support* is defined as

$$supp(D) := \{g \in G : d_g \neq 0\},$$

and we also define $|D| := \sum d_g$ and $||D|| := \sum |d_g|$ by convention when $R = \mathbb{C}$ or $R = \mathbb{Z}$ or R is the semiring $\mathbb{N}$ as we will use later. Let t be an integer coprime to m. For

$D = \sum_{g\in G} d_g g \in \mathbb{Z}[\zeta_m][G]$, we write $D^{(t)} = \sum d_g^\sigma g^t$, where σ is the automorphism of $\mathbb{Q}[\zeta_m]$ determined by $\zeta_m^\sigma = \zeta_m^t$.

The group ring notation is very useful when applying characters. A *character* χ of an abelian group G is a homomorphism $\chi : G \to \mathbb{C}^*$. The set of all such characters forms a group $\hat{G}$ which is isomorphic to G itself, and the identity element of $\hat{G}$, denoted by χ_0, which maps every element in G to 1 (i.e., $\chi_0(g) = 1$ for all $g \in G$), is called the *principal character* of G. It is clear that the character group has the multiplication in $\hat{G}$ defined by $\chi\tau(g) = \chi(g)\tau(g)$ for $\chi, \tau \in \hat{G}$. For $D = \sum_{g\in G} d_g g \in \mathbb{C}[G]$ and $\chi \in \hat{G}$, we have $\chi(D) = \sum_{g\in G} d_g \chi(g)$. For a subgroup U of the group G, we define a subgroup of $\hat{G}$ as $U^\perp := \{\chi \in \hat{G} : \chi(g) = 1 \text{ for all } g \in U\}$. If $\chi \in U^\perp$, we say that the character χ is *trivial on* U. It is easy to see that $|U^\perp| = |G|/|U|$. The following two results are standard and well-known in character theory.

Fact 1 (Orthogonality relations) *Let G be a finite abelian group of order v with identity 1_G. Then*

$$\sum_{\chi\in\hat{G}} \chi(g) = \begin{cases} 0 & \text{if } g \neq 1_G, \\ v & \text{if } g = 1_G, \end{cases}$$

and

$$\sum_{g\in G} \chi(g) = \begin{cases} 0 & \text{if } \chi \neq \chi_0, \\ v & \text{if } \chi = \chi_0. \end{cases}$$

Fact 2 (Fourier inversion formula) *Let G be a finite abelian group of order v, let $D = \sum_{g\in G} d_g g \in \mathbb{C}[G]$ by abuse of notation and $\chi(D) = \sum_{g\in G} d_g \chi(g)$. Then the coefficients in D are determined by*

$$d_g = \frac{1}{v} \sum_{\chi\in\hat{G}} \chi(Dg^{-1}).$$

2.2 Some auxiliary results

We now characterize (m, n)-generalized bent functions using the group ring equations. Instead of working with additive groups, we use multiplicative notation. We denote the cyclic group of order m by C_m, and set $G = C_2^n$. Whenever $s|m$, we also denote the subgroup of order s in C_m by C_s.

Definition 1 Let $f : G \to \mathbb{Z}_m$ be a function, and g be a generator of C_m. We define an element B_f in the group ring $\mathbb{Z}[\zeta_m][G]$ corresponding to f by

$$B_f := \sum_{x\in G} \zeta_m^{f(x)} x.$$

Furthermore, we define an element D_f in the group ring $\mathbb{Z}[C_m][G]$ by

$$D_f := \sum_{x\in G} g^{f(x)} x.$$

Remark 1 To study (m, n)-GBFs, we may assume that $C_m = \langle\{g^{f(x)} : x \in G\}\rangle$. By scaling if necessary, we may always assume $f(1_G) = 0$, i.e., $g^{f(1_G)} = g^0$ is the identity element of

C_m. From time to time, we may also interpret $\mathbb{Z}[C_m][G]$ as $\mathbb{Z}[C_m \cdot G]$, where g^0 and 1_G in $\mathbb{Z}[C_m \cdot G]$ both denote the identity element of $C_m \cdot G$.

Let τ be a character that maps g to ζ_m, then it is clear that $\tau(D_f) = B_f$. Moreover, every element $y \in G$ determines a character χ_y of G by

$$\chi_y(x) = (-1)^{y \cdot x},$$

for all $x \in G$. It is easily verified that every complex character of G is equal to some χ_y with $y \in G$. Note that

$$\chi_y(B_f) = \sum_{x \in G} \zeta_m^{f(x)} \chi_y(x) = \sum_{x \in G} \zeta_m^{f(x)} (-1)^{y \cdot x} = F(y), \tag{3}$$

for all $y \in G$, where $F(y)$ is defined in (2). This means that $\chi_y(B_f)$ is just the discrete Fourier transform of (m, n)-generalized bent functions. It then follows from (1) and (3) that f is an (m, n)-GBF if and only if

$$|\chi(B_f)|^2 = 2^n, \tag{4}$$

for all $\chi \in \hat{G}$. We now have the following characterization of (m, n)-GBFs.

Proposition 1 *Let f be a function from G to $\mathbb{Z}_m$. Then f is an (m, n)-GBF if and only if*

$$B_f B_f^{(-1)} = 2^n. \tag{5}$$

Furthermore, if $f(G) = 2\mathbb{Z}_m$, then f can be regarded as an (m', n)-GBF, where $m = 2m'$ with m' odd.

Proof From (4) it follows that

$$|\chi(B_f)|^2 = \chi(B_f B_f^{(-1)}) = 2^n,$$

for all characters χ of G. Using Facts 1 and 2 , we are able to determine all the coefficients of $B_f B_f^{(-1)}$, i.e., (4) holds if and only if (5) is satisfied. The last statement follows from the fact that $\zeta_m^{f(x)}$ becomes an m'-th root of unity. □

Observe that we may write

$$D_f D_f^{(-1)} = \sum_{x \in G} \sum_{y \in G} g^{f(y+x)} g^{-f(y)} x = \sum_{x \in G} E_x x, \tag{6}$$

where $E_x = \sum_{y \in G} g^{f(y+x)} g^{-f(y)} \in \mathbb{Z}[C_m]$. In fact, E_x corresponds to the autocorrelation function of bent functions (for more details, see [1]).

Lemma 1 *Suppose that f is a GBF from G to $\mathbb{Z}_m$. Then*

(a) *$E_x = E_x^{(-1)}$ and the coefficient of g^0 in E_x is even for all $x \in G$;*
(b) *For each character τ of order m on C_m, we have $\tau(E_x) = 0$ for all $x \neq 1_G$.*

Proof Note that $(D_f D_f^{(-1)})^{(-1)} = D_f D_f^{(-1)}$. Hence, we have $E_x = E_x^{(-1)}$ for all $x \in G$. Note that $E_{1_G} = 2^n$. Thus, we may consider $x \neq 1_G$. Suppose that $x \neq 1_G$ and $(g_1 x_1)(g_2 x_2)^{-1} = g^0 x$ for some $g_1, g_2 \in C_m$ and $x_1, x_2 \in G$. Note that $x_1 \neq x_2$ and clearly, we have $(g_2 x_2)(g_1 x_1)^{-1} = g^0 x$ as well. This shows that the coefficient of g^0 in E_x is even.

For any character τ of order m on C_m, we obtain

$$\tau(D_f)\tau(D_f)^{(-1)} = B_f B_f^{(-1)} = 2^n = \sum_{x\in G} \tau(E_x)x.$$

From (5) in Proposition 1, the conclusion follows. □

The key in our study of (m, n)-GBFs is to investigate E_x. Lemma 1 (b) allows us to define the notion of vanishing sum (v-sum), which was also studied in details in [4]. Another important notion to study v-sum is the idea of exponents and reduced exponents defined in [5]. In Sect. 3, we will use exponents to derive some new nonexistence results. To this end, we recall some notations defined in [5] and prove some preliminary lemmas.

Let S be a finite index set, and we denote by $\mathcal{P}(k)$ the set of all prime factors of the integer k.

Definition 2 Suppose that $X = \sum_{i\in S} a_i\mu_i$ where μ_i's are distinct roots of unity and all a_i's are nonzero integers. We say that u is the *exponent* of X if u is the smallest positive integer such that $\mu_i^u = 1$ for all i. We say that k is the *reduced exponent* of X if k is the smallest positive integer such that there exists j with $(\mu_i\mu_j^{-1})^k = 1$ for all i.

For example, the exponent of $\sum_{i=0}^{p-1} \zeta_3\zeta_p^i$ is $3p$, whereas the reduced exponent is p. To study vanishing sums, we consider those which are minimal.

Definition 3 Suppose that $X = \sum_{i\in S} a_i\mu_i = 0$ where μ_i's are distinct roots of unity and all a_i's are nonzero integers. We say that the relation $X = 0$ is *minimal*, if for any proper subset $I \subsetneq S$, $\sum_{i\in I} a_i\mu_i \neq 0$.

Based on the definition of minimal relation, we have the following restriction on the cardinality of the index set S, in terms of the reduced exponents of a minimal vanishing sum.

Proposition 2 [2] *Suppose that $X = \sum_{i\in S} a_i\mu_i = 0$ is a minimal relation with reduced exponent k and all a_i's are nonzero. Then k is square free and*

$$|S| \geq 2 + \sum_{p\in\mathcal{P}(k)} (p-2).$$

For convenience, we define the following notation.

Definition 4 For any group H, by $\mathbb{N}[H]$ we denote

$$\left\{\sum_{g\in H} a_g g : a_g \in \mathbb{Z} \text{ and } a_g \geq 0\right\}.$$

Now we consider the corresponding notion of minimal relation in $\mathbb{N}[C_m]$. From now on, we assume that g is a generator of C_m. We recall the notion of minimality defined in Section 4 of [4].

Definition 5 [4] Let $D = \sum_{i=0}^{m-1} a_i g^i \in \mathbb{N}[C_m]$. We say that D is a *v-sum* if there exists a character τ of order m such that $\tau(D) = \tau(\sum_{i=0}^{m-1} a_i g^i) = 0$. We say that D is *minimal* if $\tau(\sum_{i=0}^{m-1} b_i g^i) \neq 0$ whenever $0 \leq b_i \leq a_i$ for all i and $b_j < a_j$ for some j.

Suppose that $S \subseteq \{0, \ldots, m-1\}$ and $a_i > 0$ for all $i \in S$. It is clear that if $D = \sum_{i \in S} a_i g^i$ is a minimal v-sum by Definition 5, then $\tau(D) = \sum_{i \in S} a_i \tau(g)^i$ is a minimal relation by Definition 3. We now define the *reduced exponent* of D as follows.

Definition 6 Suppose that $D = \sum_{i=0}^{m-1} d_i g^i \in \mathbb{N}[C_m]$ is a minimal v-sum. We define the *reduced exponent* k of D as the reduced exponent of the vanishing sum $\tau(D) = \sum_{i=0}^{m-1} d_i \tau(g)^i$.

Note that the reduced exponent defined above does not depend on the choice of the character τ.

Lemma 2 *If $D \in \mathbb{N}[C_m]$ is a minimal v-sum with reduced exponent k, then $D = D'h$ for some $D' \in \mathbb{N}[C_k]$ and $h \in C_m$.*

Proof Write $D = \sum_{i \in S} d_i g^i$ and $\tau(D) = \sum_{i \in S} d_i \tau(g^i)$ where $S \subseteq \{0, \ldots, m-1\}$. Since k is the reduced exponent of D, by Definition 6, the reduced exponent of $\tau(D)$ is also k. Thus, there exists a j such that $(\tau(g^i)\tau(g^{-j}))^k = 1$ for all $i \in S$. It then follows that $Dg^{-j} \in \mathbb{N}[C_k]$. The proof is then completed. □

In view of Proposition 2, we derive the following result.

Corollary 1 *Suppose that $D = \sum_{i=0}^{m-1} a_i g^i \in \mathbb{N}[C_m]$ is a minimal v-sum with reduced exponent k. Then k is square free and*

$$||D|| \geq 2 + \sum_{p \in \mathcal{P}(k)} (p-2).$$

To deal with a v-sum $D \in \mathbb{N}[C_m]$ which is not minimal, we first decompose it into sum of minimal v-sums. It is straightforward to prove the following.

Lemma 3 *Let $D \in \mathbb{N}[C_m]$ be a v-sum. Then D can be written as the form $D = \sum D_i$, where D_i's are minimal v-sums in $\mathbb{N}[C_m]$.*

We aim to find a lower bound of $||D||$ when D is a v-sum. To do so, we need to extend the notion of reduced exponent and then apply Corollary 1. Suppose that $D = \sum_{i=1}^{t} D_i$ and k_i is the reduced exponent of D_i for each i. We may then define the exponent of D to be $\text{lcm}(k_1, \ldots, k_t)$. However, we note that such a decomposition is not necessarily unique. For example, if $m = 10$ and h is a generator of C_{10}, then we have

$$D = \sum_{i=1}^{9} h^i = (1+h^5) + (1+h^5)h + (1+h^5)h^2 + (1+h^5)h^3 + (1+h^5)h^4 \quad \text{and}$$

$$D = \sum_{i=1}^{9} h^i = (1+h^2+h^4+h^6+h^8) + (1+h^2+h^4+h^6+h^8)h.$$

Note that $(1+h^5)h^i$ and $(1+h^2+h^4+h^6+h^8)h^j$ are both minimal v-sums. If we use the notion of lcm of each decomposition, we will then get 2 and 5 as the reduced exponents, respectively. Thus, we need to modify the earlier definition of exponent as follows.

Definition 7 Suppose that $D = \sum_{i=0}^{m-1} d_i g^i$ is a v-sum in $\mathbb{N}[C_m]$. We define the *c-exponent* of D to be the smallest k such that there exist t minimal v-sums $D_1, \ldots, D_t$ in $\mathbb{N}[C_m]$ with $D = \sum_{i=1}^{t} D_i$ and $k = \text{lcm}(k_1, \ldots, k_t)$, where k_i is the reduced exponent of D_i for $i = 1, \ldots, t$.

Note that in the example above, the c-exponent of D is 2.

Lemma 4 *Suppose that $D = \sum_{i=0}^{m-1} d_i g^i \in \mathbb{N}[C_m]$ is a v-sum with c-exponent k. Write $m = \prod_{i=1}^{s} p_i^{\alpha_i}$ and $k = \prod_{i=1}^{t} p_i$. Note that $t \leq s$ and p_i's are distinct primes. Then we have the followings:*

(a) $||D|| \geq 2 + \sum_{i=1}^{t}(p_i - 2)$;
(b) $D = \sum_{i=1}^{t} P_i E_i$, *where P_i is the subgroup of order p_i and $E_i \in \mathbb{Z}[C_m]$ for all i;*
(c) *Suppose that $\prod_{i=1}^{t} p_i^{\alpha_i} | d$ and $d|m$. If $\phi : \mathbb{Z}[C_m] \to \mathbb{Z}[C_d]$ is the natural projection, then $\chi(\phi(D)) = 0$ whenever $\operatorname{ord}(\chi) = d$.*

Proof By Lemma 3, we may assume that $D = \sum_{i=1}^{t} D_i$ such that each D_i is a minimal v-sum. Hence, by Corollary 1, we have

$$
\begin{aligned}
||D|| &= \sum_{i=1}^{t} |D_i| \\
&\geq \sum_{i=1}^{t} \left[2 + \sum_{q \in \mathcal{P}(k_i)} (q - 2) \right] \\
&\geq 2 + \sum_{q \in \mathcal{P}(k)} (q - 2) \\
&= 2 + \sum_{i=1}^{t} (p_i - 2),
\end{aligned}
$$

because $\mathcal{P}(k) = \bigcup_{i=1}^{t} \mathcal{P}(k_i)$.

By Lemma 2, $D_i = E_i g_i$ where $E_i \in \mathbb{N}[C_{k_i}]$ and $g_i \in C_m$. Clearly, $\tau(E_i) = 0$. Therefore, from [4, Theorem 2.2], it follows that $E_i = \sum_{q \in \mathcal{P}(k_i)} Q_q F_q$, where Q_q is the subgroup of order q and $F_q \in \mathbb{Z}[C_{k_i}]$. Since $D = \sum D_i$, D is of the desired form.

Finally, note that if ϕ and χ are defined as in (c), then $\chi(\phi(D)) = 0$ as $\chi(\phi(P_i)) = \chi(P_i) = 0$ for $i = 1, \ldots, t$. □

Next, we record a very useful result from [4, Theorem 4.8, Proposition 6.2].

Proposition 3 [4] *Let $D \in \mathbb{N}[C_m]$ be a minimal v-sum with c-exponent k. Then we have the followings:*

(a) *If $k = p$ is prime and P is the subgroup of order p of C_m, then $D = Ph$ for some $h \in C_m$.*
(b) *If $k = \prod_{i=1}^{t} p_i$ with $t \geq 2$ and $p_1 < p_2 < \cdots < p_t$ are primes, then $t \geq 3$ and*

$$||D|| \geq (p_1 - 1)(p_2 - 1) + (p_3 - 1).$$

Moreover, equality holds only if $D = (P_1^* P_2^* + P_3^*)h$ for some $h \in C_m$. Here $P_i^* = P_i - \{e\}$, and P_i is the subgroup of order p_i.

Remark 2 It follows from Proposition 3 that either k is a prime or k has at least three prime factors.

3 New nonexistence results of (m, n)-GBFs

In this section, we derive some new necessary conditions on (m, n)-GBFs, and then give new nonexistence results accordingly. First we fix the following notation. As before, we assume that g is the generator of C_m, and note that Remark 1 holds for any GBF f. To avoid confusion, we set g^0 as the identity element of C_m.

The following result is very important, in the sense that it allows to eliminate all prime factors of m greater than 2^n when deriving nonexistence results.

Proposition 4 *Suppose that f is an (m, n)-GBF and $m = \prod_{i=1}^{s} p_i^{\alpha_i}$ where p_i's are distinct primes. Let k_x be the c-exponent of E_x (as defined by (6)) for each $1_G \neq x \in G$. Set*

$$I = \{1 \le i \le s : p_i \nmid k_x \ \forall x \in G\} \text{ and } \overline{m} = \prod_{i \notin I} p_i^{\alpha_i}.$$

Then there exists an $(\overline{m}, n)$-GBF. In particular, if $p_i | m$ and $p_i > 2^n$, then there exists an $(m/p_i, n)$-GBF.

Proof By induction, it suffices to show that if $p_i \in I$, then there exists an $(m/p_i, n)$-GBF. Let $\eta : \mathbb{Z}[\langle g \rangle] \to \mathbb{Z}[\langle g^{p_i} \rangle]$ be the natural projection, it then follows that

$$\eta(D_f)\eta(D_f)^{(-1)} = 2^n + \sum_{1_G \neq x \in G} \eta(E_x)x.$$

Recall that E_x is a v-sum. By assumption p_i does not divide k_x for all $1_G \neq x \in G$. It follows from Lemma 4(c) that $\tau(\eta(E_x)) = 0$ if τ is a character of order m/p_i. Therefore, $\tau(\eta(D_f))$ gives rise to an $(m/p_i, n)$-GBF.

The last statement is now clear as if $p_i > 2^n$, then by Lemma 4(a), p_i does not divide k_x for any $1_G \neq x \in G$.

□

We record the following result which will be used from time to time later.

Lemma 5 *Suppose that f is an (m, n)-GBF, and p, q are distinct primes that both divide m. Then there exist $y \neq 1_G$ and $h \in supp(E_y)$ such that $pq | \circ(h)$.*

Proof As $C_m = \langle \{g^{f(x)} : x \in G\} \rangle$, there exist $u, v \in G$ such that $p | \circ(g^{f(u)})$ and $q | \circ(g^{f(v)})$. Since $g^{f(1_G)} = g^0 \in C_m$, we know that $g^{f(u)} \in supp(E_u)$ and $g^{f(v)} \in supp(E_v)$. We are done if $q | \circ(g^{f(u)})$ or $p | \circ(g^{f(v)})$. Otherwise, $ug^{f(u)}(vg^{-f(v)}) \in supp(E_{uv})$ and then clearly $pq | \circ(g^{f(u)-f(v)})$. The proof is completed. □

Before we proceed, we need a technical result.

Lemma 6 *Let q_1, q_2, q_3 be primes that divide m and Q_1, Q_2, Q_3 be subgroups of order q_1, q_2, q_3, respectively. Suppose that $4 \nmid m$ and $\sum_{i=1}^{t} Q_i h_i = \sum_{i=1}^{t} Q_i h_i^{-1}$ for some $h_1, h_2, h_t \in C_m$ with $t \ge 2$.*

(a) *If $q_1 \neq q_2$ and $t = 2$, then we may assume $h_i^{-1} = h_i$ for $i = 1, 2$.*
(b) *If $q_1 \neq q_2 = q_3$ and $t = 3$, then we may assume $Q_2 h_2 + Q_2 h_3 = Q_2(h_2 + h_2^{-1})$ and $h_1 = h_1^{-1}$.*
(c) *If all q_i's are distinct, then we may assume $h_i = h_i^{-1}$ for all i.*

Proof By assumption, we have

$$Q_1(h_1 - h_1^{-1}) = \sum_{i=2}^{t} Q_i(h_i^{-1} - h_i).$$

Suppose that $q_1^{\beta_1}||m$. Let $\phi : \mathbb{Z}[C_m] \to \mathbb{C}[C_m]$ be a ring homomorphism that fixes $g^{m/q_1^{\beta_1}}$ and sends $g^{q_1^{\beta_1}}$ to an $m/q_1^{\beta_1}$-primitive root of unity. Then, we have $\phi(Q_i(h_i - h_i^{-1})) = 0$ for $i = 2, \ldots, t$, which implies that $\phi(Q_1h_1 - Q_1h_1^{-1}) = 0$. Write $h_1 = g_1h'$ with $g_1 \in \langle g^{m/q_1^{\beta_1}} \rangle$ and $p_1 \nmid \circ(h')$. Then, we have $Q_1g_1\phi(h') = Q_1g_1^{-1}\phi(h'^{-1})$. Hence $g_1^2 \in Q_1$ and $\phi(h') = \phi(h'^{-1})$. If q_1 is odd, then $g_1 = g^0$. If $q_1 = 2$, then as $4 \nmid m$, g_1 can be taken as g^0 as well. In both cases, we may assume $g_1 = g^0$. It follows that $\phi(h')^2 = 1$. As ϕ is of order $m/q_1^{\beta_1}$, $h'^2 = g^0$. Therefore, $g_1h' = (g_1h')^{-1}$. Furthermore, we have

$$\sum_{i=2}^{t} Q_i(h_i^{-1} - h_i) = 0. \tag{7}$$

Now (a) follows easily by applying the same argument on Q_2.

If $t = 3$ and $q_2 = q_3$, we then obtain $Q_2(h_2+h_3) = Q_2(h_2^{-1}+h_3^{-1})$. If $Q_2h_2 = Q_2h_2^{-1}$, then we must have $Q_2h_3 = Q_2h_3^{-1}$. Then, $h_2^2 \in Q_2$ and $h_3^2 \in Q_2$. Using a similar argument as before, we may assume that $h_2 = h_3 = g^0$. If $Q_2h_2 = Q_2h_3^{-1}$, then clearly, we may take $h_3 = h_2^{-1}$ and we are done.

To obtain (c), we set $t = 3$. We then get our desired results by applying part (a) to Eq. (7). The proof is then completed. □

Now we are able to give the following necessary conditions on the existence of (m, n) GBFs, where m is odd.

Theorem 1 *Suppose that $m = \prod_{i=1}^{s} p_i^{\alpha_i}$, where $3 \le p_1 < p_2 < \cdots < p_s$ are odd primes and α_i's are all positive integers. If an (m, n)-GBF exists, then $s \ge 2$ and $3p_1 + p_2 \le 2^n$.*

Proof Recall that if $1_G \ne x \in G$ and χ is a character of order m, then $\chi(E_x) = 0$. If $s = 1$, then by Lemma 4(b), $E_x = P_1W$ where P_1 is a subgroup of order p_1 and $W \subseteq C_m$. In other words, $2^n = ||E_x|| = p_1||W||$. This is impossible as $p_1 \ne 2$.

Next, we assume that $s \ge 2$. As $E_x \in \mathbb{N}[C_m]$, we may write $E_x = \sum D_j$ such that all D_j's are minimal v-sums. Let k_j be the reduced exponent of D_j. If $|\mathcal{P}(k_j)| \ge 4$, then by Corollary 1, we have $||D_j|| \ge 2 + \sum_{i=1}^{4}(p_i - 2) \ge 3p_1 + p_2$. Thus, we may assume that $|\mathcal{P}(k_j)| \le 3$. But by Proposition 3, $|\mathcal{P}(k_j)| = 1$ or 3. In case that $|\mathcal{P}(k_j)| = 3$, $||D_j|| \ge q_1(q_2-1)+q_3-q_2 \ge p_1(p_2-1)+p_3-p_2$. If $p_1 \ge 5$, then clearly, $p_1(p_2-1)+p_3-p_2 \ge 3p_1 + p_2$. If $p_1 = 3$, it then follows that

$$p_1(p_2 - 1) + p_3 - p_2 \ge 2p_2 + (p_3 - 2) \ge p_2 + (5 + 7) \ge 3p_1 + p_2$$

as $p_2 \ge 5$ and $p_3 \ge 7$.

It remains to consider the case $|\mathcal{P}(k_j)| = 1$, i.e., $D_j = Q_jh_i$ where $h_i \in C_m$ and Q_j is a subgroup of order q_j. Note that q_j's need not be distinct. Therefore, $E_x = \sum_{j=1}^{t} Q_jh_j$. If all Q_j's are the same, then $E_x = Q_1Y$ for some $Y \in \mathbb{Z}[C_m]$. This is impossible as $q_1 \nmid 2^n$. In particular, it follows that $t \ge 2$ and we may assume $Q_1 \ne Q_2$ without loss of generality. Recall that all $D_i \in \mathbb{N}[C_m]$. Therefore,

$$2^n = ||E_x|| \ge q_1 + q_2 + (t - 2)p_1.$$

Hence, we are done if $t \geq 4$.

We first study the case $t = 3$. As $q_1 \neq q_2$, we may assume $q_1 \neq q_3$ as well. Since $E_x^{(-1)} = E_x$ and m is odd, we may then assume $h_1 = g^0$. Moreover, if $Q_2 = Q_3$, then $Q_2h_2 + Q_2h_3 = Q_2(h_2 + h_2^{-1})$. Whereas if $Q_2 \neq Q_3$, then $h_2 = h_3 = 1_G$ as m is odd. Therefore, the coefficient of g^0 is either 1 or 3 in both cases. This contradicts Lemma 1(a).

Thus, we may assume $t = 2$ for all $x \neq 1_G$. Moreover, as m is odd, E_x is of the form $Q_1 + Q_2$. In particular, each non-identity element in $supp(E_x)$ is of prime order. This contradicts Lemma 5.

The proof is then completed. □

The theorem above provides an alternative proof of [7, Corollary 2], from which we can have an improved result on the case $s = 2$.

Corollary 2 *Suppose that $m = \prod_{i=1}^{s} p_i^{\alpha_i}$, where $p_1 < p_2 < \cdots < p_s$ are odd primes and α_i's are all positive integers.*

(a) *There is no (m, n)-GBF when $s = 1$.*
(b) *There is no (m, n)-GBF if $s \geq 2$ and $3p_1 + p_2 > 2^n$.*
(c) *There is no (m, n)-GBF if there is no $(\prod_{i=1}^{r} p_i^{\alpha_i}, n)$-GBF where p_{r+1} is the smallest prime such that $p_1 + p_{r+1} > 2^n$.*

Proof (a) and (b) follow directly from Theorem 1. As for (c), it suffices to show that if $t \geq r + 1$, then p_t does not divide the c-exponent of E_x for any $x \neq 1_G$. We follow the notation used in the proof of Theorem 1. We write $E_x = \sum D_j$ such that all D_j's are minimal v-sums. Again, we denote by k_j the reduced exponent of D_j. Suppose that $p_t | k_1$. If $k_1 = p_t$, then $E_x \neq D_1$ as otherwise $p_t | 2^n$. Therefore, $||E_x|| \geq ||D_1|| + ||D_2|| \geq p_t + p_1 > 2^n$. On the other hand, if $k_1 \neq p_t$, then as shown before, k_1 is a product of at least three primes. Hence, $||D_1|| \geq p_t + p_1 > 2^n$, which is impossible. □

Remark 3 For $s = 2$, our result is stronger than [7, Corollary 2].

Now we consider the case when $m = 2m'$ with m' odd. If f is a $(2m', n)$ GBF, then we define

$$G_f := \{x \in G : f(x) \text{ odd}\}.$$

Note that a $(2m', n)$ GBF is trivially an (m', n) GBF if $G_f = \emptyset$ or G. Add f by m if necessary, we may always assume $|G_f| \leq |G|/2$. Note that $G_f^{(-1)} = G_f$ as G is 2-elementary. Apply a homomorphism $\psi : \mathbb{Z}[G \cdot C_m]$ such that ψ fixes every element in G and maps the generator g of C_m to -1, then we have

$$\begin{aligned} \psi(D_f)\psi(D_f^{(-1)}) &= (G - 2G_f)(G - 2G_f^{(-1)}) \\ &= (|G| - 4|G_f|)G + 4G_f^2 \\ &= 2^n + \sum_{1_G \neq x \in G} \psi(E_x)x. \end{aligned}$$

Write

$$G_f^2 = |G_f| + 2 \sum_{1_G \neq x \in G} b_x x. \tag{8}$$

We denote $\psi(E_x)$ by a_x. It then follows that for $x \neq 1_G$,

$$a_x = |G| - 4|G_f| + 8b_x. \tag{9}$$

The following is a consequence of [8, Theorem 1].

Lemma 7 *If n is odd, then G_f is a difference set in G if and only if $G_f = \{1_G\}$.*

We now give the following nonexistence results on $(2m', n)$ GBFs.

Theorem 2 *Let n be odd and $m = 2p^\alpha$, where α is a positive integer. Suppose that an (m, n)-GBF exists. Then $p < 2^{n-3}$ unless $p = 2^{n-2} - 1$ is a Mersenne prime. In particular, if $n \le 3$, there is no (m, n)-GBF if $m = p^\alpha$ or $m = 2p^\alpha$.*

Proof Let P_2 be the subgroup of order 2 and P be a subgroup of order p. For any $x \neq 1_G$, we conclude from Lemma 4(b) that $E_x = P_2 Y_x + P Z_x$ for some $Y_x, Z_x \in \mathbb{N}[C_m]$. Note that $\psi(E_x) \neq 0$ for some $x \neq 1_G$. Otherwise, the c-exponent of all E_x is 2 and by Proposition 4, there exists a (2, 3)-GBF, which is impossible. Hence, $a_x = \psi(E_x) \neq 0$ for some $x \neq 1_G$. Therefore, we have $\psi(P)|\psi(E_x)$, i.e., $p|a_x$. Note that in view of Eq. (9), $4p|a_x$ if $|G_f|$ is odd and $8p|a_x$ if $|G_f|$ is even. We are done if $8p|a_x$ as $|a_x| < 2^n$. We may therefore assume that $|G_f|$ is odd.

Suppose that $G_f = \{1_G\}$. Then, $a_x = 2^n - 4$ if $x \neq 1_G$. Hence, $4p|a_x$. It follows that $p_1 < 2^{n-3}$ unless $4p = 2^n - 4$ which implies that $p = 2^{n-2} - 1$ is a Mersenne prime.

Suppose that $G_f \neq \{1_G\}$. As G_f is not a difference set, there exist two elements $x \neq 1_G$ and $x' \neq 1_G$ such that $b_x > b_{x'} \ge 0$. Since $p|a_x$ and $p|a_{x'}$, it follows that $p|(b_x - b_{x'})$ and $b_x - b_{x'} = tp$ for some positive integer t. To get our desired result, we need to find a bound on $b_x - b_{x'}$. Note that in view of Eq. (8), $b_x \le |G_f|/2 \le |G|/4$. Hence, we get our desired result if $t \ge 2$. Thus, we may assume that $t = 1$, i.e., $b_x = p + b_{x'}$.

Suppose that $G = \langle x \rangle \cdot G'$, where G' is a subgroup of order 2^{n-1} in G. As the coefficient of x in G_f^2 is $2b_x$, there are $2b_x = 2p + 2b_{x'}$ pairs (u, v) of elements in $G_f \times G_f$ such that $uv = x$. Therefore, there exists a set $Y \subseteq G' \cap G_f$ such that $Y \cup (Yx) \subseteq G_f$ with $|Y| = p + b_{x'}$. Write $G_f = (Y \cup Z_1) \cup (Yx \cup Z_2 x)$ such that

$$Z_1 \subseteq G', Z_2 \subseteq G', Y \cap Z_1 = \emptyset \text{ and } Y \cap Z_2 = \emptyset.$$

Since $b_x = |Y|$, it follows that $Z_1 \cap Z_2 = \emptyset$. Moreover, we have

$$G_f^2 = [2Y^2 + 2Y(Z_1 + Z_2) + Z_1^2 + Z_2^2] + [2Y^2 + 2Y(Z_1 + Z_2) + 2Z_1 Z_2]x.$$

Note that the support of $[2Y^2 + 2Y(Z_1 + Z_2) + Z_1^2 + Z_2^2]$ is in G' and the support of $[2Y^2 + 2Y(Z_1 + Z_2) + 2Z_1 Z_2]x$ is in $G'x$. We now consider the coefficients of the following group elements

$$Z = [2Y^2 + 2Y(Z_1 + Z_2) + Z_1^2 + Z_2^2] - [2Y^2 + 2Y(Z_1 + Z_2) + 2Z_1 Z_2] = (Z_1 - Z_2)^2.$$

For any $1_G \neq v \in G'$, the coefficient of v in Z is equal to $2(b_v - b_{vx})$. Clearly, the absolute value of the coefficient of v in Z is less than $|Z_1| + |Z_2|$ as Z_1 and Z_2 are disjoint. Thus, if there exists $v \neq 1_G$ in G' such that $b_v - b_{vx}$ is nonzero, then $p|(b_v - b_{vx})$ and we obtain

$$2p \le 2|b_v - b_{vx}| \le |Z_1| + |Z_2| \le (|G_f| - 2b_x) \le |G_f| - 2p.$$

Hence, we get $4p \le |G_f| \le |G|/2$ and $p \le 2^{n-3}$. Thus, it remains to deal with the case $(Z_1 - Z_2)^2 = |Z_1| + |Z_2|$.

If both $Z_1 = Z_2 = \emptyset$, then $2b_x = |G_f|$. Hence, $|G_f|$ is even and as remarked earlier, we are done in this case. Note that as $G = C_2^n$, all character values of $Z_1 - Z_2$ are integers. Thus, $|Z_1| + |Z_2|$ is a square. Since $Z_1 \cap Z_2 = \emptyset$, all nonzero coefficients of $Z_1 - Z_2$ is ± 1. On the other hand, if q is an odd prime divisor or $|Z_1| + |Z_2|$, then q divides the all nonzero coefficients of $Z_1 - Z_2$ by applying Fourier inversion formula. This is impossible. It follows that $|Z_1|+|Z_2| = 2^t$. Again, we are done if $t \geq 1$ as then $|G_f| = 2b_x + |Z_1| + |Z_2|$ is even. Hence, we may assume that $t = 0$, i.e., $|Z_1| + |Z_2| = 1$. Note that the coefficient of 1_G in $[2Y^2 + 2Y(Z_1 + Z_2) + Z_1^2 + Z_2^2]$ is $|G_f|$ and the coefficient of 1_G in $[2Y^2 + 2Y(Z_1 + Z_2) + 2Z_1Z_2]$ is the same as the coefficient of x in G_f^2. As $Z = 1$, it follows that $2b_x = |G_f| - 1$. Hence, $a_x = |G| - 4|G_f| + 4(|G_f| - 1) = 2^n - 4$. Recall that $4p|a_x$. Hence either $p = 2^{n-2} - 1$ or $p < 2^{n-3}$.

The proof is then completed. □

Corollary 3 *Let n be odd and $m = 2\prod_{i=1}^{s} p_i^{\alpha_i}$, where $p_1 < p_2 < \cdots < p_s$ are odd primes and α_i's are all positive integers.*

(a) *If $s = 1$, then there is no (m, n)-GBF if one of the following conditions is satisfied:*

  (i) *$p_1 > 2^{n-2}$;*
  (ii) *p_1 is not a Mersenne prime and $p_1 > 2^{n-3}$;*
  (iii) *$p_1 \equiv 3,\ 5 \pmod 8$.*

(b) *If $s \geq 2$, and r is the least integer such that $p_{r+1} + p_1 > 2^n + 2$, then there is no (m, n)-GBF if there is no $(2\prod_{i=1}^{r} p_i^{\alpha_i}, n)$-GBF. In particular, there is no (m, n)-GBF if $p_1 > 2^{n-2}$ and $p_1 + p_2 > 2^n + 2$.*

Proof It is easily seen that (i) and (ii) of (a) directly follow from Theorem 2. If (iii) holds, it is known that no $(2p_1^{\alpha_1}, n)$-GBF exists.

To prove (b), it is sufficient to show that for $i \geq r + 1$, p_i does not divide the c-exponent of any E_x for $x \neq 1_G$. As before, we wirte $E_x = \sum D_j$ and k_j the reduced exponent of D_j. We may assume that p_i divides k_1. If k_1 consists of at least three prime factors, then $||D_i|| \geq 2 + (p_1 - 2) + (p_i - 2)$. Thus, $2^n \geq p_1 + p_i - 2 \geq p_1 + p_{r+1} - 2 > 2^n$. This is impossible. Therefore, we have $k_1 = p_i$.

Otherwise, we assume that p_i divides the reduced exponent k_x of $\tau(E_x)$. If $k_x = p_i$, it follows from the argument in (a) that $4p_i \leq 2^n$. This is impossible as $2^n < p_1 + p_i < 4p_i$. Therefore, $p_j|k_x$ for some $j \neq i$. But then by Proposition 3, $2^n \geq p_j + p_i - 2 > p_{r+1} + p_1 - 2$. This is impossible. □

Remark 4 When compared with [7, Theorem 2], our result in Corollary 3 is stronger in all cases quoted in Table 2 [7] therein except for the case that $p = 191$.

4 Nonexistence results for $n = 3$

In this section, we show that there in no $(m, 3)$-GBF for all m odd or $m \equiv 2 \pmod 4$. By Proposition 4, we may assume that all prime factors of m are less than or equal to 7. According to Corollary 2, we conclude that there is no $(m, 3)$-GBF if m is odd. Therefore, we may write $m = 2 \cdot 3^a 5^b 7^c$. For convenience, we fix the following notation. Let g_2, g_3, g_5, g_7 be elements of order 2, 3, 5, 7, respectively. Let P_2, P_3, P_5, P_7 be subgroups of order 2, 3, 5 and 7, respectively.

We assume that f is an $(m, 3)$-GBF. We first determine what E_x is if $x \neq 1_G$. As seen before, $\tau(E_x) = 0$ for any character of order m. Recall that $\mathcal{P}(k)$ denotes the set of all prime factors of the integer k.

Lemma 8 *For any $x \neq 1_G$, write $E_x = \sum D_i$ where each D_i is a minimal v-sum with reduced exponent k_i. Then $\mathcal{P}(k_i) = \{2\}, \{3\}, \{5\}, \{7\}$ or $\{2, 3, 5\}$ or $\{2, 3, 7\}$. Moreover,*

(a) *If* $\mathcal{P}(k_i) = \{j\}$ *for some* $j \in \{2, 3, 5, 7\}$, *then* $D_i = P_j h_j$ *for some* $h_j \in C_{30}$.
(b) *If* $\mathcal{P}(k_i) = \{2, 3, 7\}$, *then* $E_x = g_2^{\alpha}(P_7^* + g_2 P_3^*)$ *for some integer* α.

Proof Let k_x be the reduced exponent of E_x. Note that $k_x \neq 2 \cdot 3 \cdot 5 \cdot 7, 3 \cdot 5 \cdot 7$, or $2 \cdot 5 \cdot 7$ as $||E_x|| > (7-2) + (5-2) + 2 > 8$. Therefore, either $|\mathcal{P}(k_i)| = 1$, $\mathcal{P}(k_i) = \{2, 3, 7\}$ or $\{2, 3, 5\}$. (a) then follows from Lemma 2.

For (b), note that $||D_i|| \leq 8$. Hence, by Proposition 3(b), $D_i = h(P_7^* + g_2 P_3^*)$ for some element $h \in C_m$. As $||E_x|| = 8$, $E_x = D_i$. As $E_x = E_x^{(-1)}$, we have $h = g_2^{\alpha}$ for some integer α. □

Corollary 4 *If* $7|k_x$, *then* $E_x = g_2^{\alpha}(P_7^* + g_2 P_3^*)$.

Proof We will follow the notation used above. By assumption, $7|k_i$ for some i. If $k_i = 7$, then $D_i = P_7 h_i$. Since $||E_x|| = 8$, it follows that $||D_j|| = 1$ if $j \neq i$. This is impossible as then $\tau(D_j) \neq 0$. Hence, k_i is not a prime and therefore, $k_i = 2 \cdot 5 \cdot 7$. By Lemma 8 (b), our desired result follows. □

Let ψ be as defined in Sect. 3. As we have seen before, $a_x = \psi(E_x) \equiv 0 \bmod 4$. With the condition $E_x = E_x^{(-1)}$, this allows us to narrow down the possibilities of E_x when 7 does not divide the c-exponent of E_x.

Lemma 9 *If* $7 \nmid k_x$, *then* E_x *is in one of the forms below:*

(a) $E_x = P_2 W$ *and* $a_x = 0$.
(b) $E_x = (P_3 + P_5)g_2^{\alpha}$ *and* $a_x = \pm 8$.
(c) $E_x = g_2^{\alpha}[g_2(g^0 + g_5 + g_5^4)(g_3 + g_3^2) + (g_5^2 + g_5^3)]$ *or* $g_2^{\alpha}[g_2(g^0 + g_5^2 + g_5^3)(g_3 + g_3^2) + (g_5 + g_5^4)]$ *and* $a_x = \pm 4$. *In particular, supp*$(E_x) \cap P_2 = \emptyset$. *[Recall that* g^0 *is the identity of* C_m. *]*

Proof We continue with the notation used in Lemma 8. If all k_i's are prime, then in view of Lemma 8,

$$E_x = P_2 X + P_3 Y + P_5 Z,$$

where $X, Y, Z \in \mathbb{N}[C_m]$. As $||E_x|| = 8$ and $8 = 2||X|| + 3||Y|| + 5||Z||$. It is clear that

$$(||X||, ||Y||, ||Z||) = (4, 0, 0),\ (1, 2, 0),\ \text{or } (0, 1, 1).$$

If $(||X||, ||Y||, ||Z||) = (1, 2, 0)$, then $E_x = P_2(h_1 + h_2) + P_3 h_3$. In this case, $\psi(E_x) = \pm 3$. This is impossible. Next, if $(||X||, ||Y||, ||Z||) = (4, 0, 0)$, then (a) holds. If $(||X||, ||Y||, ||Z||) = (0, 1, 1)$, then $E_x = P_3 h_1 + P_5 h_2$. By Lemma 6(a), $h_i = g_2^{\alpha_i}$. Note that $\psi(E_x) = \pm 2 \neq \pm 4$ if $\alpha_1 \neq \alpha_2 \bmod 2$. Since $a_x \equiv 0 \bmod 4$, (b) holds.

As k_i's are not all prime, we may assume that k_1 is not a prime. Then by Lemma 8, $k_1 = 2 \cdot 3 \cdot 5$. But then by Proposition 3(b), $||D_1|| \geq 6$. If $E_x \neq D_1$, then $||D_2|| \leq 2$. Hence $D_2 = P_2 h'$ for some $h' \in C_m$ and $||D_1|| = 6$. Thus, $D_1 = (P_2^* P_3^* + P_5^*)h$ for some $h \in C_{30}$. Since $||E_x|| = 8$, $E_x = D_1 + D_2$. But $\psi(E_x) = \psi(D_1 + D_2) = \pm 2$. This is impossible as $4|a_x$. Hence, E_x is a minimal v-sum and $E_x = D_1 = Dh$ for some $D \in \mathbb{N}[C_{30}]$. As $E_x = E_x^{(-1)}$, we have $h \in C_{30}$. So, $E_x \in \mathbb{N}[C_{30}]$. We may write $E_x = \sum_{i=0}^{4} A_i g_5^i$, where $A_i \in \mathbb{N}[C_6]$. Clearly,

$$8 = \sum_{i=0}^{4} ||A_i||.$$

Let τ be a character of order 30. If $A_i = 0$ for some i, then $\tau(A_j) = 0$ for all j as $\tau(E_x) = 0$. Then, E_x is not a minimal v-sum unless $E_x = A_j$ for some j. So, $k_1|6$ and $k_1 \neq 30$. This is impossible. Hence, $||A_i|| \geq 1$ for each i.

Claim $||A_j|| \leq 3$ for all $j = 0, \ldots, 4$.

Otherwise, we assume that $||A_\ell|| \geq 3$ for some ℓ. It then follows that $||A_j|| \leq 2$ if $j \neq \ell$. Since $E_x = E_x^{(-1)}$, we have $\ell = 0$. On the other hand, if $||A_j|| = 2$ for some j, then again $||A_t|| \neq 2$ whenever $t \neq j$. Using the condition $E_x = E_x^{(-1)}$ again, we have $j = 0$. This is impossible. Hence, all other $||A_j|| = 1$. Thus we conclude, $||A_0|| = 4$ and $||A_i|| = 1$ if $i = 1, 2, 3, 4$. Write $A_1 = h$, where $h \in C_6$. As $\tau(A_0) = \tau(h)$, we have $\tau(A_0 + g_2 h) = 0$. Note that $||A_0 + g_2 h|| = 5$. Since $\tau(A_0 + g_2 h) = 0$, we may apply a similar argument as in Lemma 8 to conclude that $A_0 + g_2 h = P_2 h_1 + P_3 h_2$ for some $h_1, h_2 \in C_6$. Therefore, $A_0 = P_2 h_1 + h_3 + h_4$ or $A_0 = h_3 + P_3 h_2$ for some $h_3, h_4 \in C_6$. In either case, it contradicts the assumption that E_x is a minimal v-sum.

Hence, we conclude that $||A_j|| \leq 2$ for all j. Using the assumption that $E_x = E_x^{(-1)}$ again, we then obtain two possible cases.

(i) $||A_0|| = ||A_1|| = ||A_4|| = 2$ and $||A_2|| = ||A_3|| = 1$ or
(ii) $||A_0|| = ||A_2|| = ||A_3|| = 2$ and $||A_1|| = ||A_4|| = 1$.

It remains to show that E_x is of the desired form when (i) holds. We may assume that $A_i = h_i$ for some $h_i \in C_6$ for $i = 2, 3$. Since $\tau(E_x) = 0$ for any character τ of order 30, we set $h_2 = h_3 = h$. As $E_x = E_x^{(-1)}$, we see that $h = g_2^\alpha$.

Note that for $i = 0, 1, 4$, $||A_i + g_2 h|| = 3$ and $\tau(A_i + g_2 h) = 0$. Therefore, $A_i + g_2 h = P_3 g_2 h$ as $g_2 h$ is in the support of all $A_i + g_2 h$. In other words, $A_i = P_3^*(g_2 h)$ for $i = 0, 1, 4$. It is now clear that E_x is of desired form. This shows that (c) holds. □

Theorem 3 *There is no $(m, 3)$-GBF for any integer m odd or $m \equiv 2 \pmod 4$.*

Proof Recall that by earlier discussion of this section, we may assume that $m = 2 \cdot 3^a \cdot 5^b \cdot 7^c$. We first remove the case $7|m$.

We may assume that 7 divides the c-exponent of E_x for some $x \neq 1_G$. By Lemma 9, we see that $E_x = h^\alpha(P_7^* + hP_3^*)$ and $\psi(E_x) = \pm 4$. It follows from Eq. (8) that $a_v = \pm 4$ for any $v \neq 1_G$. Therefore, E_v is of the form in Corollary 4 or Lemma 9(c). That means there is no element in $supp(E_v)$ of order a multiple of 21 for any v. This contradicts Lemma 5. Thus, we may assume that 7 does not divide the c-exponent of E_x for all $x \in G$. By Proposition 4, it remains to show that $(2 \cdot 3^a \cdot 5^b, 3)$-GBF does not exist.

In view of Lemma 9, $E_x \in \mathbb{N}[C_{30}]$ for all $x \neq 1_G$. It follows that $supp(D_f) \subset G \cdot C_{30} h'$ for some $h' \in C_m$. After multiplying D_f with h'^{-1}, we may assume $D_f \in \mathbb{N}[G \cdot C_{30}]$. Recall that we may assume that $1 \leq |G_f| \leq 4$. We may assume that $1_G \in G_f$ instead of $1_G \in G \setminus G_f$. We now discuss by cases.

Case (1) $|G_f| = 2$.

As $1_G \in G_f$, we write $G_f = \{1_G, v\}$. Note that $a_x = 8$ or 0. It follows that $a_v = 8$ and $a_x = 0$ if $x \neq 1_G, v$. By Lemma 9, we have $E_v = P_5 + P_3$ and $E_x = P_2 W_x$ for some $W_x \in \mathbb{Z}[C_{30}]$ if $x \neq 1_G, v$.

Let $\eta : \mathbb{Z}[G \cdot C_{30}] \to \mathbb{Z}[G \cdot C_5]$ be a ring homomorphism such that $\eta(g_2) = -1$ and $\eta(g_3) = 1$ and $\eta(g_5) = g_5$; and $\eta(x) = 1$ for all $x \in G$. Note that $\eta(E_x) = 0$ if $a_x = 0$ as $E_x = P_2 W_x$ for some $W_x \in \mathbb{N}[C_{30}]$. Thus, we get

$$\eta(D_f)\eta(D_f)^{(-1)} = 11 + P_5.$$

Write $\eta(D_f) = \sum a_i g_5^i$ where $a_i \in \mathbb{Z}$. Observe that if we further map g_5 to 1, then the resulting map is just ψ. Thus, we have $\sum a_i = \psi(D_f)$. Then as $|G_f| = 2$, $\psi(D_f) = \sum a_i = 8 - 2 \cdot 2 = 4$. By considering the coefficient of identity of $11 + P_5$, we get $\sum a_i^2 = 12$. Thus $|a_i| \geq 2$ for some i. If the maximum value of $|a_i|$ is 2, then there must be two more a_j's with $|a_j| = 2$ and the rest is 0. That is impossible as then 2 divides $\eta(D_f)$ but 2 does not divide $11 + P_5$ in $\mathbb{Z}[P_5]$.

Hence, the maximum value of $|a_i|$ is 3. Then there are exactly three a_j's with $|a_j| = 1$. Since $\sum a_i = 4$, exactly one a_i is -1. So we may assume that $\eta(D_f) = 3 + g_5 + g_5^\beta - g_5^\gamma$ with $1 \neq \beta \neq \gamma \neq 1$. Clearly, we may assume either $\beta = 4$ or $\gamma = 4$.

If $\beta = 4$, then we may take $\gamma = 2$ or 3. Then, the coefficient of g_5^γ is -2, which is impossible. If $\gamma = 4$, then $\beta = 2$ or 3. In that case, the coefficient of g_5^β is -2, which is also impossible. Therefore, we have $|G_f| \neq 2$.

Case (2) $|G_f| = 4$. We may assume that $G_f = \{1_G, v_1, v_2, v_3\}$.

Subcase (a) $v_3 = v_1 v_2$ and G_f is a subgroup of order 4. Hence, $G_f^2 = 4G_f$ and $(G - 2G_f)^2 = 8G_f - 8G_f v$ for some nonzero $v \in G$. Therefore, $a_x = \pm 8$ for all $x \in G$. In view of Lemma 9, $E_x = g_2^\alpha(P_3 + P_5)$ for all nonzero $x \in G$. By Lemma 5, this is impossible as there is no element in $supp(E_v)$ which is divisible by 15 for any v.

Subcase (b) $v_3 \neq v_1 v_2$. Let $H = \{1_G, v_1, v_2, v_1 v_2\}$ be the subgroup of order 4. Then $G_f^2 = 2G + 2 - 2v_1 v_2 v_3$. For convenience, we write $v = v_1 v_2 v_3$. Thus, $a_v = -8$ and $a_x = 0$ if $x \neq 1_G$ or v. As $v \notin H$, there exists a ring homomorphism η' that maps $H \cdot P_3$ to identity, and $\eta'(g_2) = \eta'(v) = -1$. Then as before $\eta'(E_x) = 0$ if $a_x = 0$. Hence, we obtain

$$\eta'(D_f)\eta'(D_f)^{(-1)} = 8 + (-1)(-3 - P_5) = 11 + P_5.$$

Write $\eta'(D_f) = \sum a_i g_5^i$. Observe that $\sum a_i = \eta'(G - 2G_f) = -4$. As shown above, there is no solution in $\mathbb{Z}[P_5]$.

Case (3) $|G_f| = 1$ or 3. Ten $a_x = \pm 4$ for all $x \neq 1_G$ in G. Therefore, by Lemma 9(c), for any E_x with $1_G \neq x \in G$,

$$E_x = g_2^\alpha[(g^0 + g_5 + g_5^4)(g_3 + g_3^2) + g_2(g_5^2 + g_5^3)] \text{ or}$$
$$g_2^\alpha[(g^0 + g_5^2 + g_5^3)(g_3 + g_3^2) + g_2(g_5 + g_5^4)].$$

Observe that if we write $E_x = \sum_{i=0}^4 W_{xi} g_5^i$, then $||W_{x0}|| = 2$ and $P_2 \cap supp(E_x) = \emptyset$.

Write $D_f = \sum_{i=0}^4 B_i g_5^i$ where $B_i \in \mathbb{Z}[G \cdot C_6]$ and $D_f D_f^{(-1)} = \sum_{i=0}^4 Z_i g_5^i$ with $Z_i \in \mathbb{N}[G \cdot C_6]$. For each i, $B_i = A_{i0} + A_{i1} g_3 + A_{i3} g_3^2$ where $A_{ij} \in \mathbb{N}[G \cdot P_2]$. If $||A_{ij}|| \geq 2$, i.e., $A_{ij} = x_1 h_1 + x_2 h_2 + \cdots$, where $x_1, x_2 \in G$ and $h_1, h_2 \in P_2$, then $A_{ij} A_{ij}^{(-1)} = 2 + x_1 x_2 h_1 h_2 + \cdots$. Hence, $supp(E_{x_1}) \cap \{g^0, g_2\} \neq \emptyset$. This contradicts Lemma 9(c). Thus, $|A_{ij}| \leq 1$ and $||B_i|| \leq 3$. Note that

$$||Z_0|| = 8 + \sum_{x \neq 1_G} ||W_{x0}|| = 8 + 2 \times 7 = 22 = \sum_{i=0}^4 ||B_i||^2.$$

Observe that not all $||B_i|| \leq 2$. Using the equation above, we may assume that $||B_i|| = ||B_j|| = 3$ and $||B_k|| = 2$ for some distinct i, j, k. Then we have

$$B_i = \sum_{t=0}^2 u_t g_2^{\alpha_i} g_3^t = u_0 g_2 \alpha_0 \left(1 + u_0 u_1 g_2^{\alpha_1 - \alpha_0} g_2 g_3 + u_0 u_1 g_2^{\alpha_2 - \alpha_0} g_3^2\right).$$

Let ϕ be a character on $G\cdot C_{30}$ such that $\phi(u_0u_1) = (-1)^{\alpha_1-\alpha_0}$ and $\phi(u_0u_2) = (-1)^{\alpha_2-\alpha_0}$. Note that such a ϕ exists as $u_0u_1 \neq u_0u_2$. Then, it is clear that $\phi(B_i) = 0$. Thus, $|\phi(D_f)|^2 = |\phi(B_j)\zeta_5^j + \phi(B_k)\zeta_5^k|^2 = 8$. In other words, we have

$$|\phi(B_j)|^2 + |\phi(B_k)|^2 + \phi(B_j)\overline{\phi(B_k)}\zeta_5^{j-k} + \phi(B_k)\overline{\phi(B_j)}\zeta_5^{k-j} = 8.$$

This is impossible unless $\phi(B_j) = 0$ or $\phi(B_k) = 0$. But then $||B_k|| = 2$ and $||A_{kj}|| \leq 1$ imply that $\phi(B_k) \neq 0$. Thus $\phi(B_j) = 0$ and $|\phi(B_k)|^2 = 8$. This is impossible as $||B_k|| = 2$. This finish showing that $|G_f| \neq 1$ or 3.

The proof is then completed. □

Acknowledgements The authors are very grateful to the two anonymous reviewers for all their detailed comments that improved the quality and the presentation of this paper.

References

1. Carlet C.: Boolean functions for cryptography and error correcting codes. Boolean Models Methods Math. Comput. Sci. Eng. **2**, 257–397 (2010).
2. Conway J.H., Jones A.J.: Trigonometric diophantine equations (on vanishing sums of roots of unity). Acta Arith. **30**(3), 229–240 (1976).
3. Kumar P.V., Scholtz R.A., Welch L.R.: Generalized bent functions and their properties. J. Comb. Theory Ser. A **40**(1), 90–107 (1985).
4. Lam T.Y., Leung K.H.: On vanishing sums of roots of unity. J. Algebra **224**(1), 91–109 (2000).
5. Lenstra Jr., H.W.: Vanishing sums of roots of unity. In: Proceedings of the Bicentennial Congress Wiskundig Genootschap (Vrije Univ., Amsterdam, 1978), Part II, *Math. Centre Tracts*, vol. 101, pp. 249–268. Math. Centrum, Amsterdam (1979)
6. Leung K.H., Schmidt B.: Nonexistence results on generalized bent functions $\mathbb{Z}_q^m \to \mathbb{Z}_q$ with odd m and $q \equiv 2 \pmod 4$. J. Comb. Theory Ser. A **163**, 1–33 (2019).
7. Liu H., Feng K., Feng R.: Nonexistence of generalized bent functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_m$. Des. Codes Cryptogr. **82**(3), 647–662 (2017).
8. Mann H.B.: Difference sets in elementary Abelian groups. Ill. J. Math. **9**, 212–219 (1965).
9. Martinsen T., Meidl W., Mesnager S., Stănică P.: Decomposing generalized bent and hyperbent functions. IEEE Trans. Inform. Theory **63**(12), 7804–7812 (2017).
10. Rothaus O.S.: On “bent” functions. J. Comb. Theory Ser. A **20**(3), 300–305 (1976).
11. Schmidt K.U.: $\mathbb{Z}_4$-valued quadratic forms and quaternary sequence families. IEEE Trans. Inform. Theory **55**(12), 5803–5810 (2009).
12. Schmidt K.U.: Quaternary constant-amplitude codes for multicode CDMA. IEEE Trans. Inform. Theory **55**(4), 1824–1832 (2009).
13. Stănică P., Martinsen T., Gangopadhyay S., Singh B.K.: Bent and generalized bent Boolean functions. Des. Codes Cryptogr. **69**(1), 77–94 (2013).
14. Tang C., Xiang C., Qi Y., Feng K.: Complete characterization of generalized bent and 2^k-bent Boolean functions. IEEE Trans. Inform. Theory **63**(7), 4668–4674 (2017).