Des. Codes Cryptogr. (2017) 85:471–482
DOI 10.1007/s10623-016-0319-z

Nonexistence of two classes of generalized bent functions

Jianing Li[1] · **Yingpu Deng**[1,2]

Received: 24 July 2015 / Revised: 29 November 2016 / Accepted: 30 November 2016 /
Published online: 19 December 2016

Abstract We obtain some new nonexistence results of generalized bent functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$ (called type $[n, q]$) in the case that there exist cyclotomic integers in $\mathbb{Z}[\zeta_q]$ with absolute value $q^{\frac{n}{2}}$. This result generalizes two previous nonexistence results $[n, q] = [1, 2 \times 7]$ of Pei (Lect Notes Pure Appl Math 141:165–172, 1993) and $[3, 2 \times 23^e]$ of Jiang and Deng (Des Codes Cryptogr 75:375–385, 2015). We also remark that by using a same method one can get similar nonexistence results of GBFs from $\mathbb{Z}_2^n$ to $\mathbb{Z}_m$.

Keywords Generalized bent functions · Cyclotomic fields · Prime ideal factorizations · Class groups

Mathematics Subject Classification 11R04 · 94A15

1 Introduction

Bent functions were first introduced by Rothaus [16] in 1976, which are functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2$ with some property, where $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ for a positive integer m. Dillon [1] showed that bent functions are the characteristic functions of elementary Hadamard difference sets. Bent functions have many applications to coding theory, cryptography and sequence designs [13]. In coding theory, bent functions have the maximum distance to the first order binary Reed–Muller code. In a cryptosystem, functions with large nonlinearity values are usually

Communicated by A. Pott.

✉ Jianing Li
lijianing19891026@163.com

Yingpu Deng
dengyp@amss.ac.cn

1 Key Laboratory of Mathematics Mechanization, NCMIS, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, People's Republic of China

2 University of Chinese Academy of Sciences, Beijing 100049, People's Republic of China

employed to resist linear crypto-analysis and correlation-attack, and bent functions are just the ones with maximum nonlinearity.

Bent functions have many generalizations. Kumar et al. [9] considered bent functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$ in 1985, where $q \geq 2$ and $n \geq 1$ are integers. Later, bent functions were generalized to arbitrary finite abelian groups [11,17], even to arbitrary finite groups [15,20].

A natural question is when bent functions do exist. Rothaus [16] proved that bent functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2$ exist if and only if n is even. However, this problem is far from being solved for other types of generalized bent functions. For generalized bent functions (GBF for short) from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$ defined in [9], Kumar et al. constructed them except the case that n is odd and $q \equiv 2 \pmod 4$. There are many nonexistence results for GBF defined in [9], for example, see [2–4,7,8,14] and the references in [8]. Especially, Feng and co-authors built connections between the nonexistence of GBF and class numbers of imaginary quadratic fields in [2–4]. In fact, they proved stronger results that there are no algebraic integers with prescribed absolute values in some cyclotomic field. However, GBFs' existence request that there are algebraic integers with prescribed absolute values in some cyclotomic field and some specific conditions (so-called bent conditions) are also satisfied. In [8], Jiang and Deng showed that there are no GBFs from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$ with $n = 3$ and $q = 2 \cdot 23^e$ for $e \geq 1$. Notice that there are algebraic integers with prescribed absolute values $(2 \cdot 23^e)^{\frac{3}{2}}$ in the cyclotomic field $\mathbb{Q}(\zeta_{23^e})$, but Jiang and Deng showed that the bent conditions are not satisfied.

Motivated by the results in [7,8], we obtain further nonexistence results for GBFs from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$.

This paper is organized as follows. In Sect. 2, we list some previous work and state our main result. In Sect. 3, we list some facts of algebraic number theory which we need. We prove the main result in Sect. 4. In Sect. 5, we apply our method to GBFs from $\mathbb{Z}_2^n$ to $\mathbb{Z}_m$ and obtain similar results. Finally, a short conclusion is given.

2 Previous work and our main result

Let $q \geq 2$ be an integer, $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ and $\zeta_q = \exp\left(\frac{2\pi i}{q}\right)$. A function f from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$ is called a generalized bent function (GBF) of type $[n, q]$ if $F(\lambda)\overline{F(\lambda)} = q^n$ for every $\lambda \in \mathbb{Z}_q^n$ where

$$F(\lambda) = \sum_{x \in \mathbb{Z}_q^n} \zeta_q^{f(x)} \cdot \zeta_q^{-x \cdot \lambda}$$

is the Fourier transform of the function $\zeta_q^{f(x)}$, $x \cdot \lambda$ is the standard dot product, and $\overline{F(\lambda)}$ is the complex conjugate of $F(\lambda)$.

Note that if there is no element in $\mathbb{Z}[\zeta_q]$ with absolute value $q^{\frac{n}{2}}$, then there is no GBF of type $[n, q]$. Feng [2] and Feng and Liu [3,4] get nonexistence results by showing that there are no cyclotomic integers with prescribed absolute values. For a survey of their results, see [8]. In this paper, we will focus on the nonexistence of GBFs of type $[n, q = 2 \times p^e]$ where $p \equiv 7 \pmod 8$ is a prime. Feng [2] proved the following result:

(1) Let $p \equiv 7 \pmod 8$ be a prime, f the order of 2 modulo p^e, and m the smallest odd positive integer such that $x^2 + py^2 = 2^{m+2}$ has $\mathbb{Z}$-solutions. Then there is no GBF of type $[n < \frac{m}{s}, 2p^e]$, where n is odd and $s = \frac{p^e - p^{e-1}}{2f}$.

However, in this paper we focus on the nonexistence of GBFs in the case that *there exist cyclotomic integers with prescribed absolute value*. Restricting to the case $q = 2p^e$ ($p \equiv 7 \bmod 8$), there are three known results:

(2) Pei [14] proved that there is no GBF of type $[n = 1, q = 2 \times 7]$. Notice that the absolute value of $\left(\frac{1+\sqrt{-7}}{2}\right)\sqrt{-7} \in \mathbb{Z}[\zeta_7]$ is $14^{\frac{1}{2}}$.

(3) Ikeda [7] proved that there is no GBF of type $[n = 1, q = 2 \times p^e]$, where $p \equiv 7 \pmod 8$ is a prime. This result includes Pei's result.

(4) Jiang and Deng [8] proved that there is no GBF of type $[n = 3, q = 2 \times 23^e]$ for each $e \geq 1$. Notice that the absolute value of $\left(\frac{3+\sqrt{-23}}{2}\right)\left(\sqrt{-23}\right)^e \in \mathbb{Z}[\zeta_{23^e}]$ is $(2 \times 23^e)^{\frac{3}{2}}$.

In this article we extend (2) and (4) to a general situation by extending the methods developed in [7,8].

We need a definition to state our result. Let $p \equiv 7 \pmod 8$ be a prime number. Then 2 splits in $\mathbb{Q}(\sqrt{-p})$. Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Q}(\sqrt{-p})$ above 2. We define t_p to be the minimal positive integer such that $\mathfrak{p}^{t_p}$ is principal. By Gauss's genus theory, t_p is odd. For more about t_p, see Remark 2. In this article, our main result is the following:

Theorem 1 *If $p \equiv 7 \pmod 8$ is a prime and the order of 2 modulo p is $\frac{p-1}{2}$, then there do not exist GBFs of type $[n = t_p, q = 2p]$. If p further satisfies $2^{p-1} \not\equiv 1 \pmod{p^2}$, then there do not exist GBFs of type $[n = t_p, q = 2p^e]$ for any $e \geq 1$.*

Remark 1 The condition $2^{p-1} \not\equiv 1 \pmod{p^2}$ is to ensure the order of 2 modulo p^e to be $\frac{\phi(p^e)}{2}$, where ϕ is Euler function, see Lemma 1. For $p < 6.7 \times 10^{15}$, $p = 3511$ is the only prime such that $p \equiv 7 \pmod 8$ and $2^{p-1} \equiv 1 \pmod{p^2}$, see [5].

Remark 2 Some basic facts about the number t_p

Of course, t_p is the order of $\mathfrak{p}$ in the class group of $\mathbb{Q}(\sqrt{-p})$. The definition of t_p does not depend on the choice of $\mathfrak{p}$. Another prime ideal above 2 is the inverse of $\mathfrak{p}$ in the class group, so they have the same order. By Gauss's genus theory or class field theory [19, Theorem 10.4(b)], the class number of $\mathbb{Q}(\sqrt{-p})$ is odd. Hence t_p is also odd. In [2, Remark 2] , Feng gave an estimate that $t_p > \frac{\log p}{\log 2} - 2$. In particular, $t_p \geq 3$, if $p \geq 23$. Feng also showed that t_p is the smallest odd positive integer such that $x^2 + py^2 = 2^{t_p+2}$ have solutions with $(x, y) \in \mathbb{Z}^2$.

We give a small table of the primes less than 200 which satisfy all conditions in Theorem 1. From the table below, it can be seen that our result includes the results of Pei and Jiang–Deng.

p	7	23	47	71	79	103	167	191	199
t_p	1	3	5	7	5	5	11	13	9

By the estimate in Remark 2 we know that $t_p = 1$ if and only if $p = 7$. So our result is different from Ikeda's.

Now we explain the condition $n = t_p$ briefly. Fix a prime p satisfying all conditions in Theorem 1. Let $q = 2p^e$ and n be a positive odd integer.

If $n < t_p$, Feng [2] actually shows that there does not exist an element in $\mathbb{Z}[\zeta_q]$ with absolute value $q^{n/2}$, so there is no GBF of type $[n, q = 2p^e]$.

If $n \geq t_p$, there exist cyclotomic integers in $\mathbb{Z}[\zeta_q]$ with absolute value $q^{n/2}$, see Lemma 3. Our result shows that there is no GBF in the case $n = t_p$. Therefore, Feng's result and our result have shown that there is no GBF of type $[n \leq t_p, q = 2p^e]$ for odd n. However, there are no nonexistence results of GBFs in the case $n > t_p$.

3 Basic facts from algebraic number theory

The methods of proving nonexistence results of GBFs almost all involve algebraic number theory, mainly the basic arithmetic (ideals, units, class groups) of cyclotomic fields and their subfields. The reader can consult [12, Chapter 2, 3] or [19, Chapter 2]. In this section, we list some facts and prove some results which we will need in the proof of our main theorem.

Let $m \not\equiv 2 \pmod 4$ be an integer and $F = \mathbb{Q}(\zeta_m)$ the cyclotomic field, where $\zeta_m = \exp\left(\frac{2\pi i}{m}\right)$. Let $\mathcal{O}_F$ be the ring of integers in F. Then for any prime number p, we know that

$$p\mathcal{O}_F = (\mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_g)^e$$

where $\mathfrak{P}_1, \mathfrak{P}_2, \cdots, \mathfrak{P}_g$ are distinct prime ideals of $\mathcal{O}_F$. If $e > 1$, we say that p ramifies in F. For each i, $\mathcal{O}_F/\mathfrak{P}_i$ is called the residue field of $\mathfrak{P}_i$, it is a finite field containing $\mathbb{F}_p$. The degree of this extension $[\mathcal{O}_F/\mathfrak{P}_i : \mathbb{F}_p]$ is called the residue class degree of $\mathfrak{P}_i/p$. Let ϕ be the Euler function. Then we have the following cyclotomic decomposition laws. For proofs, see [19, Chapter 2].

Fact 1 *Suppose $p \nmid m$ and let f be the smallest positive integer such that $p^f \equiv 1 \pmod m$. Then p splits into $g = \phi(m)/f$ distinct primes in F, each of which has residue class degree f.*

Fact 2 *We have that p ramifies in F if and only if $p|m$. If $m = p^e$ is a prime power, then $p\mathcal{O}_F = (1-\zeta_m)^{\phi(m)}$.*

We also need the following two facts about $\mathbb{Q}(\sqrt{-p})$. For proofs, see [12, Chapter 3].

Fact 3 *Let $p \equiv 3 \pmod 4$ be a prime. Then $\mathbb{Q}(\sqrt{-p}) \subset \mathbb{Q}(\zeta_p)$.*

Fact 4 *Let $p \equiv 7 \pmod 8$ be a prime. Then 2 splits in $\mathbb{Q}(\sqrt{-p})$, say $(2) = \mathfrak{p}\overline{\mathfrak{p}}$ where $\mathfrak{p} = \left(2, \frac{1+\sqrt{-p}}{2}\right)$ and $\overline{\mathfrak{p}} = \left(2, \frac{1-\sqrt{-p}}{2}\right)$ are prime ideals of $\mathbb{Q}(\sqrt{-p})$.*

Lemma 1 *Let p be an odd prime. If the order of 2 modulo p is $\frac{p-1}{2}$ and $2^{p-1} \not\equiv 1 \pmod{p^2}$. Then the order of 2 modulo p^e is $\frac{\phi(p^e)}{2}$ for each $e \geq 1$.*

Proof Let f_e be the order of 2 modulo p^e. Hence $2^{f_e} \equiv 1 \pmod p$ and $\frac{p-1}{2} | f_e$. So it remains to prove that $2^{\frac{p-1}{2}}$ has order p^{e-1}. Write $2^{\frac{p-1}{2}} = 1 + kp$ for some $k \in \mathbb{Z}$. We claim that $p \nmid k$. Otherwise we have $2^{p-1} = 1 + 2kp + k^2p^2 \equiv 1 \pmod{p^2}$. Since $p \nmid k$, the order of $1 + kp$ modulo p^e is p^{e-1} by direct computation. Therefore, $f_e = \frac{p-1}{2}p^{e-1} = \frac{\phi(p^e)}{2}$. □

In the remaining of this section, we give the basic setting which will be used in Sect. 4.

Let $e \geq 1$ be an integer. Let $p \equiv 7 \pmod 8$ be a prime such that the order of 2 modulo p is $\frac{p-1}{2}$ and $2^{p-1} \not\equiv 1 \pmod{p^2}$. Let $\zeta = \zeta_{p^e} = \exp(\frac{2\pi i}{p^e}) \in \mathbb{C}$, $L = \mathbb{Q}(\sqrt{-p})$ and $K = \mathbb{Q}(\zeta)$. Then $L \subset K$ by Fact 3. Let $\mathcal{O}_L, \mathcal{O}_K$ be the rings of integers of L and K respectively. By Fact 1 and Fact 2, we have the following prime ideal factorization.

$$p\mathcal{O}_K = (1-\zeta)^{\phi(p^e)}\mathcal{O}_K,$$
$$p\mathcal{O}_L = (\sqrt{-p}\mathcal{O}_L)^2$$

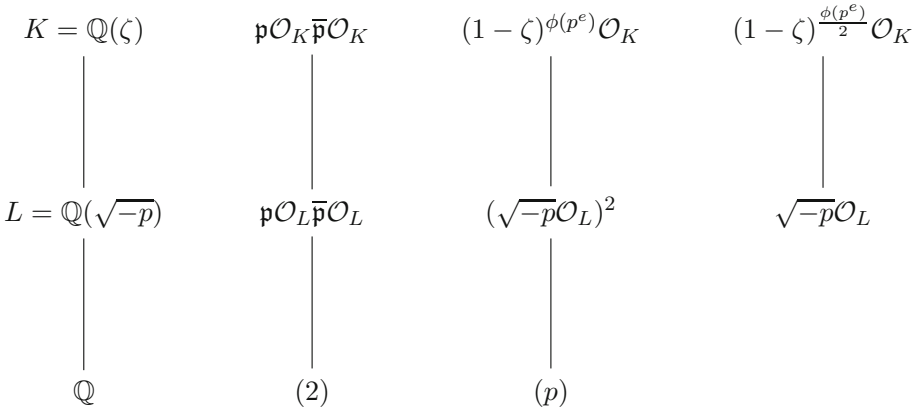
and

$$\sqrt{-p}\mathcal{O}_K = ((1-\zeta)\mathcal{O}_K)^{\frac{\phi(p^e)}{2}}.$$
$$2\mathcal{O}_L = \mathfrak{p}\mathcal{O}_L\overline{\mathfrak{p}}\mathcal{O}_L$$

where $\mathfrak{p} = \left(2, \frac{1+\sqrt{-p}}{2}\right)$ and $\overline{\mathfrak{p}} = \left(2, \frac{1-\sqrt{-p}}{2}\right)$ are prime ideals of L.

By Fact 1 and the above lemma, we know that the residue degree of 2 in $K/\mathbb{Q}$ is $\frac{\phi(p^e)}{2}$, so there are only two prime ideals above 2 in K. Hence $2\mathcal{O}_K = \mathfrak{p}\mathcal{O}_K\overline{\mathfrak{p}}\mathcal{O}_K$ where $\mathfrak{p}\mathcal{O}_K$ and $\overline{\mathfrak{p}}\mathcal{O}_K$ are prime ideals of K.

We illustrate the above decompositions by the following diagram.



Now we list a fact about the action of the Galois group on ideals. Let $\sigma_2 \in \mathrm{Gal}(K/\mathbb{Q})$ be the automorphism such that $\sigma_2(\zeta) = \zeta^2$. Since $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/p^e\mathbb{Z})^\times$, the order of 2 modulo p^e is $\frac{\phi(p^e)}{2}$ which implies that the order of σ_2 in $\mathrm{Gal}(K/\mathbb{Q})$ is $\frac{\phi(p^e)}{2}$. Since $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/p^e\mathbb{Z})^\times$ is cyclic and the degree of K/L is $\frac{\phi(p^e)}{2}$, $\mathrm{Gal}(K/L)$ is generated by σ_2. In particular, σ_2 fixes $\mathfrak{p}\mathcal{O}_K = \left(2, \frac{1+\sqrt{-p}}{2}\right)\mathcal{O}_K$ and $\overline{\mathfrak{p}}\mathcal{O}_K = \left(2, \frac{1-\sqrt{-p}}{2}\right)\mathcal{O}_K$.

The following lemma will reduce the equation $\alpha\bar{\alpha} = 2^n, \alpha \in \mathcal{O}_K$ to $\alpha\bar{\alpha} = 2^n, \alpha \in \mathcal{O}_L$, where n is a positive integer. It is a slight refined version of [2, Lemma 2.2].

Lemma 2 *If $\alpha\overline{\alpha} = 2^n$ for some $\alpha \in \mathcal{O}_K$, then there exists a unique $i \in \{0, 1, \ldots, p^e - 1\}$ such that $\alpha\zeta^{-i} \in \mathcal{O}_L$.*

Proof By the above argument, we know that σ_2 fix $\mathfrak{p}\mathcal{O}_K$ and $\overline{\mathfrak{p}}\mathcal{O}_K$. Since the prime ideal factors of α are $\mathfrak{p}\mathcal{O}_K$ and $\overline{\mathfrak{p}}\mathcal{O}_K$, we have an equality of ideals of $\mathcal{O}_K$:

$$(\sigma_2(\alpha)) = (\alpha).$$

Then there is a unit u of $\mathcal{O}_K$ such that $\sigma_2(\alpha) = u\alpha$. Since $\mathrm{Gal}(K/\mathbb{Q})$ is abelian, we have

$$2^n = \sigma_2(2^n) = \sigma_2(\alpha\overline{\alpha}) = \sigma_2(\alpha)\sigma_2(\overline{\alpha}) = \sigma_2(\alpha)\overline{\sigma_2(\alpha)} = u\alpha\overline{u\alpha} = 2^n u\bar{u}.$$

Then $u\bar{u} = 1$. By the fact that $\mathrm{Gal}(K/\mathbb{Q})$ is abelian again, we have $\sigma(u)\overline{\sigma(u)} = 1$ for every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. By a well-known fact [19, Lemma 1.6], u is a root of unity. Hence there is a unique $i \in \{0, 1, \ldots, p^e - 1\}$ such that $u = \pm\zeta^i$. Let $\beta = \alpha\zeta^{-i}$. Then

$$\sigma_2(\beta) = \alpha(\pm\zeta^{-i}),$$

so $\sigma_2(\beta^2) = \beta^2$. Since L is the fixed field of σ_2, this implies $\beta^2 \in \mathcal{O}_L$. But $[K : L] = \frac{p-1}{2}$ is odd, so $\beta = \alpha\zeta^{-i} \in \mathcal{O}_L$. □

Remark 3 The equation $2^t = x\overline{x}$ for $x \in \mathcal{O}_L$ has explicit solutions, where $t = t_p$ is the order of $\mathfrak{p}$ in the class group of L. Let $\gamma \in \mathcal{O}_L$ such that $\mathfrak{p}^t = (\gamma)$. Note that $\pm\gamma$ and $\pm\bar{\gamma}$ have absolute value $2^{\frac{t}{2}}$. On the other hand, if $x \in \mathcal{O}_L$ has absolute value $2^{\frac{t}{2}}$, then we have

$$(x)(\overline{x}) = (2^t) = \mathfrak{p}^t\overline{\mathfrak{p}}^t$$

as ideals of $\mathcal{O}_L$. Then $(x) = \mathfrak{p}^a\overline{\mathfrak{p}}^{t-a}$ for some $a \in \{0, 1, \ldots, t\}$. Note that if $0 < a < t$, $\mathfrak{p}^a\overline{\mathfrak{p}}^{t-a}$ is not principal by definition of t. Since (x) is principal, we have that (x) must be $\mathfrak{p}^t$ or $\overline{\mathfrak{p}}^t$. Because the units of $\mathcal{O}_L$ are ± 1, we have $x = \pm\gamma$ or $\pm\bar{\gamma}$. Therefore, the elements in $\mathcal{O}_L$ with absolute value $2^{\frac{t}{2}}$ are $\pm\gamma$ and $\pm\bar{\gamma}$.

4 Proof of Theorem 1

In this section, we give the proof of Theorem 1.

Now assume that f is a GBF from $\mathbb{Z}_q^t$ to $\mathbb{Z}_q$, where $t = t_p, q = 2p^e$. Then $F(\lambda) \in \mathcal{O}_K$ has absolute value $q^{\frac{t}{2}}$. We will finally get a contradiction.

Lemma 3 *$F(\lambda)$ must be one of the following elements*

$$(\sqrt{-p})^{et} \cdot \gamma \cdot (\pm\zeta^i)$$

or

$$(\sqrt{-p})^{et} \cdot \overline{\gamma} \cdot (\pm\zeta^i),$$

where $i \in \{0, 1, \ldots, p^e - 1\}$. In particular, $F(\lambda) \notin (2)\mathcal{O}_K$.

Proof It is easily seen that every element above has absolute value $q^{\frac{t}{2}}$.

By the prime ideal factorizations we have

$$(F(\lambda)\overline{F(\lambda)}) = (q^t) = (2^t p^{et})\mathcal{O}_K = (\mathfrak{p}\mathcal{O}_K)^t(\overline{\mathfrak{p}}\mathcal{O}_K)^t(1-\zeta)^{\phi(p^e)et}.$$

Note that $\overline{(1-\zeta)} = (1-\zeta)$, we know that the exact power of $(1-\zeta)$ in $(F(\lambda))$ must be $\frac{\phi(p^e)et}{2}$, so $(1-\zeta)^{\frac{\phi(p^e)et}{2}} = (\sqrt{-p})^{et} | (F(\lambda))$ as ideals of $\mathcal{O}_K$. Hence $\alpha := \frac{F(\lambda)}{\sqrt{-p}^{et}} \in \mathcal{O}_K$ and $\alpha\overline{\alpha} = 2^t$. Then by Lemma 2, we know that there is a unique $i \in \{0, 1, \ldots, p^e - 1\}$ such that $\beta := \alpha\zeta^{-i} \in \mathcal{O}_L$. So $\beta\overline{\beta} = 2^t$.

By Remark 3, we have that $\beta = \pm\gamma$ or $\pm\overline{\gamma}$. Hence

$$F(\lambda) = (\sqrt{-p})^{et} \cdot \alpha = (\sqrt{-p})^{et} \cdot \beta\zeta^i = (\sqrt{-p})^{et} \cdot \gamma \cdot (\pm\zeta^i)$$

or

$$(\sqrt{-p})^{et} \cdot \overline{\gamma} \cdot (\pm\zeta^i)$$

for some $i \in \{0, 1, \ldots, p^e - 1\}$. □

Lemma 4 *If $v \in \mathbb{Z}_q^t$ is an element of order 2, then for every $\lambda \in \mathbb{Z}_q^t$,*

$$F(\lambda) = \pm F(\lambda + v).$$

Proof As v is of order 2, for $x \in \mathbb{Z}_q^t$, we have $\zeta_q^{x\cdot v} = \pm 1$. So

$$F(\lambda) + F(\lambda + v) = \sum_{x \in \mathbb{Z}_q^t} \zeta_q^{f(x) - x\cdot\lambda}(1 + \zeta_q^{-x\cdot v}) \in (2) = \mathfrak{p}\mathcal{O}_K \cap \overline{\mathfrak{p}}\mathcal{O}_K,$$

or said differently,

$$(2)|(F(\lambda)+F(\lambda+v))$$

as ideals of $\mathcal{O}_K$.

Then $F(\lambda)\in\mathfrak{p}\mathcal{O}_K \iff F(\lambda+v)\in\mathfrak{p}\mathcal{O}_K$. By the above Lemma, we have $F(\lambda+v)=F(\lambda)\cdot(\pm\zeta^i)$ for some $i\in\{0,1,\ldots,p^e-1\}$. Then

$$F(\lambda)+F(\lambda+v)=F(\lambda)(1\pm\zeta^i).$$

Note that if $i\neq 0$, (2) and $(1\pm\zeta^i)$ are coprime ideals. So $(2)|(F(\lambda))$. This contradicts to Lemma 3. Therefore, $i=0$. □

The above proof is essentially the same as in [7, Lemma 3] and [8, Lemma 8].

Let G be the Sylow-2 subgroup of $\mathbb{Z}_q^t$. Then $G\cong\mathbb{F}_2^t$. For every $v\in G\setminus\{0\}$, define

$$N_v:=\{\lambda\in\mathbb{Z}_q^t|F(\lambda)=F(\lambda+v)\}$$

and

$$M_v:=\{\lambda\in\mathbb{Z}_q^t|F(\lambda)=-F(\lambda+v)\}.$$

By Lemma 4, $\mathbb{Z}_q^t=N_v\sqcup M_v$ (the symbol $\sqcup$ means disjoint union) and $|N_v|+|M_v|=q^t$.

Lemma 5 *We have* $|N_v|=|M_v|=\frac{q^t}{2}$ *for each* $v\in G\setminus\{0\}$.

Proof We need the following well-know orthogonality relations,

$$\sum_{x\in\mathbb{Z}_q^t}{\zeta_q}^{x\cdot\alpha}=\begin{cases}0 & \text{if } \alpha\neq 0,\\ q^t & \text{if } \alpha=0.\end{cases}$$

Then for each $v\in G\setminus\{0\}$, we have

$$\begin{aligned}\sum_{\lambda}F(\lambda)\overline{F(\lambda+v)}&=\sum_{\lambda}\left(\sum_{x}{\zeta_q}^{f(x)}\cdot{\zeta_q}^{-x\cdot\lambda}\right)\left(\sum_{y}{\zeta_q}^{-f(y)}\cdot{\zeta_q}^{y\cdot(\lambda+v)}\right)\\&=\sum_{x}\sum_{y}{\zeta_q}^{f(x)-f(y)}\cdot{\zeta_q}^{y\cdot v}\sum_{\lambda}{\zeta_q}^{-\lambda(x-y)}\\&=q^t\sum_{x}\sum_{y=x}{\zeta_q}^{f(x)-f(y)}\cdot{\zeta_q}^{y\cdot v}=q^t\sum_{x}{\zeta_q}^{x\cdot v}=0.\end{aligned}$$

By the definition of GBF, we have that $F(\lambda)\overline{F(\lambda)}=q^t$ for each λ. So for each $v\in G\setminus\{0\}$,

$$0=\sum_{\lambda\in N_v}F(\lambda)\overline{F(\lambda+v)}+\sum_{\lambda\in M_v}F(\lambda)\overline{F(\lambda+v)}=q^t(|N_v|-|M_v|).$$

Hence, $|N_v|=|M_v|$. Also we know that $|N_v|+|M_v|=q^t$. Therefore, $|N_v|=|M_v|=\frac{q^t}{2}$. □

If $t=1$, then there is only one 2−order element v in $\mathbb{Z}_q$. Note that if $\lambda\in N_v$, then $\lambda+v\in N_v$. Hence 2 divides $|N_v|$. But $|N_v|=\frac{q}{2}=p^e$ is odd. This is a contradiction. So there do not exist GBFs from $\mathbb{Z}_q$ to $\mathbb{Z}_q$.

As we have pointed out in Sect. 2, this result and the above proof are due to Ikeda [7].

In the remaining part of the proof, we assume $t\geq 3$ so that $|G|=2^t\geq 8$. Consider the following 2^{2^t-1} subsets of $\mathbb{Z}_q^t$:

$$\bigcap_{v\in G\setminus\{0\}}X_v$$

where $X_v=N_v$ or M_v. By Lemma 4, we have the following proposition.

Proposition 1 *$\mathbb{Z}_q^t$ is a disjoint union of these 2^{2^t-1} subsets.*

The following lemmas will tell us that among the 2^{2^t-1} sets there are 2^t nonempty sets at most.

Lemma 6 *If $u, v, w \in G \setminus \{0\}$ satisfy $u + v + w = 0$, then we have*

$$N_u \cap N_v \cap M_w = N_u \cap M_v \cap N_w = M_u \cap N_v \cap N_w = M_u \cap M_v \cap M_w = \emptyset.$$

Proof We only need the fact $F(\lambda) \notin 2\mathcal{O}_K$, so the proof below is essentially the same as the case $p = 23$ in [8, Lemma 11].

The condition implies that u, v, w are pairwise different. Note that

$$\begin{aligned}
&\lambda \in N_u \cap N_v \cap M_w \\
\iff\ &\lambda + u \in N_u \cap M_v \cap N_w \\
\iff\ &\lambda + v \in M_u \cap N_v \cap N_w \\
\iff\ &\lambda + w \in M_u \cap M_v \cap M_w.
\end{aligned}$$

So it is enough to prove $M_u \cap M_v \cap M_w = \emptyset$. By considering the surjective group homomorphism

$$\begin{aligned}
(\cdot u) : \mathbb{Z}_q^t &\longrightarrow \left\{0, \frac{q}{2}\right\} \subset \mathbb{Z}_q \\
y &\mapsto y \cdot u,
\end{aligned}$$

we know that there are half elements of $\mathbb{Z}_q^t$ satisfy $y \cdot u = 0$ and half elements of $\mathbb{Z}_q^t$ satisfy $y \cdot u \neq 0$. Note that $\zeta_q^{y \cdot u} = 1$ if $y \cdot u = 0$ and $\zeta_q^{y \cdot u} = -1$ if $y \cdot u \neq 0$.

Now take an element $\lambda \in M_u \cap M_v \cap M_w$. For simplicity, let $\sum_y = \sum_y \zeta_q^{f(y)-\lambda \cdot y}$. Then

$$\begin{aligned}
F(\lambda) &= \sum_{y \in \mathbb{Z}_q^t} = \sum_{y \cdot u = 0} + \sum_{y \cdot u \neq 0} \\
&= -F(\lambda + u) = -\sum_{y \cdot u = 0} + \sum_{y \cdot u \neq 0}.
\end{aligned}$$

So we get

$$0 = \sum_{y \cdot u = 0} = \sum_{y \cdot u = 0, y \cdot v = 0} + \sum_{y \cdot u = 0, y \cdot v \neq 0}.$$

Similarly, we have

$$0 = \sum_{y \cdot v = 0} = \sum_{y \cdot u = 0, y \cdot v = 0} + \sum_{y \cdot u \neq 0, y \cdot v = 0}.$$

From $F(\lambda) = -F(\lambda + w)$, we have

$$0 = \sum_{y \cdot w = 0},$$

and

$$F(\lambda) = \sum_{y \cdot w \neq 0} = \sum_{y \cdot (u+v) \neq 0} = \sum_{y \cdot u = 0, y \cdot v \neq 0} + \sum_{y \cdot u \neq 0, y \cdot v = 0} = -2 \sum_{y \cdot u = 0, y \cdot v = 0} \in 2\mathcal{O}_K.$$

This contradicts to Lemma 3. So $M_u \cap M_v \cap M_w = \emptyset$. □

Lemma 7 *Let $\bigcap_{a\in G\setminus\{0\}} X_a$ be a subset of $\mathbb{Z}_q^t$ where $X_a = N_a$ or M_a. If $\{a \in G | X_a = N_a\} \cup \{0\}$ is not a subgroup of G with index 1 or 2, then $\bigcap_{a\in G\setminus\{0\}} X_a = \emptyset$.*

Proof If $A := \{a \in G | X_a = N_a\} \cup \{0\}$ is not a subgroup, then there are two different elements $u, v \in A \setminus \{0\}$ such that $u + v \notin A$. Hence $X_u = N_u$, $X_v = N_v$ and $X_{u+v} = M_{u+v}$. Then by the above Lemma, we have

$$\bigcap_{a\in G\setminus\{0\}} X_a \subset N_u \cap N_v \cap M_{u+v} = \emptyset.$$

Recall $G \cong \mathbb{F}_2^t$. If the index of A in G is larger than 2, then $\dim_{\mathbb{F}_2} A \leq t-2$ as a subspace of G. Then there is a subspace B such that $A \cap B = \{0\}$ and $\dim_{\mathbb{F}_2} B \geq 2$. Take two different elements $u, v \in B \setminus \{0\}$. Then $u + v \in B \setminus \{0\}$. So u, v and $u + v$ are not in A. Hence $X_u = M_u$, $X_v = M_v$ and $X_{u+v} = M_{u+v}$. Then by the above Lemma, we have

$$\bigcap_{a\in G\setminus\{0\}} X_a \subset M_u \cap M_v \cap M_{u+v} = \emptyset.$$

□

Let Γ be the set of subgroups of G with index 2. Since $G \cong \mathbb{F}_2^t$, so $|\Gamma| = 2^t - 1$ by basic linear algebra.

In virtue of Lemma 7, we define

$$N_G := \bigcap_{v\in G\setminus\{0\}} N_v$$

and

$$N_H := \left(\bigcap_{v\in H\setminus\{0\}} N_v\right) \bigcap \left(\bigcap_{u\notin H} M_u\right),$$

for each $H \in \Gamma$.

Proposition 2 *We have the decomposition*

$$\mathbb{Z}_q^t = \left(\bigsqcup_{H\in\Gamma} N_H\right) \bigsqcup N_G.$$

For each $v \in G \setminus \{0\}$,

$$N_v = \bigsqcup_{\Gamma\ni H\ni v} N_H \bigsqcup N_G.$$

Proof By Proposition 1, we have that $\mathbb{Z}_q^t$ is a disjoint union of 2^{2^t-1} subsets, where each subset is of the form $\bigcap_{v\in G\setminus\{0\}} X_v$ with $X_v = N_v$ or M_v. By Lemma 7, the only possible nonempty sets are N_G and N_H where $H \in \Gamma$. So $\mathbb{Z}_q^t = \left(\bigsqcup_{H\in\Gamma} N_H\right) \bigsqcup N_G$.

Since $N_v = N_v \cap \mathbb{Z}_q^t$, the second statement follows by the first statement. □

We are now in a position to give a proof of Theorem 1.

Proof of Theorem 1 By Proposition 2, we have the following equation

$$q^t = \sum_{H\in\Gamma} |N_H| + |N_G|. \tag{1}$$

For each $v \in G \setminus \{0\}$, by Lemma 5 we have

$$|N_v| = \frac{q^t}{2} = \sum_{\Gamma \ni H \ni v} |N_H| + |N_G|.$$

Sum the latter $2^t - 1$ equations, we have

$$\begin{aligned}(2^t-1)\frac{q^t}{2} &= \sum_{v\in G\setminus\{0\}} \sum_{\Gamma \ni H \ni v} |N_H| + (2^t-1)|N_G| \\ &= \sum_{H\in\Gamma} \left(\sum_{v\in H\setminus\{0\}} 1 \right) |N_H| + (2^t-1)|N_G| = (2^{t-1}-1) \sum_{H\in\Gamma} |N_H| + (2^t-1)|N_G|.\end{aligned}$$

Hence

$$(2^t-1)\frac{q^t}{2} = (2^{t-1}-1) \sum_{H\in\Gamma} |N_H| + (2^t-1)|N_G|. \tag{2}$$

Combining (1) and (2), we get

$$(2^t-1)\frac{q^t}{2} = (2^{t-1}-1)(q^t - |N_G|) + (2^t-1)|N_G|.$$

Then

$$|N_G| = p^{te}.$$

In particular, N_G is not empty. However, if $\lambda \in N_G$, then we have $\lambda + v \in N_G$ for all $v \in G$, so 2^t divides $|N_G| = p^{te}$. This contradiction shows that there do not exist GBFs of type $[t = t_p, q = 2p^e]$ for any $e \geq 1$, and this completes the proof of Theorem 1.

□

5 Nonexistence of GBFs from $\mathbb{Z}_2^n$ to $\mathbb{Z}_m$

A function f from $\mathbb{Z}_2^n$ to $\mathbb{Z}_m$ is called a GBF if the equality

$$|F(\lambda)| := \left| \sum_{x\in\mathbb{Z}_2^n} \zeta_m^{f(x)} (-1)^{x\cdot\lambda} \right| = 2^{\frac{n}{2}}$$

holds for every $\lambda \in \mathbb{Z}_2^n$, where $x \cdot \lambda$ is the standard dot product.

There are many constructions of this type GBF, see [18]. For nonexistence results, a good reference is [10], where Liu–Feng–Feng proved many nonexistence results for GBFs of this type by showing that there are no cyclotomic integers with prescribed absolute values.

We get a nonexistence result in the case that there are cyclotomic integers with prescribed absolute values.

If $p \equiv 7 \pmod 8$ is a prime. Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Q}(\sqrt{-p})$ above 2. We define t_p to be the minimal positive integer such that $\mathfrak{p}^{t_p}$ is principal.

Theorem 2 *If $p \equiv 7 \pmod 8$ is a prime and the order of 2 modulo p is $\frac{p-1}{2}$, then there do not exist GBFs from $\mathbb{Z}_2^{t_p}$ to $\mathbb{Z}_{2p}$. If p further satisfies $2^{p-1} \not\equiv 1 \pmod{p^2}$, then there do not exist GBFs from $\mathbb{Z}_2^{t_p}$ to $\mathbb{Z}_{2p^e}$ for any $e \geq 1$.*

The proof of Theorem 2 is as same as the one of Theorem 1. So we only give a sketch:

Proof Assume that f is a GBF from $\mathbb{Z}_2^{t_p}$ to $\mathbb{Z}_{2p^e}$. Then $F(\lambda)\overline{F(\lambda)} = 2^{t_p}$.

Firstly, by tracing the arguments in Sect. 3 and Lemma 3, one can prove that $F(\lambda)$ must be one of the following elements

$$\gamma \cdot (\pm\zeta_{p^e}^i)$$

or

$$\overline{\gamma} \cdot (\pm\zeta_{p^e}^i),$$

where $\gamma \in \mathbb{Q}(\sqrt{-p})$ is a generator of $\mathfrak{p}^{t_p}$ and $i \in \{0, 1, \cdots, p^e - 1\}$.

Secondly, for any $v \in \mathbb{Z}_2^t \setminus \{0\}$, define $N_v := \{\lambda \in \mathbb{Z}_2^{t_p} | F(\lambda) = F(\lambda + v)\}$, $M_v := \{\lambda \in \mathbb{Z}_2^{t_p} | F(\lambda) = -F(\lambda + v)\}$ and $N_{all} := \bigcap_{v \in \mathbb{Z}_2^{t_p} \setminus \{0\}} N_v$. One can use the above form of $F(\lambda)$ and same arguments in Sect. s4 to formulate and prove analogues of Lemmas 4, 5, 6, 7, and Propositions 1, 2.

Finally, by a similar computation as in the proof of Theorem 1, on one hand one can prove that $|N_{all}| = 1$, on the other hand 2^{t_p} divides $|N_{all}|$. This contradiction shows that there do not exist GBFs from $\mathbb{Z}_2^{t_p}$ to $\mathbb{Z}_{2p^e}$. □

6 Conclusion and future work

In this article we give some new nonexistence results of GBFs under the condition that there exist cyclotomic integers with prescribed absolute values. The nonexistence problem is far from solved. Our future work goes toward the case when the order of 2 modulo p is less than $\frac{p-1}{2}$.

Acknowledgements The authors thank the anonymous referees for many helpful corrections and suggestions, many of which have been incorporated into this version of the paper. The authors are indebted to the editor Alexander Pott for his thorough careful reading and valuable suggestions. The authors also thank Yupeng Jiang, Chang Lv and Jiangshuai Yang for helpful discussions. The work of this paper was supported by the NNSF of China (Grant No. 11471314) and the National Center for Mathematics and Interdisciplinary Sciences, CAS.

References

1. Dillon J.F.: Elementary Hadamard difference sets. PhD dissertation, University of Maryland (1974).
2. Feng K.: Generalized bent functions and class group of imaginary quadratic fields. Sci China Ser. A **44**, 562–570 (2001).
3. Feng K., Liu F.: New results on the nonexistence of generalized bent functions. IEEE Trans. Inf. Theory **49**, 3066–3071 (2003).
4. Feng K., Liu F.: Non-existence of some generalized bent functions. Acta Math. Sin. (Engl. Ser.) **19**, 39–50 (2003).
5. Francois D.G., Dominic K.: A Wieferich prime search up to 6.7×10^{15}. J. Integer Seq. **14**, 1–14 (2011).
6. Fröhlich A., Taylor M.J.: Algebraic Number Theory. Cambridge University Press, Cambridge (1991).
7. Ikeda M.: A remark on the non-existence of generalized bent functions. Lect. Notes Pure Appl. Math. **204**, 109–119 (1999).
8. Jiang Y., Deng Y.: New results on nonexistence of generalized bent functions. Des. Codes Cryptogr. **75**, 375–385 (2015).
9. Kumar P.V., Scholtz R.A., Welch L.R.: Generalized bent functions and their properties. J. Comb. Theory Ser. A **40**, 90–107 (1985).
10. Liu H., Feng K., Feng R.: Nonexistence of generalized bent functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_m$. Des. Codes Cryptogr. (2016). doi:10.1007/s10623-016-0192-9.

11. Logachev O.A., Salnikov A.A., Yashchenko V.V.: Bent functions over a finite abelian group. Discret. Math. Appl. **7**, 547–564 (1997).
12. Marcus D.A.: Number Fields. Springer, Berlin (1997).
13. Olsen J.D., Scholtz R.A., Welch L.R.: Bent-function sequences. IEEE Trans. Inf. Theory **28**, 858–864 (1982).
14. Pei D.: On nonexistence of generalized bent functions. Lect. Notes Pure Appl. Math. **141**, 165–172 (1993).
15. Poinsot L.: Bent functions on a finite nonabelian group. J. Discret. Math. Sci. Cryptogr. **9**, 349–364 (2006).
16. Rothaus O.S.: On "bent" functions. J. Comb. Theory. A **20**, 300–305 (1976).
17. Solodovnikov V.I.: Bent functions from a finite abelian group to a finite abelian group. Diskret. Mat. **14**, 99–113 (2002).
18. Stănică P., Martinsen T., Gangopadhyay S., Brajesh K.S.: Bent and generalized bent Boolean functions. Des. Codes Cryptogr. **69**, 77–94 (2013).
19. Washington L.C.: Introduction to Cyclotomic Fields, 2nd edn. Graduate Texts in Mathematics. Springer, New York (1997).
20. Xu B.: Bentless and nonlinearity of functions on finite groups. Des. Codes Cryptogr. (2014). doi:10.1007/s10623-014-9968-y.