New results on nonexistence of generalized bent functions

Yupeng Jiang and Yingpu Deng

Key Laboratory of Mathematics Mechanization,
Academy of Mathematics and Systems Science,
Chinese Academy of Sciences, Beijing 100190, P.R. China
E-mail: {jiangyupeng,dengyp}@amss.ac.cn

Abstract

We get two kinds of new results on nonexistence of generalized bent function. The first one is Based on Feng's results by using Schmidt's field descent method. For the second kind, considering special property of the field $\mathbb{Q}(\zeta_{23^e})$, We get new nonexistence results of generalized bent functions with type $[3, 2 \cdot 23^e]$.

Keywords: Field Descent Method, Generalized Bent Functions

1 Introduction

Let q and n be positive integers, $q \geq 2$, $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$, $\zeta_q = e^{\frac{2\pi i}{q}}$. A function $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ is called a generalized bent function(GBF) if the equality

$$\left| \sum_{x \in \mathbb{Z}_q^n} \zeta_q^{f(x) - x \cdot \lambda} \right| = q^{\frac{n}{2}}$$

holds for every $\lambda \in \mathbb{Z}_q^n$, where $x \cdot y$ stands for the dot product. We call $[n, q]$ the type of such function f. Denote $F(\lambda) = \sum_{x \in \mathbb{Z}_q^n} \zeta_q^{f(x) - x \cdot \lambda}$. The above equation is

$$F(\lambda)\overline{F(\lambda)} = q^n.$$

If f is a GBF, then it is easy to prove that

$$\sum_{\lambda \in \mathbb{Z}_q^n} F(\lambda)\overline{F(\lambda + \mu)} = \begin{cases} 0 & \text{if } \mu \neq 0, \\ q^{2n} & \text{if } \mu = 0. \end{cases}$$

The conception of a bent function (for $q = 2$) was presented by Rothaus [15] in 1976, and generalized by Kumar et al. [10] in 1985. Being a family of functions with maximum nonlinearity, bent functions draw much attention and are widely investigated. They have been extensively studied for their applications in cryptography, coding theory and combinatorial design. In a cryptography system, functions with large nonlinearity values are usually employed to resist linear crpto-analysis and correlation-attack, so the security of system can be increased. In a code-division multiple-access communication system, we need a family of periodic sequences which have small correlation values between distinct codes and small auto-correlation values to distinguish users and provide self-synchronization capacity. Bent sequences generated by bent functions have such properties and are widely used [13]. Bent functions lead to vectors with maximum distance from the first order Reed-Muller code. In combinatorial design, Dillon [3] showed that bent functions are the characteristic fucntions of elementary Hadarmard difference sets.

Rothaus proved that there exists a bent function of type $[n, 2]$ if and only if n is even. Later, Kumar et al. constructed a GBF for all cases of even n or $q \not\equiv 2 \pmod 4$. There are many materials about the construction of bent functions, for a survey see [8]. On the other hand, to prove the nonexistence of some kind of GBF is also important. So far there is no GBF constructed in the case n is odd and $q \equiv 2 \pmod 4$. Several nonexistence results of GBF have been proved.

Let $q = 2N$, then N is odd. There are no GBF of the following types.

(1) [10] There exists an integer $s \geq 1$ such that

$$2^s \equiv -1 \pmod N.$$

(2) [14] $n = 1$, $N = 7$.

(3) [2] $n = 1$, $N = p^e$ where $e \geq 1$, p is a prime, $p \equiv 7 \pmod 8$ and $p \neq 7$.

(4) [9] $n = 1$, N has prime factorization that $N = \prod_{i=1}^{t} p_i^{e_i}$ and for each i there exists $s_i \leq 1$ such that

$$p_i^{s_i} \equiv -1 \pmod{\frac{N}{p_i^{e_i}}}.$$

Feng and his co-workers also get nonexistence results. We give in the following. All the cases p_i is prime, and n satisfies some condition similar to the first case.

(a) [4] $N = p^e,\ p \equiv 7 \pmod 8$ and $n < \frac{m}{s}$ where m is the smallest odd positive integer such that $x^2 + py^2 = 2^{m+2}$ has $\mathbb{Z}$-solution and $s = \frac{\phi(N)}{2f}$, f is the order of 2 $\pmod N$.

(b) [4] $N = p_1^{e_1}p_2^{e_2},\ p_1 \equiv 3 \pmod 4,\ p_2 \equiv 5 \pmod 8,\ (\frac{p_1}{p_2}) = -1$.

(c) [5] $N = p_1^{e_1}p_2^{e_2},\ p_1 \equiv 3 \pmod 4,\ p_2 \equiv 2^\lambda + 1 \pmod{2^{\lambda+1}},\ (\frac{p_1}{p_2}) = -1,\ (\frac{2}{p_2})_4 \neq 1$.

(d) [11] $N = p_1p_2,\ p_1 \equiv p_2 \equiv 7 \pmod 8,\ (\frac{p_1}{p_2}) = -1$.

(e) [11] $N = p_1p_2,\ p_1 \equiv 3 \pmod 8,\ p_2 \equiv 7 \pmod 8,\ (\frac{p_1}{p_2}) = -1$.

(f) [11] $N = p_1p_2,\ p_1 \equiv 3 \pmod 8,\ p_2 \equiv 7 \pmod 8,\ (\frac{p_2}{p_1}) = -1$.

(g) [6] $N = p_1p_2,\ p_1 \equiv 2^\lambda + 1 \pmod{2^{\lambda+1}},\ \lambda \geq 3,\ p_2 \equiv 7 \pmod 8,\ (\frac{p_1}{p_2}) = 1,\ (\frac{p_2}{p_1})_4 \neq 1,\ (\frac{2}{p_2}) \neq 1$.

(h) [6] $N = p_1p_2,\ p_1 \equiv 5 \pmod 8,\ p_2 \equiv 3 \pmod 4,\ (\frac{p_1}{p_2}) = 1,\ (\frac{p_2}{p_1})_4 \neq 1$.

In fact, Feng proved there is no element in the ring $\mathbb{Z}[\zeta_q]$ with magnitude $q^{\frac{n}{2}}$. This gives a chance to use Schmidt's field descent method [16] to get new result on nonexistence of GBF.

We also develop a method to prove that there is no GBF with type $[3, 2\cdot 23^e]$. As there are elements in $\mathbb{Z}[\zeta_{23^e}]$ with magnitude $(2\cdot 23^e)^{\frac{3}{2}}$, Feng's method doesn't work here.

2 Results based on Feng's

In this section, we introduce the field descent method in [16] and then to get new results of nonexistence of generalized bent functions.

2.1 Field descent method

Definition 1. *Let m, n be positive integers, and let $m = \prod_{i=1}^t p_i^{c_i}$ be the prime power decomposition of m. For each prime divisor q of n let*

$$m_q := \begin{cases} \prod_{p_i \neq q} p_i & \text{if } m \text{ is odd or } q = 2, \\ 4\prod_{p_i \neq 2,\ q} p_i & \text{otherwise.} \end{cases}$$

Let $\mathcal{D}(n)$ be the set of prime divisors of n. Define $F(m,n) = \prod_{i=1}^t p_i^{b_i}$ to be the minimum multiple of $\prod_{i=1}^t p_i$ such that for every pair (i,q), $i \in \{1,\ldots,t\}$, $q \in \mathcal{D}(n)$, at least one of the following conditions is satisfied:

(a) $q = p_i$ *and* $(p_i, b_i) \neq (2,\ 1)$,

(b) $b_i = c_i$,

(c) $q \neq p_i$ *and* $q^{O_{m_q}(q)} \not\equiv 1 \pmod{p_i^{b_i+1}}$.

Here $O_{m_q}(q)$ *means the order of* q *modulo* m_q.

According to the definition, we know that for fixed m, $F(m,n)$ depends only on the set $\mathcal{D}(n)$, so we have $F(m,\ n) = F(m, n^t)$ for $\forall\ t \geq 1$. b_i is the smallest integer satisfies at least one of the three conditions for all $q \in \mathcal{D}(n)$ and $1 \leq b_i \leq c_i$.

We have the following important theorem.

Theorem 1. *Assume* $X\overline{X} = n$ *for* $X \in \mathbb{Z}[\zeta_m]$, *where* n *and* m *are positive integers. Then*

$$X\zeta_m^j \in \mathbb{Z}[\zeta_{F(m,n)}]$$

for some $j \in \mathbb{Z}$.

As $X\zeta_m^j\overline{X\zeta_m^j} = X\overline{X} = n$, this theorem says that if there is an element in $\mathbb{Z}[\zeta_m]$ satisfying $X\overline{X} = n$, then there is an element in $\mathbb{Z}[\zeta_{F(m,n)}]$ with the same magnitude. We can use this to get new results on non-existence of GBF.

2.2 New nonexistence results

First we introduce a lemma in [11]. For a prime p and positive integers e, n, we use $p^e \| n$ means $p^e | n$ and $p^{e+1} \nmid n$.

Lemma 1. *Soppose that* $K = \mathbb{Q}(\zeta_N)$, $2 \nmid N$ *and*

(1) p *is an odd prime factor of* N *and* $p^m \| N$,

(2) there exists an integer s *such that* $p^s \equiv -1 \pmod{\frac{N}{p^m}}$.

If there exists $\alpha \in \mathbb{Z}[\zeta_N]$ *such that* $\alpha\bar{\alpha} = pM (M \in \mathbb{Z})$, *then there exists* $\beta \in \mathbb{Z}[\zeta_N]$ *such that* $\beta\bar{\beta} = M$.

In the same article, the authors gave examples that there is no GBF with type $[n, 2p_1p_2](n = 1, 3, 5)$ with (p_1, p_2) have the following values $(p_1, p_2) = (239, 383), (263, 463), (263, 479), (311, 359), (359, 191), (367, 383), (463, 479), (479, 271)$. All are in the class (d) of §1.

Let $N = p_1p_2$, $K = \mathbb{Q}(\zeta_N)$, As all the above cases have Legendre symbol $(\frac{p_1}{p_2}) = -1$, so that $p_1^s \equiv -1 \pmod{p_2}$ for some integer s. If there is a GBF with type $[n, 2p_1p_2]$, then there exists

$$\alpha \in \mathbb{Z}[\zeta_N], \quad \alpha\bar{\alpha} = (2N)^n.$$

By the above lemma, there exists

$$\beta \in \mathbb{Z}[\zeta_N], \quad \beta\bar{\beta} = (2p_2)^n.$$

They in fact proved that(Theorem2.1 in [11]) for every

$$\alpha \in \mathbb{Z}[\zeta_N], \quad \alpha\bar{\alpha} \neq (2p_2)^n, \quad n = 1, 3, 5 \tag{$*$}$$

Theorem 2. *Let n, (p_1, p_2) be as the above, there is no GBF with type $[n, 2p_1^e p_2]$ for all $e \geq 1$.*

Proof. Let $M = p_1^e p_2$, If there exists GBF with type $[n, 2M]$, we have

$$\gamma \in \mathbb{Z}[\zeta_M], \qquad \gamma\bar{\gamma} = (2M)^n.$$

Using the above lemma repeatedly, we can get

$$\delta \in \mathbb{Z}[\zeta_M], \qquad \delta\bar{\delta} = (2p_2)^n.$$

By Theorem 1, there is

$$\beta \in \mathbb{Z}[\zeta_{F(M,(2p_2)^n)}], \qquad \beta\bar{\beta} = (2p_2)^n.$$

We are going to prove that $F(M, (2p_2)^n) = p_1p_2$, so a contradiction to $(*)$. As $p_2 \| M$, by the definition of $F(M, (2p_2)^n)$, $p_2 \| F(M, (2p_2)^n)$. we only need to determine the power index of p_1. Since M is odd, we have

$$M_2 = p_1p_2, \qquad M_{p_2} = p_1.$$

Using a computer, we have

$$p_1 \| 2^{O_{M_2}(2)} - 1, \quad p_1 \| p_2^{O_{M_{p_2}}(p_2)} - 1$$

for all the above (p_1, p_2), so $F(M, (2p_2)^n) = p_1p_2$. Here we only give the calculation for the first pair $(p_1, p_2) = (239, 383)$.

$$O_{239\cdot 383}(2) = 22729, \qquad O_{239}(383) = 119.$$

$$239 \| 2^{22729} - 1, \qquad 239 \| 383^{119} - 1.$$

So we finish the proof. □

Remark 1. We in fact prove that there is no element in $\mathbb{Z}[\zeta_M]$ with magnitude $(2M)^{\frac{n}{2}}$. In the above theorem, we only choose all (p_1, p_2) of the class (d). For other cases in Feng et al.'s articles, as we only need to determine the index t_1, t_2 such that

$$p_1^{t_1} \| 2^{O_{M_2}(2)} - 1, \qquad p_1^{t_2} \| p_2^{O_{M_{p_2}}(p_2)} - 1.$$

when $p_1 \| M_2$ and $p_1 \| M_{p_2}$. Numbers satisfies $m^2 | a^{\phi(m)} - 1$ are quite rare, with ϕ the Euler function. There are only 104 such numbers for $a = 2$ [1]. It is reasonable to believe for these cases $t_1 = t_2 = 1$, so we may get more nonexistence results.

Theorem 3. *(p_1, p_2) as the above, there is no GBF with type $[1, 2p_1^e p_2^3]$ and $[1, 2p_1^e p_2^5]$ for all $e \geq 1$.*

Proof. We first prove the case $[1, 2p_1^e p_2^3]$. Just as the proof of Theorem 2, if such a GBF exists, then there is

$$\alpha \in \mathbb{Z}[\zeta_{F(p_1^e p_2^3, 2p_2^3)}], \qquad \alpha\bar{\alpha} = 2p_2^3.$$

By the definition of $F(m, n)$, compare to the case $F(p_1^e p_2, (2p_2)^3)$, we only need one more step to determine the index

$$p_2^t \| 2^{O_{p_1 p_2}(2)} - 1.$$

By a computer, it is easy to find that for all the (p_1, p_2), we have $t = 1$. So we have $F(p_1^e p_2^3, 2p_2^3) = p_1 p_2$ and $\alpha \in \mathbb{Z}[\zeta_{p_1 p_2}]$, then $2\alpha\overline{2\alpha} = (2p_2)^3$, a contradiction to $(*)$. For the case $[1, 2p_1^e p_2^5]$, using the same method, we have

$$\alpha \in \mathbb{Z}[\zeta_{p_1 p_2}], \qquad \alpha\bar{\alpha} = 2p_2^5.$$

Then $4\alpha\overline{4\alpha} = (2p_2)^5$, contradict to $(*)$. □

Remark 2. For the same reason of Remark 1, it is believed that for other cases in Feng et al.'s articles, we can get similar results.

3 Type $[3, 2 \cdot 23^e]$

In this section, we are going to prove that there is no GBF with type $[n, 2 \cdot 23^e]$, $n = 1, 3$. The $n = 1$ case is proved by Feng in [4](class (a) in §1). First we consider when $e = 1$. Here is some facts obaut the cyclotomic field $K = \mathbb{Q}(\zeta_{23})$, which can be seen in many textbooks about algebraic

number theory, such as [7] and [12]. There is a unique quadratic number field $L = \mathbb{Q}(\sqrt{-23})$ included in K. Let $\mathcal{O}_K$ and $\mathcal{O}_L$ denote their rings of algebraic integers respectively. Notice that the order of 2 mod 23 is 11, then we have the following prime ideal factorizations

$$2\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2 \qquad \mathfrak{p}_1 = (2, \frac{1-\sqrt{-23}}{2})\mathcal{O}_L, \mathfrak{p}_2 = (2, \frac{1+\sqrt{-23}}{2})\mathcal{O}_L$$

$$2\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2 \qquad \mathfrak{P}_1 = (2, \frac{1-\sqrt{-23}}{2})\mathcal{O}_K, \mathfrak{P}_2 = (2, \frac{1+\sqrt{-23}}{2})\mathcal{O}_K$$

23 is ramified in K with ramification index 22.

$$\sqrt{-23}\mathcal{O}_K = \mathfrak{P}^{11} \qquad \mathfrak{P} = (1-\zeta_{23})\mathcal{O}_K$$

It is easy to check that $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are not principal ideals, and there cubic is.

$$\mathfrak{p}_1^3 = \frac{3+\sqrt{-23}}{2}\mathcal{O}_L \qquad \mathfrak{p}_2^3 = \frac{3-\sqrt{-23}}{2}\mathcal{O}_L$$

Recalling the definition of ideal norm $\mathcal{N}$, we have a homomorphism from the ideal class group of K to the ideal class group of L and $\mathcal{N}(\mathfrak{P}_i) = \mathfrak{p}_i^{11}$ for $i = 1, 2$, as the idea class of $\mathfrak{p}_i$ has order 3, which is relatively prime to 11, so $\mathfrak{P}_i$ is not principal, and

$$\mathfrak{P}_1^3 = \frac{3+\sqrt{-23}}{2}\mathcal{O}_K \qquad \mathfrak{P}_2^3 = \frac{3-\sqrt{-23}}{2}\mathcal{O}_K$$

Lemma 2. *If $\alpha \in \mathbb{Z}[\zeta_{23}]$ then $\alpha\bar{\alpha} \neq 46$. Moreover if $\alpha\bar{\alpha} = (46)^3$, then α must have the form*

$$\alpha = \sqrt{-23}^3 \cdot \frac{3 \pm \sqrt{-23}}{2} \cdot (\pm\zeta_{23}^i).$$

Proof. If $\alpha\bar{\alpha} = 46$. then we have the following prime ideal factorization

$$(\alpha\mathcal{O}_K)(\bar{\alpha}\mathcal{O}_K) = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}^{22}.$$

If $\mathfrak{P}^t|\alpha\mathcal{O}_K$, then $\mathfrak{P}^t|\bar{\alpha}\mathcal{O}_K$, so $\mathfrak{P}^{11}|\alpha\mathcal{O}_K$, and

$$\frac{\alpha}{\sqrt{-23}} \in \mathbb{Z}[\zeta_{23}], \qquad \frac{\alpha}{\sqrt{-23}}\mathcal{O}_K = \mathfrak{P}_1 \text{ or } \mathfrak{P}_2.$$

contradict to that $\mathfrak{P}_i$ is not principal. So $\alpha\bar{\alpha} \neq 46$.

If $\alpha \in \mathcal{O}_K$ with $\alpha\bar{\alpha} = 46^3$. For the same reason

$$\beta = \frac{\alpha}{\sqrt{-23}^3} \in \mathbb{Z}[\zeta_{23}], \qquad (\beta\mathcal{O}_K)(\bar{\beta}\mathcal{O}_K) = \mathfrak{P}_1^3\mathfrak{P}_2^3.$$

We have $\beta\mathcal{O}_K = \mathfrak{P}_1^3$ or $\mathfrak{P}_2^3$, if not we can get $\beta\mathcal{O}_K = 2\mathfrak{P}_1$ or $2\mathfrak{P}_2$, contradiction with that $\mathfrak{P}_i$ is not principal. We assume $\beta = \frac{3\pm\sqrt{-23}}{2}u$ with u a unit in $\mathcal{O}_K$, then $u\bar{u} = 1$. For any Galois automorphism σ of K, we have

$$\sigma(u)\overline{\sigma(u)} = \sigma(u)\sigma(\bar{u}) = 1,$$

so u is a root of unity and have the form of $\pm\zeta_{23}^i$. Then

$$\alpha = \sqrt{-23}^3 \cdot \frac{3 \pm \sqrt{-23}}{2} \cdot (\pm\zeta_{23}^i).$$

We finish the proof. □

From the above Lemma, we know that there is no GBF of type $[1, 46]$. If f is a GBF of type $[3, 46]$, then for every $\lambda \in \mathbb{Z}_{46}^3$,

$$F(\lambda) = \sqrt{-23}^3 \cdot \frac{3 \pm \sqrt{-23}}{2} \cdot (\pm\zeta_{23}^i).$$

There are 7 elements in the additive group of $\mathbb{Z}_{46}^3$ with order 2, such as $v = (23, 0, 0)$. We have the following lemma.

Lemma 3. *If $v \in \mathbb{Z}_{46}^3$ is an element of order 2, then for every $\lambda \in \mathbb{Z}_{46}^3$, we have*

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

Proof. As v is of order 2, for $x \in \mathbb{Z}_{46}^3$, we have $\zeta_{46}^{x\cdot v} = \pm 1$. So

$$F(\lambda) + F(\lambda + v) = \sum_{x\in\mathbb{Z}_{46}^3} \zeta_{46}^{f(x)-x\dot{\lambda}}(1 + \zeta_{46}^{-x\dot{v}}) = 2\alpha \in \mathfrak{P}_1 \cap \mathfrak{P}_2$$

for some $\alpha \in \mathbb{Z}[\zeta_{23}]$. Then $F(\lambda) \in \mathfrak{P}_i \Leftrightarrow F(\lambda + v) \in \mathfrak{P}_i$. By the above Lemma, we have $F(\lambda + v) = F(\lambda) \cdot (\pm\zeta_{23}^i)$ for some $0 \le i < 23$. Then

$$F(\lambda) + F(\lambda + v) = F(\lambda)(1 \pm \zeta_{23}^i) \in \mathfrak{P}_1 \cap \mathfrak{P}_2$$

By results in algebraic number theory, if $i \neq 0$,

$$(1 - \zeta_{23}^i)\mathcal{O}_K = \mathfrak{P}$$

and $1 + \zeta_{23}^i$ is a unit. $F(\lambda)(1 \pm \zeta_{23}^i)$ can't both be in $\mathfrak{P}_1$ and $\mathfrak{P}_2$, so $i = 0$ and we finish the proof. □

Let $v_1 = (23, 0, 0),\ v_2 = (0, 23, 0),\ v_3 = (23, 23, 0)$. Notice that

$$v_i + v_j = v_k,$$

if $\{i,\ j,\ k\}$ is a permutation of $\{1,\ 2,\ 3\}$. Define

$$N_i = \{x \in \mathbb{Z}_{46}^3 \mid F(x) = F(x + v_i)\}$$
$$M_i = \{x \in \mathbb{Z}_{46}^3 \mid F(x) = -F(x + v_i)\}.$$

Let n_i, m_i denote the cardinality of N_i, M_i, so $n_i + m_i = (46)^3$.

Lemma 4. $n_i = m_i = 4 \cdot (23)^3$.

Proof. As $\sum_{x \in \mathbb{Z}_{46}^3} F(x)\overline{F(x + v_i)} = 0$. By the above lemma,

$$F(x)\overline{F(x + v_i)} = \begin{cases} (46)^3 & \text{if } x \in N_i, \\ -(46)^3 & \text{if } x \in M_i. \end{cases}$$

so $(n_i - m_i) \cdot (46)^3 = 0$ then $n_i = m_i = 4 \cdot (23)^3$. □

Now consider the following 4 sets

$$T_1 = N_1 \cap N_2 = \{x \in \mathbb{Z}_{46}^3 \mid F(x) = F(x + v_1) = F(x + v_2)\}$$
$$T_2 = N_1 \cap M_2 = \{x \in \mathbb{Z}_{46}^3 \mid F(x) = F(x + v_1) = -F(x + v_2)\}$$
$$T_3 = M_1 \cap N_2 = \{x \in \mathbb{Z}_{46}^3 \mid F(x) = -F(x + v_1) = F(x + v_2)\}$$
$$T_4 = M_1 \cap M_2 = \{x \in \mathbb{Z}_{46}^3 \mid F(x) = -F(x + v_1) = -F(x + v_2)\}$$

Denote their cardinalities by t_1, t_2, t_3, t_4. We have the following lemma.

Lemma 5. $t_1 = t_2 = t_3 = t_4 = 2 \cdot (23)^3$.

Proof. First it is easy to note that $t_1 + t_2 = n_1 = n_2 = t_1 + t_3$, so we have $t_2 = t_3$ and then $t_1 = t_4$. For our result, we only need to prove $t_1 = t_2$. We define 8 more sets.

$$W_1 = T_1 \cap N_3 = \{x \mid F(x) = F(x + v_1) = F(x + v_2) = F(x + v_3)\}$$
$$W_2 = T_1 \cap M_3 = \{x \mid F(x) = F(x + v_1) = F(x + v_2) = -F(x + v_3)\}$$
$$W_3 = T_2 \cap N_3 = \{x \mid F(x) = F(x + v_1) = -F(x + v_2) = F(x + v_3)\}$$
$$W_4 = T_2 \cap M_3 = \{x \mid F(x) = F(x + v_1) = -F(x + v_2) = -F(x + v_3)\}$$
$$W_5 = T_3 \cap N_3 = \{x \mid F(x) = -F(x + v_1) = F(x + v_2) = F(x + v_3)\}$$
$$W_6 = T_3 \cap M_3 = \{x \mid F(x) = -F(x + v_1) = F(x + v_2) = -F(x + v_3)\}$$
$$W_7 = T_4 \cap N_3 = \{x \mid F(x) = -F(x + v_1) = -F(x + v_2) = F(x + v_3)\}$$
$$W_8 = T_4 \cap M_3 = \{x \mid F(x) = -F(x + v_1) = -F(x + v_2) = -F(x + v_3)\}$$

each with cardinality w_i. Notice that

$$\begin{aligned} x \in W_2 &\Longleftrightarrow x + v_1 \in W_3 \\ &\Longleftrightarrow x + v_2 \in W_5 \\ &\Longleftrightarrow x + v_3 \in W_8 \end{aligned}$$

so $w_2 = w_3 = w_5 = w_8$. Notice that $N_3 = W_1 \cup W_3 \cup W_5 \cup W_7$, so

$$w_1 + w_3 + w_5 + w_7 = n_3.$$

Also we have $M_2 = W_3 \cup W_4 \cup W_7 \cup W_8$, then

$$w_3 + w_4 + w_7 + w_8 = m_2.$$

By the above lemma $n_3 = m_2$. so we get $w_1 = w_4$. Then

$$t_1 = w_1 + w_2 = w_3 + w_4 = t_2.$$

we finish the proof. □

Lemma 6. $W_2 = W_3 = W_5 = W_8 = \emptyset$.

Proof. From the proof of the above lemma, we only need to prove $W_2 = \emptyset$. If $x \in W_2$, then $F(x) = F(x + v_1)$,

$$F(x) = \sum_{(y_1,y_2,y_3)\in\mathbb{Z}_{46}^3} \zeta_{46}^{f(y)-x\cdot y} = \Big(\sum_{y_1\equiv 0(2)} + \sum_{y_1\equiv 1(2)} \Big) \zeta_{46}^{f(y)-x\cdot y}$$

$$F(x+v_1) = \sum_{(y_1,y_2,y_3)\in\mathbb{Z}_{46}^3} \zeta_{46}^{f(y)-(x+v_1)\cdot y} = \Big(\sum_{y_1\equiv 0(2)} - \sum_{y_1\equiv 1(2)} \Big) \zeta_{46}^{f(y)-x\cdot y}$$

The sum of the $y_1 \equiv 1 \mod 2$ part must be zero, so

$$F(x) = \sum_{y_1\equiv 0(2)} \zeta_{46}^{f(y)-x\cdot y}.$$

For the same reason from $F(x) = F(x + v_2)$ and $F(x) = -F(x + v_3)$ we get

$$F(x) = \sum_{y_2\equiv 0(2)} \zeta_{46}^{f(y)-x\cdot y}.$$

$$F(x) = \sum_{y_1+y_2\equiv 1(2)} \zeta_{46}^{f(y)-x\cdot y}.$$

so we have

$$F(x) = \Big(\sum_{y_1 \equiv 0(2)} + \sum_{y_2 \equiv 0(2)} - \sum_{y_1+y_2 \equiv 1(2)} \Big) \zeta_{46}^{f(y)-x\cdot y}.$$

and then

$$F(x) = 2 \sum_{y_1 \equiv y_2 \equiv 0(2)} \zeta_{46}^{f(y)-x\cdot y}.$$

which is impossible as $F(x)$ must has the form of $\sqrt{-23}^3 \cdot \frac{3\pm\sqrt{-23}}{2} \cdot (\pm\zeta_{23}^i)$ By Lemma 2. □

From the above two lemma, we have $t_1 = w_1 = 2 \cdot (23)^3$. If $x \in W_1$, then $x + v_1$, $x + v_2$ and $x + v_3$ must also in W_1. so $w_1 \equiv 0 \mod 4$, contradiction. Now we have proved there is no GBF of type $[n, 46]$ for $n = 1, 3$. For general e, the proof is similar. Again we denote $K = \mathbb{Q}(\zeta_{23^e})$. Just notice that the order of 2 mod 23^e is $11 \cdot 23^{e-1}$ then we have

$$2\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2 \qquad \mathfrak{P}_1 = (2, \frac{1-\sqrt{-23}}{2})\mathcal{O}_K, \mathfrak{P}_2 = (2, \frac{1+\sqrt{-23}}{2})\mathcal{O}_K$$

As $\gcd(11 \cdot (23)^{e-1}, 3) = 1$, we also get $\mathfrak{P}_i$ is not principal and its cubic is principal. We have

Theorem 4. *There is no GBF with type* $[n, 2 \cdot (23)^e]$ *for* $n = 1, 3$.

Remark 3. In the proof of Lemma 4 and 5, we only use the property of GBF. For odd N, if we have $F(x) = \pm F(x + v)$ and $2 \not| F(x)$ for all $x \in \mathbb{Z}_{2N}^3$ and v with order 2. Then there is no GBF with type $[3, 2N]$. For the $n = 3$ case, we only use 3 order-2 elements of total 7. For $n > 3$, if we use more order-2 elements, the same method may also work, but it must be too complicated.

4 Conclusion and future work

In this article we give two new kinds of nonexistence of GBF, one based on the field descent method and Feng et al's results, and the other based on the property of the cyclotomic field $\mathbb{Q}(\zeta_{23^e})$. Since Kumar et al gave the definition of GBF in 1985 [10], it is almost thirty years and there is no GBF constructed in the case $[n, q]$ with n odd and $q \equiv 2 \bmod 4$. It is believed that no such GBF exists. Although Feng and some others gave some results, this question is far from solved.

Acknowledgments The work of this paper was supported by the NNSF of China (Grants Nos. 11071285, 61121062) and 973 Project (2011CB302401).

References

[1] T. Agoh, K. Dilcher, L. Skula, Fermat quotients for composite muduli, J. Number Theory, **66**(1997), 29-50.

[2] E. Akyildiz, I. S. Gulogu and M. Ikeda, A note of generalized bent functions, J. Pure Appl. Alg., **106**(1996), 1-9.

[3] J. F. Dillon, Elementary Hadamard difference sets, Ph. D. dissertation, University of Maryland, 1974.

[4] Keqin Feng, Generalized bent funcions and class group of imaginary quadratic fields, Sci China(Series A) **44**(2001), 562-570.

[5] Keqin Feng and Fengmei Liu, New results on the nonexistence of generalized bent functions, IEEE Trans. Inform. Theory, **49**(2003), 3066-3071.

[6] Keqin Feng and Fengmei Liu, Nonexistence of some generalized bent functions, Acta Math. Sin.(English Series), **19**(2003), 39-50.

[7] A. Fröhlich and M. J. Taylor, Algebraic Number Theory, Cambridge University Press, 1991.

[8] Tor Helleseth and Alexander Kholosha, On generalized bent functions, Information theory and applications workshop(ITA), 2010.

[9] M. Ikeda, A remark on the non-existence of generalized bent functions, in Lecture Notes in Pure and Applied Mathematics, **204**(1999), 109-119.

[10] P. V. Kumar, Scholtz R. A. and Welch L. R., Generalized bent functions and their properties, J. Comb. Theory(A) **40**(1985), 90-107.

[11] Fengmei Liu, Zhi Ma and Keqin Feng, New results on nonexistence of generalized bent functions(II), Sci. China(Series A), **45**(2002), 721-730.

[12] D. A. Marcus, Number Fields, Springer-Verlag, 1977.

[13] J. D. Olsen, R. A. Scholtz and L. R. Welch, Bent-function sequences, IEEE Trans. Inform. Theory, **28**(1982), 858-864.

[14] D. Pei, On non-existence of generalized bent functions, in Lecture Notes in Pure and Applied Mathematics, **141**(1993), 165-172.

[15] O. S. Rothaus, On "bent" functions, J. Comb. Theory(A) **20**(1976), 300-305.

[16] B. Schmidt, Cyclotomic integers and finite geometry, J. Amer. Math. Soc. **12**(1999), no. 4, 929-952.