Des. Codes Cryptogr. (2017) 82:647–662
DOI 10.1007/s10623-016-0192-9

Nonexistence of generalized bent functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_m$

Haiying Liu[1] · Keqin Feng[2] · Rongquan Feng[1]

Received: 27 March 2015 / Revised: 10 January 2016 / Accepted: 14 January 2016 /
Published online: 17 February 2016

Abstract In this paper, several nonexistence results on generalized bent functions $f : \mathbb{Z}_2^n \to \mathbb{Z}_m$ are presented by using the knowledge on cyclotomic number fields and their imaginary quadratic subfields.

Keywords Generalized bent function · Imaginary quadratic field · Cyclotomic field · Class number · Decomposition field

Mathematics Subject Classification 11A07 · 11R04 · 11T71

1 Introduction

Let m and n be positive integers, $m \geq 2$, $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} = \{0, 1, \ldots, m-1\}$. A mapping $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is called a Boolean function with n variables. The Fourier transform of the function f is given by $W_f : \mathbb{Z}_2^n \to \mathbb{R}$ with

$$W_f(y) = \sum_{x \in \mathbb{Z}_2^n} (-1)^{f(x)+x\cdot y},$$

Communicated by C. Mitchell.

✉ Haiying Liu
hyliumath@pku.edu.cn

Keqin Feng
kfeng@math.tsinghua.edu.cn

Rongquan Feng
fengrq@math.pku.edu.cn

[1] School of Mathematical Sciences, Peking University, Beijing 100871, China

[2] Department of Mathematical Sciences, Tsinghua University, Beijing 100084, China

where $x \cdot y = \sum_{i=1}^{n} x_i y_i \in \mathbb{Z}_2$ and $\mathbb{R}$ is the field of real numbers. A Boolean function f is called a bent function if $\left|W_f(y)\right| = 2^{\frac{n}{2}}$ holds for every $y \in \mathbb{Z}_2^n$. Bent functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2$ are introduced and studied by Rothaus [7] in 1976. Kumar et al. [3] generalized the notation in 1985 by considering the functions from $\mathbb{Z}_m^n$ to $\mathbb{Z}_m$, and in 2009 [8], Schmidt studied another generalized bent function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_m$, especially $m = 2^h$. In this paper we will deal with functions $f : \mathbb{Z}_2^n \to \mathbb{Z}_m$. For $m = 2$, this is the usual Boolean function. Let $\zeta_m = e^{\frac{2\pi\sqrt{-1}}{m}} \in \mathbb{C}$, the Fourier transform of f is given by $W_f : \mathbb{Z}_2^n \to \mathbb{Z}[\zeta_m] \subseteq \mathbb{C}$ with

$$W_f(y) = \sum_{x \in \mathbb{Z}_2^n} (-1)^{x \cdot y} \zeta_m^{f(x)} \quad \left(y \in \mathbb{Z}_2^n\right). \tag{1}$$

The inverse Fourier transform is

$$\zeta_m^{f(x)} = \frac{1}{2^n} \sum_{y \in \mathbb{Z}_2^n} (-1)^{x \cdot y} W_f(y) \quad \left(x \in \mathbb{Z}_2^n\right), \tag{2}$$

and from (1) we get

$$\begin{aligned}\sum_{y \in \mathbb{Z}_2^n} |W_f(y)|^2 &= \sum_{y \in \mathbb{Z}_2^n} \sum_{x, x' \in \mathbb{Z}_2^n} (-1)^{(x+x') \cdot y} \zeta_m^{f(x)-f(x')} \\ &= \sum_{x, x' \in \mathbb{Z}_2^n} \zeta_m^{f(x)-f(x')} \sum_{y \in \mathbb{Z}_2^n} (-1)^{(x+x') \cdot y} \\ &= 2^n \sum_{x \in \mathbb{Z}_2^n} 1 = 2^{2n}.\end{aligned}$$

Therefore, the maximum value $M = max\{\left|W_f(y)\right| : y \in \mathbb{Z}_2^n\}$ has lower bound $2^{\frac{n}{2}}$ and $M = 2^{\frac{n}{2}}$ if and only if $\left|W_f(y)\right| = 2^{\frac{n}{2}}$ for all $y \in \mathbb{Z}_2^n$.

Definition 1 A function $f : \mathbb{Z}_2^n \to \mathbb{Z}_m$ is called (m, n)-generalized bent function if $\left|W_f(y)\right| = 2^{\frac{n}{2}}$ for all $y \in \mathbb{Z}_2^n$, (m, n)-GBF in short.

For $m = 2$, this is the (Boolean) bent function in [7]. It is well-known that there exist bent functions $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ if and only if n is even. For even numbers n, many constructions on bent functions with n variables have been found. One of the simplest examples is Rothaus's bent function $f(x) = x_1x_2 + x_3x_4 + \cdots + x_{2t-1}x_{2t}$, where $n = 2t$. For $m = 4$ and $m = 8$, several constructions and existence results on GBFs have been found in [5,8–13]. Generalized bent functions have been widely investigated since they are applied in many fields such as communication theory, cryptography and closely related to coding theory and combinatorial design theory.

The main aim of this paper is to present several nonexistence results on (m, n)-GBFs. Firstly we collect existence results in Sect. 2 by using previous facts given in [10,11] and some simple observations. Then we show nonexistence results in the last three sections. In Sect. 3 we prove that there is no $\{p^l, n\}$-type GBF for any $n \geq 1$ and any odd prime power p^l by using a result in [4]. In Sect. 4 and Sect. 5 we use the basic knowledge on cyclotomic number field $K = \mathbb{Q}(\zeta_m)$ to get some nonexistence results. The point is that, for (m, n)-GBFs f, the values of $W_f(y)$ belong to the ring $\mathbb{Z}[\zeta_m]$. We introduce some basic facts at the beginning of Sect. 4. Then we get further nonexistence results on GBF in Sect. 4 for semiprimitive case and in Sect. 5 for other cases by field-descent method. We end with conclusions in Sect. 6.

2 Existence results

Firstly, we collect previous existence results on (m, n)-GBF $f : \mathbb{Z}_2^n \to \mathbb{Z}_m$ where $n \geq 1$, $m \geq 2$.

Lemma 1 (1)([7]) *There exists a* $(2, n)$*-GBF if and only if n is even.*

(2)([10]) *If both m and n are even numbers, then there exists an* (m, n)*-GBF.*

(3)([12]) *If there exists a* $(2, n+1)$*-GBF, then there exists a* $(4, n)$*-GBF.*

Remark 1 (A) For the proof of (2), let $m = 2l$, $n = 2t$, σ be an arbitrary permutation on $\mathbb{Z}_2^t$ and $g : \mathbb{Z}_2^t \to \mathbb{Z}_m$ be an arbitrary function. Consider the following function $f = f(x, y) : \mathbb{Z}_2^t \oplus \mathbb{Z}_2^t = \mathbb{Z}_2^n \to \mathbb{Z}_m$,

$$f(x, y) = g(y) + lx \cdot \sigma(y) \quad (x, y \in \mathbb{Z}_2^t).$$

It is easy to see that f is a GBF.

(B) The conclusion (3) has been proved in [12] as a consequence of some more general results. Here we give a direct simple proof.

Suppose that $f = f(x, x') : \mathbb{Z}_2^n \oplus \mathbb{Z}_2 = \mathbb{Z}_2^{n+1} \longrightarrow \mathbb{Z}_2 (x \in \mathbb{Z}_2^n, x' \in \mathbb{Z}_2)$ is a Boolean bent function. Then for $y \in \mathbb{Z}_2^n$ and $y' \in \mathbb{Z}_2$,

$$\begin{aligned} \pm 2^{\frac{n+1}{2}} = W_f(y, y') &= \sum_{x \in \mathbb{Z}_2^n, x' \in \mathbb{Z}_2} (-1)^{f(x,x') + x \cdot y + x'y'} \\ &= \sum_{x \in \mathbb{Z}_2^n} \left((-1)^{f(x,0) + x \cdot y} + (-1)^{f(x,1) + x \cdot y + y'} \right). \end{aligned} \tag{3}$$

For $a, b \in \mathbb{Z}_2 = \{0, 1\}$ and $y \in \mathbb{Z}_2^n$, let

$$N_y(a, b) = \sum_{\substack{x \in \mathbb{Z}_2^n \\ f(x,0) = a,\ f(x,1) = b}} (-1)^{x \cdot y},$$

then by (3) we get

$$\begin{aligned} \pm 2^{\frac{n+1}{2}} &= \left(N_y(0,0) + N_y(0,1) - N_y(1,0) - N_y(1,1) \right) \\ &\quad + (-1)^{y'} \left(N_y(0,0) + N_y(1,0) - N_y(0,1) - N_y(1,1) \right). \end{aligned}$$

Taking $y' = 0$ and 1 we get

$$2 \left(N_y(0,0) - N_y(1,1) \right) = 2 \left(N_y(0,1) - N_y(1,0) \right) = \pm 2^{\frac{n+1}{2}}. \tag{4}$$

Now we define $F : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_4 = \{0, 1, 2, 3\}$,

$$F(x) = \begin{cases} 0, & \text{if } f(x,0) = f(x,1) = 0 \\ 1, & \text{if } f(x,0) = 0,\ f(x,1) = 1 \\ 2, & \text{if } f(x,0) = f(x,1) = 1 \\ 3, & \text{if } f(x,0) = 1,\ f(x,1) = 0. \end{cases}$$

Then for each $y \in \mathbb{Z}_2^n$,

$$\begin{aligned} W_F(y) &= \sum_{x \in \mathbb{Z}_2^n} (-1)^{x \cdot y} \zeta_4^{F(x)} \quad (\zeta_4 = \sqrt{-1}) \\ &= N_y(0,0) + \zeta_4 N_y(0,1) - N_y(1,1) - \zeta_4 N_y(1,0) \\ &= \left(N_y(0,0) - N_y(1,1) \right) + \zeta_4 \left(N_y(0,1) - N_y(1,0) \right). \end{aligned}$$

By (4), we get

$$\begin{aligned}|W_F(y)|^2 &= \big(N_y(0,0) - N_y(1,1)\big)^2 + \big(N_y(0,1) - N_y(1,0)\big)^2\\ &= 2^{n-1} + 2^{n-1} = 2^n.\end{aligned}$$

Therefore, F is a GBF.

(C) For even $n \geq 2$, there exist $(4, n)$-GBFs by Lemma 1(2). For odd $n \geq 1$, there exist Boolean bent functions $f : \mathbb{Z}_2^{n+1} \longrightarrow \mathbb{Z}_2$ by Lemma 1(1). Thus there exist $(4, n)$-GBFs by Lemma 1(3). Therefore, we have $(4, n)$-GBFs for any positive integer n.

Next we show the following simple observation.

Lemma 2 (1) *If there exist (m, n)-GBFs and (m, n')-GBFs, then there exist $(m, n + n')$-GBFs.*

(2) *If there exists an (m, n)-GBF, then for any positive integer l there exists an (lm, n)-GBF. In other words, if there is no (m, n)-GBF, then there is no (m', n)-GBF for any factor $m' \geq 2$ of m.*

Proof (1) Let $f : \mathbb{Z}_2^n \to \mathbb{Z}_m$ and $f' : \mathbb{Z}_2^{n'} \to \mathbb{Z}_m$ be GBFs. It is easy to see that

$$F : \mathbb{Z}_2^{n+n'} \to \mathbb{Z}_m, \quad F(x, x') = f(x) + f'(x') \qquad \left(x \in \mathbb{Z}_2^n, x' \in \mathbb{Z}_2^{n'}\right)$$

is a GBF.

(2) Given a GBF $f : \mathbb{Z}_2^n \to \mathbb{Z}_m$, consider the following well-defined function

$$F : \mathbb{Z}_2^n \to \mathbb{Z}_{lm}, \quad F(x) = lf(x) \qquad (x \in \mathbb{Z}_2^n).$$

For each $y \in \mathbb{Z}_2^n$,

$$W_F(y) = \sum_{x \in \mathbb{Z}_2^n} (-1)^{x \cdot y} \zeta_{lm}^{F(x)} = \sum_{x \in \mathbb{Z}_2^n} (-1)^{x \cdot y} \zeta_m^{f(x)} = W_f(y).$$

Therefore, F is a GBF if f is a GBF. □

From Lemma 1(1), Remark 1(C) and Lemma 2 we know that if both m and n are even or $4 \mid m$, then there exists a (m, n)-GBF. The remaining cases are

Case (I) $\quad 2 \nmid m$, or

Case (II) $\quad 2 \nmid n$ and $m \equiv 2 \pmod 4$.

No GBF has been constructed in the above cases by our knowledge so far. In the following three sections we will show several nonexistence results for these cases.

3 Nonexistence results (I)

In this section we present a nonexistence result on GBF as a corollary to the following lemma, which is a retelling of the main theorem in [4] given by Lam and Leung.

Lemma 3 [4] *Let $m = p_1^{a_1} \cdots p_s^{a_s}$, where $p_1, \ldots, p_s$ are distinct prime numbers and $a_i \geq 1$ $(1 \leq i \leq s)$. Let $S = \{\zeta_m^i : 0 \leq i \leq m-1\}$. Then for any integer $n \geq 1$, the equation $x_1 + \cdots + x_n = 0$ has a solution $x_j \in S$ $(1 \leq j \leq n)$ if and only if $n = n_1 p_1 + \cdots + n_s p_s$ has a non-negative integer solution $(n_1, \ldots, n_s)$.*

Corollary 1 *Let $m = p_1^{a_1} \cdots p_s^{a_s}$, where $p_1, \ldots, p_s$ are distinct odd prime numbers and $a_i \geq 1$ $(1 \leq i \leq s)$. If*

$$2^n = n_1 p_1 + \cdots + n_s p_s$$

has no non-negative integer solutions $(n_1, \ldots, n_s)$, then there is no (m, n)-GBF.

Proof Suppose that $f : \mathbb{Z}_2^n \to \mathbb{Z}_m$ is a GBF. Then $\left|W_f(y)\right|^2 = 2^n$ for any $y \in \mathbb{Z}_2^n$. By inverse Fourier transform (2), for $0 \neq a \in \mathbb{Z}_2^n$, we have

$$\begin{aligned}\sum_{x\in\mathbb{Z}_2^n} \zeta_m^{f(x+a)-f(x)} &= \frac{1}{2^{2n}} \sum_{x\in\mathbb{Z}_2^n} \sum_{y\in\mathbb{Z}_2^n} W_f(y)(-1)^{(x+a)\cdot y} \sum_{z\in\mathbb{Z}_2^n} \overline{W_f(z)}(-1)^{x\cdot z} \\ &= \frac{1}{2^{2n}} \sum_{y,z\in\mathbb{Z}_2^n} W_f(y)\overline{W_f(z)}(-1)^{a\cdot y} \sum_{x\in\mathbb{Z}_2^n} (-1)^{x\cdot(y+z)} \\ &= \frac{1}{2^n} \sum_{y\in\mathbb{Z}_2^n} W_f(y)\overline{W_f(y)}(-1)^{a\cdot y} = \frac{1}{2^n} \sum_{y\in\mathbb{Z}_2^n} \left|W_f(y)\right|^2(-1)^{a\cdot y} \\ &= \sum_{y\in\mathbb{Z}_2^n} (-1)^{a\cdot y} = 0.\end{aligned}$$

The left-hand side is a sum of 2^n elements and each element is a power of ζ_m. By Lemma 3, the equation $2^n = n_1 p_1 + \cdots + n_s p_s$ has a non-negative integer solution $(n_1, \ldots, n_s)$. This completes the proof of Corollary 1. □

Corollary 2 *There is no (m, n)-GBF provided one of the following conditions on m and n is satisfied.*

(1) *m is an odd prime power and n is an arbitrary positive integer;*
(2) *$m = p_1^{a_1} \cdots p_s^{a_s}$, $3 \leq p_1 < p_2 < \cdots < p_s$ and $2^n < p_1 + p_2$;*
(3) *$m = p_1^{a_1} p_2^{a_2}$, $p_1 \neq p_2$, a_1, $a_2 \geq 1$, $2^n = p_1 p_2 - m_1 p_1 - m_2 p_2$ for some positive integers m_1 and m_2.*

Proof This is a direct consequence of Corollary 1.

For (1), $2^n = px$ has no solution $x \in \mathbb{Z}$ since p is an odd prime;

For (2), if $2^n = n_1 p_1 + \cdots + n_s p_s$ $(n_i \geq 0)$, then $n_i \geq 1$ for at least two i. Therefore, $2^n \geq p_1 + p_2$;

For (3), if $p_1 p_2 - m_1 p_1 - m_2 p_2 = 2^n = n_1 p_1 + n_2 p_2$, then $p_1 p_2 - p_1 - p_2 = p_1(n_1+m_1-1)+p_2(n_2+m_2-1)$ which contradicts to the well-known fact that $p_1 p_2 - p_1 - p_2$ is the largest integer N such that $N = p_1 x_1 + p_2 x_2$ has no non-negative integer solution (x_1, x_2). Therefore, $2^n = n_1 p_1 + n_2 p_2$ has no non-negative integer solution (n_1, n_2). □

Example 1 By Corollary 2 it can be computed that there is no $(7^{a_1} 13^{a_2}, n)$-GBF for all $a_1, a_2 \geq 1$ and $1 \leq n \leq 6$.

4 Nonexistence results (II): semiprimitive case

In this and next sections we will consider the cases $2 \nmid n$ and $2 \nmid m$ or $m \equiv 2 \pmod 4$. Firstly, we introduce some basic facts on cyclotomic number field $\mathbb{Q}(\zeta_m)$ where $\mathbb{Q}$ is the field of rational numbers. We refer to books [2] and [14] for details. If $m \equiv 2 \pmod 4$, i.e.,

$m = 2t$ and $2 \nmid t$, we have $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_t)$ since $\zeta_t = \zeta_m^2$ and $-\zeta_m = \zeta_m^{\frac{m}{2}+1} = \zeta_{2t}^{t+1} = \zeta_t^{\frac{t+1}{2}}$. Therefore, we can only consider $\mathbb{Q}(\zeta_m)$ for odd m.

FACT(1). For the cyclotomic field $K = \mathbb{Q}(\zeta_m)$ where $m \geq 3$ and $m \not\equiv 2 \pmod 4$, $K/\mathbb{Q}$ is a Galois extension with degree $[K : \mathbb{Q}] = \varphi(m)$, where $\varphi(m)$ is the Euler (totient) function. The Galois group of $K/\mathbb{Q}$ is

$$Gal(K/\mathbb{Q}) = \left\{\sigma_a : a \in \mathbb{Z}_m^*\right\},$$

where $\mathbb{Z}_m^* = \{1 \leq a \leq m-1 : (a, m) = 1\}$ is the multiplicative group of units in the ring $\mathbb{Z}_m$, $|\mathbb{Z}_m^*| = \varphi(m)$, and the automorphism σ_a of K is defined by $\sigma_a(\zeta_m) = \zeta_m^a$. We have $\sigma_a \sigma_b = \sigma_{ab}$ for $a, b \in \mathbb{Z}_m^*$. Therefore, we have the following isomorphism of groups

$$\mathbb{Z}_m^* \cong Gal(K/\mathbb{Q}), \qquad a \mapsto \sigma_a.$$

FACT(2). Let L be any (algebraic) number field which means $L/\mathbb{Q}$ is a finite extension. An element $\alpha \in L$ is called an (algebraic) integer in L if there exists a monic polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$. The set of all integers in L is a (commutative) ring, called the ring of integers in L and denoted by $\mathcal{O}_L$. For $K = \mathbb{Q}(\zeta_m)$ we have

$$\mathcal{O}_K = \mathbb{Z}[\zeta_m] = \mathbb{Z} \oplus \zeta_m \mathbb{Z} \oplus \cdots \oplus \zeta_m^{\varphi(m)-1}\mathbb{Z}.$$

Namely, each integer $\alpha \in \mathcal{O}_K$ can be uniquely expressed as

$$\alpha = a_0 + a_1 \zeta_m + \cdots + a_{\varphi(m)-1}\zeta_m^{\varphi(m)-1} \quad (a_i \in \mathbb{Z}).$$

We denote the group of units in $\mathcal{O}_L$ by U_L, and the group of roots of unity in $\mathcal{O}_L$ by W_L. Then $W_L \subseteq U_L$, and for $K = \mathbb{Q}(\zeta_m)(2 \nmid m)$, $W_K = \langle \zeta_{2m} \rangle = \{\zeta_{2m}^i : 0 \leq i \leq 2m-1\}$ and for $\alpha \in \mathcal{O}_K$, we have $\alpha \in W_K$ if and only if $|\sigma(\alpha)| = 1$ for each $\sigma \in Gal(K/\mathbb{Q})$.

FACT(3). Let L be a number field. Any nonzero ideal A of $\mathcal{O}_L$ can be uniquely (up to the order) expressed as

$$A = P_1^{a_1} \cdots P_s^{a_s},$$

where $P_1, \ldots, P_s$ are distinct (nonzero) prime ideals of $\mathcal{O}_L$ and $a_i \geq 1$ $(1 \leq i \leq s)$. In other words, the set $S(L)$ of all nonzero ideals of $\mathcal{O}_L$ is a free multiplicative commutative semigroup with a basis $B(L)$, the set of all nonzero prime ideals of $\mathcal{O}_L$. Such semigroup $S(L)$ can be extended to the commutative group $I(L)$, called the group of fractional ideals of L. Each element of $I(L)$, called a fractional ideal, has the form AB^{-1} where A, B are ideals of $\mathcal{O}_L$. For each $\alpha \in L^* = L\backslash\{0\}$, $\alpha\mathcal{O}_L$ is a fractional ideal, called a principal fractional ideal. And we have $(\alpha\mathcal{O}_L)(\beta\mathcal{O}_L) = \alpha\beta\mathcal{O}_L$ and $(\alpha\mathcal{O}_L)^{-1} = \alpha^{-1}\mathcal{O}_L$. Therefore, the set $P(L)$ of all principal fractional ideals is a subgroup of $I(L)$.

FACT(4). The group $C(L) = \frac{I(L)}{P(L)}$ is finite and called the (ideal) class group of L. $|C(L)|$ is called the class number of L, denoted by $h(L)$. An element $[A]$ of $C(L)$ is called the ideal class of a fractional ideal A. Therefore, $[A]^{h(L)} = 1$ for any ideal class $[A]$ in $C(L)$.

FACT(5). Let $K = \mathbb{Q}(\zeta_m)$ where $2 \nmid m \geq 3$, and $G = Gal(K/\mathbb{Q}) = \{\sigma_a : a \in \mathbb{Z}_m^*\}$. Let $H = \langle \sigma_2 \rangle$ be the cyclic subgroup of G generated by σ_2 and M be the subfield of K corresponding to H by Galois Theory. Namely, for $\alpha \in K$, we have $\alpha \in M$ if and only if $\sigma_2(\alpha) = \alpha$. H and M are called the decomposition group and decomposition field of 2 in K, respectively. We have

$$[K : M] = |H| =: r, \ [M : \mathbb{Q}] = [G : H] = \frac{\varphi(m)}{r} =: g,$$

where $[K : M] = dim_M K$, the dimension of K as a vector space over M, $[G : H] = \left|G/H\right|$. And $r = ord_2(m)$, the order of 2 in $\mathbb{Z}_m^*$. That is, r is the least positive integer such that $2^r \equiv 1 \pmod{m}$.

$2\mathscr{O}_M$ is an ideal of $\mathscr{O}_M$ and

$$2\mathscr{O}_M = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_g,$$

where $\mathfrak{p}_i$ are distinct prime ideals of $\mathscr{O}_M$. For each $1 \le i \le g$, $\mathfrak{p}_i\mathscr{O}_K = P_i$ is a prime ideal of $\mathscr{O}_K$. Therefore, we have the decomposition of 2 in $\mathscr{O}_K$ as

$$2\mathscr{O}_K = P_1 P_2 \cdots P_g,$$

where $P_1, \ldots, P_g$ are distinct prime ideals of $\mathscr{O}_K$. From $\mathfrak{p}_i \subseteq \mathscr{O}_M$ we know that $\sigma_2(P_i) = \sigma_2(\mathfrak{p}_i\mathscr{O}_K) = \sigma_2(\mathfrak{p}_i)\mathscr{O}_K = \mathfrak{p}_i\mathscr{O}_K = P_i \quad (1 \le i \le g)$.

FACT(6). (decomposition law in imaginary quadratic fields) Let $d = p_1 \cdots p_s$ where $p_1, \ldots, p_s$ are distinct odd prime numbers, $s \ge 1$, $K = \mathbb{Q}(\sqrt{-d})$. Then

(I). $\mathscr{O}_K = \{A + B\sqrt{-d} : A,\ B \in \mathbb{Z}\}$, if $d \equiv 1 \pmod{4}$;

$\mathscr{O}_K = \{\frac{1}{2}(A + B\sqrt{-d}) : A,\ B \in \mathbb{Z},\ A \equiv B \pmod{2}\}$, if $d \equiv 3 \pmod{4}$;

(II).

$$2\mathscr{O}_K = \begin{cases} P^2, & if\ d \equiv 1 \pmod{4} \\ P\bar{P}, P \ne \bar{P}, & if\ d \equiv 7 \pmod{8} \\ P, & if\ d \equiv 3 \pmod{8}; \end{cases}$$

(III). For any odd prime number p,

$$p\mathscr{O}_K = \begin{cases} P^2, & if\ p|d \\ P\bar{P}, P \ne \bar{P}, & if\ p \nmid d \text{ and } \left(\frac{-d}{p}\right) = 1 \\ P, & if\ p \nmid d \text{ and } \left(\frac{-d}{p}\right) = -1, \end{cases}$$

where P denotes a prime ideal of $\mathscr{O}_K$, $\bar{P} = \{\bar{\alpha} : \alpha \in P\}$ and $\left(\frac{-d}{p}\right)$ is the Legendre symbol.

After above preparations, we can prove the following result.

Theorem 1 *Let m and n be odd positive integers. Assume that the following semiprimitive condition is satisfied.*

There exists a positive integer l such that

$$2^l \equiv -1 \pmod{m}. \tag{5}$$

Then there is no (m, n)-GBF and $(2m, n)$-GBF for any odd integer $n \ge 1$.

Proof For any odd integer $n \ge 1$, if there is no $(2m, n)$-GBF, then by Lemma 2(2) there is no (m, n)-GBF. So we only need to show that there is no $(2m, n)$-GBF.

Suppose that there exists a GBF $f : \mathbb{Z}_2^n \to \mathbb{Z}_{2m}$, then $\alpha = W_f(0) = \sum_{x \in \mathbb{Z}_2^n} \zeta_{2m}^{f(x)} \in \mathscr{O}_K$ where $K = \mathbb{Q}(\zeta_{2m}) = \mathbb{Q}(\zeta_m)$, $\mathscr{O}_K = \mathbb{Z}[\zeta_m]$ by FACT(2). And $\alpha\bar{\alpha} = \left|W_f(0)\right|^2 = 2^n$ since f is a GBF. Let l be the least positive integer satisfying (5). Then $r = ord_2(m) = 2l$ and, by FACT(5), we have

$$2\mathscr{O}_K = P_1 \cdots P_g,\ g = \frac{\varphi(m)}{r},$$

where P_i are distinct prime ideals of $\mathscr{O}_K$, and

$$2^n\mathscr{O}_K = (P_1 \cdots P_g)^n. \tag{6}$$

On the other hand, from $\alpha \mid \alpha\bar{\alpha} = 2^n$, where $\bar{\alpha}$ is the complex conjugate number of α, we have

$$\alpha\mathscr{O}_K = P_1^{a_1} \cdots P_g^{a_g} \quad (a_i \geq 0).$$

By FACT(5), we know that $\sigma_2(P_i) = P_i$, so that $\sigma_{-1}(P_i) = \sigma_{2^l}(P_i) = P_i$ $(1 \leq i \leq g)$. Therefore,

$$\sigma_{-1}(\alpha)\mathscr{O}_K = \sigma_{-1}(P_1)^{a_1} \cdots \sigma_{-1}(P_g)^{a_g} = P_1^{a_1} \cdots P_g^{a_g} = \alpha\mathscr{O}_K.$$

But $\alpha = \sum_{i=0}^{\varphi(m)-1} a_i \zeta_m^i$ $(a_i \in \mathbb{Z})$ by FACT(2), so we get

$$\sigma_{-1}(\alpha) = \sum_{i=0}^{\varphi(m)-1} a_i (\zeta_m^{-1})^i = \bar{\alpha}.$$

Therefore,

$$\alpha\bar{\alpha}\mathscr{O}_K = (\alpha\mathscr{O}_K)(\sigma_{-1}(\alpha)\mathscr{O}_K) = P_1^{2a_1} \cdots P_g^{2a_g}. \tag{7}$$

From uniqueness of the decompositions (6) and (7) of $\alpha\bar{\alpha} = 2^n$, we have $2a_1 = n$ which contradicts to $2 \nmid n$. Therefore, there is no $(2m, n)$-GBF for any odd integer $n \geq 1$. This completes the proof of Theorem 1. □

At the beginning of the paper [1], the author presented an explicit description on odd integers $m \geq 3$ satisfying the semiprimitive condition (5) (for $m = 1$, this condition is true automatically). For each nonzero integer d, let $d = 2^t d'$ where $t \geq 0$ and $2 \nmid d'$. We denote t by $V_2(d)$. For easy displaying, we let $d_i := ord_2(p_i)$ in the following.

Lemma 4 [1] *Let $m = p_1^{a_1} \cdots p_s^{a_s}$ $(s \geq 1)$ where p_i are distinct odd prime numbers. Then there exists $l \geq 1$ such that $2^l \equiv -1 \pmod{m}$ if and only if $V_2(d_i) \geq 1$ is independent of i.*

Now we determine $V_2(d_i)$. If $p_i \equiv 7 \pmod{8}$, then $2^{\frac{p_i-1}{2}} \equiv \left(\frac{2}{p_i}\right) = 1 \pmod{p_i}$. Since $2 \nmid \frac{p_i-1}{2}$ and $d_i \mid \frac{p_i-1}{2}$, we know that $V_2(d_i) = 0$. If $p_i \equiv 3 \pmod{8}$, then $2^{\frac{p_i-1}{2}} \equiv \left(\frac{2}{p_i}\right) = -1 \pmod{p_i}$. Therefore, $d_i = 2a$, where $a \mid \frac{p_i-1}{2}$. Since $\frac{p_i-1}{2}$ is odd, a is odd and $V_2(d_i) = V_2(2) = 1$. If $p_i \equiv 5 \pmod{8}$, then $2^{\frac{p_i-1}{2}} \equiv \left(\frac{2}{p_i}\right) = -1 \pmod{p_i}$ and $\frac{p_i-1}{2} = 2b$, $2 \nmid b$. Thus $d_i = 4b'$, $b' \mid b$, so that $V_2(d_i) = V_2(4) = 2$. At last, for $p_i \equiv 1 \pmod{8}$, Table 1 below shows that $V_2(d_i)$ can be different integers.

For odd $m = p_1^{a_1} \cdots p_s^{a_s}$, by Theorem 1 and Lemma 4 we know that if $V_2(d_i) \geq 1$ is independent of i, then there is no (m, n)-GBF and $(2m, n)$-GBF for any odd integer $n \geq 1$. Therefore, we get the following result.

Corollary 3 *Let $m = p_1^{a_1} \cdots p_s^{a_s}$ where p_i are distinct odd prime numbers and $a_i \geq 1$. Then there is no (m, n)-GBF and $(2m, n)$-GBF for all odd integers $n \geq 1$ provided one of the following conditions is satisfied.*

Table 1 The values of $V_2(d_i)$ for prime numbers $p_i \equiv 1 \pmod{8}$

$p_i \equiv 1 \pmod{8}$	17	41	73	89	97	113	137	193	257	1553	1777	65,537
d_i	8	20	9	11	48	28	68	96	16	194	74	32
$V_2(d_i)$	3	2	0	0	3	2	2	5	4	1	1	5

(I): For each $1 \le i \le s$, $p_i \equiv 3 \pmod 8$, or $p_i \equiv 1 \pmod 8$ with $V_2(d_i) = 1$;
(II): For each $1 \le i \le s$, $p_i \equiv 5 \pmod 8$, or $p_i \equiv 1 \pmod 8$ with $V_2(d_i) = 2$;
(III): For each $1 \le i \le s$, $p_i \equiv 1 \pmod 8$ and $V_2(d_i) \ge 3$ is independent of i.

Remark 2 At the end of this section we explain the meaning of the semiprimitive condition (5). Let $K = \mathbb{Q}(\zeta_m)$, $2 \nmid m$, and M be the decomposition field of 2 in K. The decomposition group of 2 is the subgroup $\langle \sigma_2 \rangle$ of $G = Gal(K/\mathbb{Q}) = \{\sigma_a : a \in \mathbb{Z}_m^*\}$. Then there exists $l \ge 1$ such that $2^l \equiv -1 \pmod m \Leftrightarrow \sigma_{-1}(= \sigma_2^l) \in \langle \sigma_2 \rangle \Leftrightarrow$ for each $\alpha \in M$, $\bar{\alpha}(= \sigma_{-1}(\alpha)) = \alpha \Leftrightarrow M \subseteq \mathbb{R}$.

Namely, the semiprimitive condition (5) is equivalent to M is a real number field. In the next section, we will show several new nonexistence results on GBF for the field M is not real.

5 Nonexistence results (III): field-descent

In this section we use the field-descent method given in [1] to show some nonexistence results on (m, n)-GBFs for odd integers $n \ge 1$. The method is based on the following result.

Lemma 5 *[1] Let $K = \mathbb{Q}(\zeta_m)$ and M be the decomposition field of 2 in K. If there exists $\alpha \in \mathcal{O}_K$ such that $\alpha\bar{\alpha} = 2^n$, then there is $\beta \in \mathcal{O}_K$ such that $\beta^2 \in \mathcal{O}_M$ and $\beta\bar{\beta} = 2^n$. Moreover, if $[K : M]$ is odd, then $\beta \in \mathcal{O}_M$.*

From Corollary 3 we know that for an odd prime number p, there is no $(2p^l, n)$-GBF for any $l \ge 1$ and odd numbers $n \ge 1$ if $p \equiv 3, 5 \pmod 8$, or $p \equiv 1 \pmod 8$ and $V_2(ord_2(p)) \ge 1$. For the remaining (non-semiprimitive) case $p \equiv 7 \pmod 8$, we have the following result.

Theorem 2 *Let $m = p^l$, where $l \ge 1$ and $p \equiv 7 \pmod 8$ be a prime number. Let $s = \frac{g}{2}$, where g is defined as before and λ be the least positive odd integer such that $x^2 + py^2 = 2^{\lambda+2}$ has a solution (x, y), $x, y \in \mathbb{Z}$. Then there is no $(2p^l, n)$-GBF for any odd integer $1 \le n < \frac{\lambda}{s}$.*

Proof Suppose there exists a $(2p^l, n)$-GBF f, then $\alpha = W_f(0) \in \mathcal{O}_K$ $(K = \mathbb{Q}(\zeta_{p^l}))$ and $\alpha\bar{\alpha} = 2^n$. By Lemma 5, there exists $\beta \in \mathcal{O}_K$ such that $\beta^2 \in \mathcal{O}_M$ and $\beta\bar{\beta} = 2^n$, where M is the decomposition field of 2 in K. Since $\left(\frac{2}{p}\right) = 1$, $[K : M] = r$ is odd. Therefore, $\beta \in \mathcal{O}_M$ and $[M : \mathbb{Q}] = g = 2s$, where s is odd since $\varphi(p^l) = (p-1)p^{l-1} \equiv 2 \pmod 4$. The Galois group $G = Gal(K/\mathbb{Q})$ is isomorphic to the cyclic group $\mathbb{Z}_{p^l}^*$. By Galois theory, there exists an unique quadratic field T, $\mathbb{Q} \subset T \subseteq M$, $[T : \mathbb{Q}] = 2$ and $[M : T] = s$. It is well known that T is the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$ $\big($one of the ways for proving this fact is by the quadratic Gauss sum $\sum_{i=1}^{p-1} \left(\frac{i}{p}\right)\zeta_p^i = \sqrt{-p}$, so that $\sqrt{-p} \in \mathbb{Q}(\zeta_p) \subseteq \mathbb{Q}(\zeta_m) = K$ and $T = \mathbb{Q}(\sqrt{-p})\big)$.

$$\begin{tikzcd}
K = \mathbb{Q}(\zeta_m) \arrow[d, dash, "r"'] & (1) \arrow[d, dash] \\
M \arrow[d, dash, "s"'] & \langle \sigma_2 \rangle \arrow[dd, dash] \\
T = \mathbb{Q}(\sqrt{-p}) \arrow[d, dash, "2"'] & \\
\mathbb{Q} & G
\end{tikzcd}$$

Table 2 The values of s and λ for prime numbers $p \equiv 7 \pmod{8}$

p	7	23	31	47	71	79	103	127	151	191	199
s	1	1	3	1	1	1	1	9	5	1	1
$h(T)$	1	3	3	5	7	5	5	5	7	13	9
λ	1	3	3	5	7	5	5	5	7	13	9

Let $N_{M/T} : M \longrightarrow T$ be the norm mapping and $\gamma = N_{M/T}(\beta) \in \mathscr{O}_T$, then $\gamma\bar{\gamma} = N_{M/T}(\beta)N_{M/T}(\bar{\beta}) = N_{M/T}(\beta\bar{\beta}) = N_{M/T}(2^n) = 2^{ns}$ where ns is odd. By FACT(6) in Sect. 4, $\gamma \in \mathscr{O}_T$ can be expressed as $\gamma = \frac{1}{2}(A + B\sqrt{-p})$ where $A, B \in \mathbb{Z}$, $A \equiv B \pmod{2}$. Therefore, $2^{ns} = \gamma\bar{\gamma} = \frac{1}{4}(A^2 + pB^2)$. By the definition of λ and $2 \nmid ns$ we get $ns \geq \lambda$. Therefore, there is no $(2p^l, n)$-GBF if $2 \nmid n$ and $n < \frac{\lambda}{s}$. This completes the proof of Theorem 2. □

Remark 3 (A). Let p be an odd prime number. For any $l \geq 1$, we denote $r_l = ord_2(p^l)$ and $g_l = \frac{\varphi(p^l)}{r_l}$. It is easy to see that if $2^{p-1} \not\equiv 1 \pmod{p^2}$, then $r_l = p^{l-1}r_1$, so that $g_l = \frac{\varphi(p^l)}{r_l} = \frac{\varphi(p)p^{l-1}}{r_1 p^{l-1}} = g_1$ for all $l \geq 2$. It is known that $2^{p-1} \not\equiv 1 \pmod{p^2}$ for all odd prime numbers $p < 6 \cdot 10^9$ except $p = 1093$ and 3511. Thus it is enough to compute g_1 for such p.

(B). The definition of λ is elementary. Now we prove the existence of λ and explain its meaning from an algebraic number theory point of view. Since λ is the least odd integer such that $x^2 + py^2 = 2^{\lambda+2}$ has a solution $(x, y) = (A, B) \in \mathbb{Z}^2$, we know that both A and B are odd, so that $\delta = \frac{1}{2}(A + B\sqrt{-p}) \in \mathscr{O}_T$ and $\delta\bar{\delta} = 2^\lambda$. From $p \equiv 7 \pmod{8}$ we know that $2\mathscr{O}_T = P\bar{P}$ where P and $\bar{P} = \sigma_{-1}(P)$ are distinct prime ideals of $\mathscr{O}_T$ (FACT(6) in Sect. 4). Let $[P]$ be the ideal class of P in the class group $C(T)$. We have $1 = [2\mathscr{O}_T] = [P][\bar{P}]$, so that $[\bar{P}] = [P]^{-1}$. From $\delta\bar{\delta}\mathscr{O}_T = 2^\lambda\mathscr{O}_T = P^\lambda\bar{P}^\lambda$ and the minimum property of λ we get $\delta\mathscr{O}_T = P^\lambda$ or $\bar{P}^\lambda$ and λ is the order of $[P]$ in $C(T)$. Therefore, $\lambda | h(T)$ (the class number of T). By Gauss's genus theory, $h(T)$ is odd for $T = \mathbb{Q}(\sqrt{-p})$ and $p \equiv 7 \pmod{8}$. On the other hand, we have $2^{\lambda+2} = A^2 + pB^2 > p$ which implies that $\lambda > \frac{\log p}{\log 2} - 2$. In particular, we have $\lambda \geq 3$ if $p \equiv 7 \pmod{8}$ and $p \geq 23$. And $\lambda = h(T)$ if $h(T)$ is a prime number.

Example 2 There are 11 primes satisfying $p \equiv 7 \pmod{8}$ within 200. Table 2 presents the values of s, $h(T)$ and λ for $T = \mathbb{Q}(\sqrt{-p})$.

For $p = 47, 79$ and 103, we have $s = 1$ and $\lambda = 5$. By Theorem 2, there is no $(2 \cdot p^l, 1)$-GBF and $(2 \cdot p^l, 3)$-GBF for all $l \geq 1$. For $p = 199$, we have $s = 1$ and $\lambda = 9$. There is no $(2 \cdot 199^l, n)$-GBF for $n = 1, 3, 5, 7$ and all $l \geq 1$. Similarly, there is no $(2 \cdot 191^l, n)$-GBF for $n = 1, 3, 5, 7, 9, 11$ and all $l \geq 1$.

The following two corollaries are direct consequences of Theorem 2 and Remark 3.

Corollary 4 *Suppose that* $p \equiv 7 \pmod{8}$ *is a prime number,* $2^{p-1} \not\equiv 1 \pmod{p^2}$*, and* $ord_2(p) = \frac{p-1}{2}$*. Then there is no* $(2p^l, n)$*-GBF for all* $l \geq 1$ *and* $2 \nmid n < \lambda$ *where* λ *is defined in Theorem 2.*

Corollary 5 *Suppose that* $p \equiv 7 \pmod{8}$ *is a prime number,* $p \geq 23$, $2^{p-1} \not\equiv 1 \pmod{p^2}$ *and the ideal class number* $h(T)$ *of* $T = \mathbb{Q}(\sqrt{-p})$ *is a prime number. Then there is no* $(2p^l, n)$*-GBF for all* $l \geq 1$ *and* $2 \nmid n < \frac{h(T)}{s}$ *where* $s = \frac{g_1}{2}$.

From now on we assume $m = p_1^{a_1} p_2^{a_2}$ where p_1, p_2 are distinct odd prime numbers, $a_1, a_2 \geq 1$. Let $r' = ord_2(p_1^{a_1})$, $r'' = ord_2(p_2^{a_2})$, then $r = ord_2(m) = lcm\{r', r''\}$. Let M_1, M_2 and M be the decomposition fields of 2 in $K_1 = \mathbb{Q}(\zeta_{p_1^{a_1}})$, $K_2 = \mathbb{Q}(\zeta_{p_2^{a_2}})$ and $K = \mathbb{Q}(\zeta_m) = K_1K_2$, respectively. Then $g_1 = [M_1 : \mathbb{Q}] = \frac{\varphi(p_1^{a_1})}{r'}$, $g_2 = [M_2 : \mathbb{Q}] = \frac{\varphi(p_2^{a_2})}{r''}$ and $g = [M : \mathbb{Q}] = \frac{\varphi(m)}{r} = \frac{\varphi(p_1^{a_1})\varphi(p_2^{a_2})}{lcm\{r', r''\}} = \frac{\varphi(p_1^{a_1})}{r'}\frac{\varphi(p_2^{a_2})}{r''} \cdot gcd\{r', r''\} = g_1g_2 \cdot gcd\{r', r''\}$.

Theorem 3 *Suppose $p_1 \equiv 7 \pmod 8$, $p_2 \equiv 3, 5 \pmod 8$ and $m = p_1^{a_1} p_2^{a_2}$ $(a_1, a_2 \geq 1)$. Then $g = 2s$ and s is odd, where g is defined as above. Let $\lambda_1 \geq 1$ be the least odd integer such that $x^2 + p_1y^2 = 2^{\lambda_1+2}$ has a solution (x, y), $x, y \in \mathbb{Z}$. Let $\lambda_2 \geq 1$ be the least odd integer such that $x^2 + p_1y^2 = 2^{\lambda_2+2}p_2$ has a solution (x, y), $x, y \in \mathbb{Z}$. (If there is no solution $(x, y) \in \mathbb{Z}^2$ of $x^2 + p_1y^2 = 2^{\lambda_2+2}p_2$ for any odd $\lambda_2 \geq 1$, we assume that $\lambda_2 = +\infty$). Let $\lambda = min\{\lambda_1, \lambda_2\}$. Then there is no (m, n)-GBF and $(2m, n)$-GBF provided one of the following conditions is satisfied.*

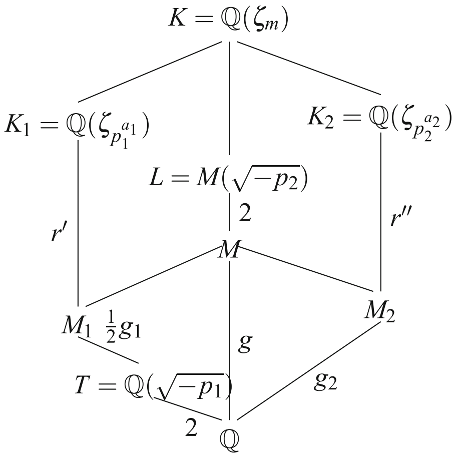
(I). $2 \nmid n < \frac{\lambda_1}{s}$ and $\left(\frac{-p_1}{p_2}\right) = -1$;

(II). $2 \nmid n < \frac{\lambda}{s}$ and $\left(\frac{-p_1}{p_2}\right) = 1$.

Proof Firstly, we consider the case $p_1 \equiv 7 \pmod 8$ and $p_2 \equiv 3 \pmod 8$. We know that

$$r' \text{ is odd and } r' \mid \frac{1}{2}\varphi\left(p_1^{a_1}\right) = \frac{p_1 - 1}{2} p_1^{a_1-1},$$
$$r'' = 2b,\ b \text{ is odd and } b \mid \frac{1}{2}\varphi\left(p_2^{a_2}\right) = \frac{p_2 - 1}{2} p_2^{a_2-1}.$$

Therefore, $g_1 = \frac{\varphi(p_1^{a_1})}{r'} \equiv 2 \pmod 4$, $g_2 = \frac{\varphi(p_2^{a_2})}{r''}$ is odd, and $g = g_1g_2 \cdot gcd\{r', r''\} = 2s$, $2 \nmid s$. The imaginary quadratic field $T = \mathbb{Q}(\sqrt{-p_1})$ is a subfield of K_1. Since $M \cap K_i = M_i$ $(i = 1, 2)$ and $[M_1 : \mathbb{Q}] = g_1$ is even, $[M_2 : \mathbb{Q}] = g_2$ is odd, we know that $T \subseteq M_1 \subseteq M$, $\sqrt{-p_2} \notin M$. Therefore, $L = M(\sqrt{-p_2})$ is a quadratic extension of M in K. Moreover, since $Gal(K/M)$ is the cyclic group generated by σ_2 and $[K : M] = \frac{\varphi(m)}{g}$ is even, we know that L is the unique quadratic extension of M in K.


$K = \mathbb{Q}(\zeta_m)$
$K_1 = \mathbb{Q}(\zeta_{p_1^{a_1}})$
$K_2 = \mathbb{Q}(\zeta_{p_2^{a_2}})$
$L = M(\sqrt{-p_2})$
2
r'
r''
M
M_1 $\frac{1}{2}g_1$
M_2
g
$T = \mathbb{Q}(\sqrt{-p_1})$
g_2
2
$\mathbb{Q}$

Suppose that there exists a $(2m, n)$-GBF, $2 \nmid n \geq 1$. Then we have $\alpha \in \mathcal{O}_K$ such that $\alpha\bar{\alpha} = 2^n$. By Lemma 5, there is a $\beta \in \mathcal{O}_L$ such that $\beta^2 \in \mathcal{O}_M$ and $\beta\bar{\beta} = 2^n$. Since

$\{1, \sqrt{-p_2}\}$ is a basis for extension L/M, we have $\beta = A + B\sqrt{-p_2}$, $A, B \in M$. By $\beta^2 = A^2 - p_2B^2 + 2AB\sqrt{-p_2} \in \mathscr{O}_M$ and $\sqrt{-p_2} \notin M$ we get $AB = 0$. Therefore, $\beta = A \in \mathscr{O}_L \cap M = \mathscr{O}_M$ or $\beta = B\sqrt{-p_2} \in \mathscr{O}_L$.

If $\beta = A \in \mathscr{O}_M$, then $\gamma = N_{M/T}(\beta) \in \mathscr{O}_T$ where $N_{M/T}(\beta) = \Pi_{\sigma \in Gal(M/T)}\sigma(\beta)$ is the norm mapping from M to T (and also from $\mathscr{O}_M$ to $\mathscr{O}_T$). We have $\gamma\bar{\gamma} = N_{M/T}(\beta\bar{\beta}) = N_{M/T}(2^n) = 2^{ns}$ where $s = \frac{g}{2} = [M : T]$. By FACT(6) in Sect. 4, $\gamma = \frac{1}{2}(x + y\sqrt{-p_1})$ where $x, y \in \mathbb{Z}$. Then $x^2 + p_1y^2 = 4\gamma\bar{\gamma} = 2^{ns+2}$. From $2 \nmid ns$ and the definition of λ_1 we get $ns \geq \lambda_1$.

If $\beta = B\sqrt{-p_2} \in \mathscr{O}_L$ and $B \in M$, consider the element $\gamma = \prod_{\sigma \in Gal(L/T)/Gal(L/M)} \sigma(\beta) = \prod_{\sigma \in Gal(M/T)} \sigma(B) \cdot \prod_{\sigma \in Gal(L/T)/Gal(L/M)} \sigma(\sqrt{-p_2}) = N_{M/T}(B) \cdot (\pm\sqrt{-p_2})^s$ where $N_{M/T}(B) \in T$. Let $\delta = N_{M/T}(B)p_2^{\frac{s+1}{2}} \in T \cap \mathscr{O}_L = \mathscr{O}_T$. Then $\delta = \frac{1}{2}(x + y\sqrt{-p_1})$, $x, y \in \mathbb{Z}$ and $x^2 + p_1y^2 = 4\delta\bar{\delta} = 4N_{M/T}(B\bar{B})p_2^{s+1} = 4\gamma\bar{\gamma}p_2 = 2^{ns+2}p_2$. Therefore, $p_2 \nmid xy$ and $x^2 \equiv -p_1y^2 \pmod{p_2}$. So $\left(\frac{-p_1}{p_2}\right) = 1$. This means that if $\left(\frac{-p_1}{p_2}\right) = -1$ then $\beta = B\sqrt{-p_2}$ is impossible. If $\left(\frac{-p_1}{p_2}\right) = 1$, from $x^2 + p_1y^2 = 2^{ns+2}p_2$ and the definition of λ_2 we get $ns \geq \lambda_2$.

In summary, if there is a $(2m, n)$-GBF with odd n, then $n \geq \frac{\lambda_1}{s}$ when $\left(\frac{-p_1}{p_2}\right) = -1$ and $n \geq min\{\frac{\lambda_1}{s}, \frac{\lambda_2}{s}\} = \frac{\lambda}{s}$ when $\left(\frac{-p_1}{p_2}\right) = 1$. This completes the proof of Theorem 3 for the case $p_1 \equiv 7 \pmod 8$ and $p_2 \equiv 3 \pmod 8$.

Now we consider the case $p_1 \equiv 7 \pmod 8$ and $p_2 \equiv 5 \pmod 8$. In this case,

$$r' \text{ is odd and } r' \mid \frac{1}{2}\varphi\left(p_1^{a_1}\right),$$
$$r'' = 4b,\ b \text{ is odd and } b \mid \frac{1}{4}\varphi\left(p_2^{a_2}\right).$$

Therefore, $g_1 = \frac{\varphi(p_1^{a_1})}{r'} \equiv 2 \pmod 4$, $g_2 = \frac{\varphi(p_2^{a_2})}{r''}$ is odd, and $g = g_1g_2 \cdot gcd\{r', r''\} = 2s$, $2 \nmid s$. Then we have the same field extension diagram as the one in the case $(p_1, p_2) \equiv (7, 3) \pmod 8$ except $L = M(\sqrt{p_2})$ for $p_2 \equiv 5 \pmod 8$. The conclusion can be derived by the similar argument. This completes the proof of Theorem 3. □

Remark 4 We have seen the existence of λ_1 in Remark (B) of Theorem 2. Namely, $2\mathscr{O}_T = P\bar{P}$ and λ_1 is the order of the ideal class $[P]$ in the class group $C(T)$. In particular, $\lambda_1 \mid h(T) = |C(T)|$. By Gauss's genus theory, $h(T)$ is odd, and so is λ_1.

Now we give a method to determine the value of λ_2 in the case $p_1 \equiv 7 \pmod 8$, $p_2 \equiv 3, 5 \pmod 8$ and $\left(\frac{-p_1}{p_2}\right) = 1$. By definition, $\lambda_2 = +\infty$ if the equation $x^2 + p_1y^2 = 2^{l+2}p_2$ has no solution $(x, y) \in \mathbb{Z}^2$ for any odd integer $l \geq 1$. Otherwise λ_2 is the least odd integer such that $x^2 + p_1y^2 = 2^{\lambda_2+2}p_2$ has a solution $(x, y) \in \mathbb{Z}^2$. We claim that if $\lambda_2 \neq +\infty$, then $\lambda_2 \leq \lambda_1$. So that $\lambda = min\{\lambda_1, \lambda_2\} = \lambda_2$.

Suppose that $\lambda_2 \neq +\infty$, then $x^2 + p_1y^2 = 2^{\lambda_2+2}p_2$ has a solution $(x, y) = (A, B) \in \mathbb{Z}^2$. From the minimal property of λ_2 we know that $2 \nmid AB$, and so $\pi = \frac{1}{2}(A + B\sqrt{-p_1}) \in \mathscr{O}_T$. Therefore,

$$(\pi\mathscr{O}_T)(\overline{\pi}\mathscr{O}_T) = (2^{\lambda_2}p_2)\mathscr{O}_T = (P\bar{P})^{\lambda_2}Q\bar{Q}.$$

The last equation is because of $2\mathscr{O}_T = P\bar{P}$ and $p_2\mathscr{O}_T = Q\bar{Q}$.

Again, from the minimal property of λ_2 we get

$$\pi\mathscr{O}_T = (P')^{\lambda_2}Q',\ \ P' \in \{P, \bar{P}\},\ \ Q' \in \{Q, \bar{Q}\}.$$

Therefore, $[P']^{\lambda_2}[Q'] = 1$. Namely, $[Q']$ belongs to the cyclic group of order λ_1 generated by $[P]$. On the other hand, suppose that $[P']^l[Q'] = 1$ for some l, $0 \le l < \lambda_1 - 1$. If l is odd, then $\lambda_2 = l \le \lambda_1 - 1$. If l is even, then $[\bar{P}']^{\lambda_1 - l}[\bar{Q}'] = ([P']^l[Q'])^{-1} = 1$ so that $\lambda_2 = \lambda_1 - l \le \lambda_1$.

In summary, if the equation $x^2 + p_1y^2 = 2^{l+2}p_2$ has no solution $(x, y) \in \mathbb{Z}^2$ for $l = 0, 1, \ldots, \lambda_1 - 1$, then $\lambda_2 = +\infty$ and $\lambda = \lambda_1$. Otherwise, there exists an unique odd l such that $1 \le l \le \lambda_1$ and $x^2 + p_1y^2 = 2^{l+2}p_2$ has a solution $(x, y) \in \mathbb{Z}^2$. Then $\lambda_2 = l \le \lambda_1$ and $\lambda = min\{\lambda_1, \lambda_2\} = \lambda_2$.

Example 3 Consider $m = p_1^{a_1}p_2^{a_2}$ where $p_1 = 199 \equiv 7 \pmod 8$. By Table 2 we know that $g_1 = 2$, $r' = \frac{\varphi(p_1^{a_1})}{g_1} = 99 \cdot 199^{a_1-1}$ and $\lambda_1 = 9$.

(1). For $p_2 = 59 \equiv 3 \pmod 8$, $r'' = 2b$, $b = 29 \cdot 59^{a_2-1}$, $g_2 = 1$. Thus $g = g_1g_2 \cdot gcd\{r', r''\} = 2$ and $s = \frac{g}{2} = 1$. Since $\left(\frac{-p_1}{p_2}\right) = \left(\frac{-199}{59}\right) = -1$. By Theorem 3 we get that there is no $(199^{a_1} \cdot 59^{a_2}, n)$-GBF and $(2 \cdot 199^{a_1} \cdot 59^{a_2}, n)$-GBF for $a_1,\ a_2 \ge 1$ and $n = 1, 3, 5, 7$.

(2). For $p_2 = 101 \equiv 5 \pmod 8$, $r'' = 4b$, $b = 25 \cdot 101^{a_2-1}$, $g_2 = 1$. Thus $g = g_1g_2 \cdot gcd\{r', r''\} = 2$ and $s = \frac{g}{2} = 1$. Since $\left(\frac{-p_1}{p_2}\right) = \left(\frac{-199}{101}\right) = -1$, by Theorem 3 we get that there is no $(199^{a_1} \cdot 101^{a_2}, n)$-GBF and $(2 \cdot 199^{a_1} \cdot 101^{a_2}, n)$-GBF for $a_1, a_2 \ge 1$ and $n = 1, 3, 5, 7$.

(3). For $p_2 = 5$, $r'' = 4b$, $b = 5^{a_2-1}$, $g_2 = 1$. Thus $g = g_1g_2 \cdot gcd\{r', r''\} = 2$ and $s = \frac{g}{2} = 1$. From $11^2 + 199 \cdot 1^2 = 320 = 2^6 \cdot 5$ we get $\lambda_2 = 9 - 4 = 5$ (in fact, $21^2 + 199 \cdot 1^2 = 2^7 \cdot 5$) and $\lambda = \lambda_2 = 5$. Since $\left(\frac{-p_1}{p_2}\right) = \left(\frac{-199}{5}\right) = 1$, by Theorem 3 we get that there is no $(199^{a_1} \cdot 5^{a_2}, n)$-GBF and $(2 \cdot 199^{a_1} \cdot 5^{a_2}, n)$-GBF for $a_1, a_2 \ge 1$ and $n = 1, 3$.

Theorem 4 *Suppose that* $p_1 \equiv 3 \pmod 8$, $p_2 \equiv 5 \pmod 8$ *and* $m = p_1^{a_1}p_2^{a_2}$ $(a_1,\ a_2 \ge 1)$. *Then* $g = 2s$ *and* s *is odd. Let* $\lambda \ge 1$ *be the least odd integer such that* $p_1x^2 + p_2y^2 = 2^{\lambda+2}$ *has a solution* (x, y), $x,\ y \in \mathbb{Z}$. *Then there is no* (m, n)*-GBF and* $(2m, n)$*-GBF provided* n *is odd and one of the following conditions is satisfied.*

(I). $\left(\frac{p_2}{p_1}\right) = 1$*; or*

(II). $\left(\frac{p_2}{p_1}\right) = -1$ *and* $n < \frac{\lambda}{s}$.

Proof We have

$$r' = 2a,\ \ 2 \nmid a,\ \ g_1 = \frac{\varphi\left(p_1^{a_1}\right)}{r'} \text{ is odd,}$$

$$r'' = 4b,\ \ 2 \nmid b,\ \ g_2 = \frac{\varphi\left(p_2^{a_2}\right)}{r''} \text{ is odd.}$$

Therefore, $g = g_1g_2 \cdot gcd\{r', r''\} = 2g_1g_2 \cdot gcd\{a, b\} = 2s$, $2 \nmid s$. From $2 \nmid g_1g_2$ we know that neither $\mathbb{Q}(\sqrt{-p_1})$ nor $\mathbb{Q}(\sqrt{p_2})$ are subfields of M. Therefore, $\sigma_2(\sqrt{-p_1}) = -\sqrt{p_1}$ and $\sigma_2(\sqrt{p_2}) = -\sqrt{p_2}$, so that $\sigma_2(\sqrt{-p_1p_2}) = \sqrt{-p_1p_2}$ which means $T = \mathbb{Q}(\sqrt{-p_1p_2})$ is the quadratic subfield of M and the quadratic extension of M is $L = M(\sqrt{p_2})$ $(= M(\sqrt{-p_1}))$. Thus we have the field extension diagram as following.

$$\begin{tikzcd}
 & K=\mathbb{Q}(\zeta_m) \arrow[dl, -] \arrow[d, -] \arrow[dr, -] & \\
K_1=\mathbb{Q}(\zeta_{p_1^{a_1}}) \arrow[ddd, -, "r'"'] & \arrow[d, -] & K_2=\mathbb{Q}(\zeta_{p_2^{a_2}}) \arrow[ddd, -, "r''"] \\
 & L=M(\sqrt{p_2}) \arrow[d, -, "2"] & \\
 & M \arrow[dl, -] \arrow[d, -, "s"] \arrow[dr, -] & \\
M_1 \arrow[ddr, -, "g_1"'] & T=\mathbb{Q}(\sqrt{-p_1p_2}) \arrow[d, -, "2"] & M_2 \arrow[ddl, -, "g_2"] \\
 & \arrow[d, -] & \\
 & \mathbb{Q} &
\end{tikzcd}$$

Suppose that there exists a $(2m, n)$-GBF and $2 \nmid n \geq 1$. Then we have $\alpha \in \mathcal{O}_L$ such that $\alpha^2 \in \mathcal{O}_M$ and $\alpha\bar{\alpha} = 2^n$. From $\alpha = A + B\sqrt{p_2}$ $(A,\ B \in M)$ and $\alpha^2 = A^2 + p_2B^2 + 2AB\sqrt{p_2} \in \mathcal{O}_M$ we know that $AB = 0$. Therefore, $\alpha = A \in M \cap \mathcal{O}_L = \mathcal{O}_M$ or $\alpha = B\sqrt{p_2}$. If $\alpha = A \in \mathcal{O}_M$, then $\beta = N_{M/T}(\alpha) \in \mathcal{O}_T$ and $\beta\bar{\beta} = N_{M/T}(\alpha\bar{\alpha}) = N_{M/T}(2^n) = 2^{ns}$. By $\beta = \frac{1}{2}(x + y\sqrt{-p_1p_2})$, $x,\ y \in \mathbb{Z}$, we have $x^2 + p_1p_2y^2 = 2^{ns+2}$. So that $x^2 \equiv 2^{ns+2} \pmod{p_1}$ and then $\left(\frac{2}{p_1}\right) = 1$ since $2 \nmid ns$. But $\left(\frac{2}{p_1}\right) = -1$ since $p_1 \equiv 3 \pmod 8$. We get a contradiction. Therefore, $\alpha = B\sqrt{p_2} \in \mathcal{O}_L,\ B \in M$. Let

$$\gamma = \prod_{\sigma \in Gal(L/T)/Gal(L/M)} \sigma(\alpha) = N_{M/T}(B)(\pm\sqrt{p_2}^{s}) \in \mathcal{O}_L,$$

where $N_{M/T}(B) \in T$. Then $\delta = N_{M/T}(B)p_2^{\frac{s+1}{2}} = \gamma\sqrt{p_2} \in \mathcal{O}_L \cap T = \mathcal{O}_T$ and

$$\delta\bar{\delta} = N_{M/T}(B\bar{B})p_2^{s+1} = \gamma\bar{\gamma}p_2 = \left(\prod_{\sigma}(\alpha\bar{\alpha})\right)p_2 = 2^{ns}p_2.$$

By $\delta = \frac{1}{2}(x + y\sqrt{-p_1p_2})$, $x,\ y \in \mathbb{Z}$ we get $x^2 + p_1p_2y^2 = 2^{ns+2}p_2$, which implies $x^2 \equiv 2^{ns+2}p_2 \pmod{p_1}$. Thus $1 = \left(\frac{2p_2}{p_1}\right) = -\left(\frac{p_2}{p_1}\right)$, and $p_2|x$. So that $p_2(\frac{x}{p_2})^2 + p_1y^2 = 2^{ns+2}$. By the definition of λ we get $ns \geq \lambda$.

In summary, there is no (m, n)-GBF and $(2m, n)$-GBF if $2 \nmid n$ and $\left(\frac{p_2}{p_1}\right) = 1$, or $2 \nmid n < \frac{\lambda}{s}$ and $\left(\frac{p_2}{p_1}\right) = -1$. This completes the proof of Theorem 4. □

Remark 5 We explain the existence of λ in the case $p_1 \equiv 3 \pmod 8$, $p_2 \equiv 5 \pmod 8$ and $\left(\frac{p_2}{p_1}\right) = -1$. By definition, λ is the least odd integer such that $x^2 + p_1p_2y^2 = 2^{\lambda+2}p_2$ has a solution $(x, y) \in \mathbb{Z}^2$. By FACT(6) in Sect. 4, we have the decomposition in $T = \mathbb{Q}(\sqrt{-p_1p_2})$, $p_2\mathcal{O}_T = Q^2$ and $2\mathcal{O}_T = P\bar{P}$ since $-p_1p_2 \equiv 1 \pmod 8$. We know that $Q = (p_2, \sqrt{-p_1p_2})$ is not a principal (prime) ideal in $\mathcal{O}_T$ and $[Q]^2 = [(p_2\mathcal{O}_T)] = 1$. Thus the order of $[Q]$ is two. We also know that $h(T) = 2k$, $2 \nmid k$ ([6], Propositions 3 and 4). Let d be the order of $[P]$, then $x^2 + p_1p_2y^2 = 2^{d+2}$ has a solution $(x, y) \in \mathbb{Z}^2$. Thus $x^2 \equiv 2^{d+2} \pmod{p_1}$, so that $1 = \left(\frac{2}{p_1}\right)^{d+2} = (-1)^{d+2}$, which implies that $2 \mid d$ and $d = 2e$. Since $d \mid h(T) = 2k$

we get $e \mid k$. Therefore, e is odd. Thus both $[P^e]$ and $[Q]$ are elements of order two. Since the size of the class group $C(T)$ is $h(T) \equiv 2 \pmod 4$ and then it has unique element of order two, we get $[P^e] = [Q]$. Therefore, $[P^e Q] = 1$. Namely, $P^e Q$ is a principal ideal $\alpha \mathcal{O}_T$, where $\alpha = \frac{1}{2}(x + y\sqrt{-p_1 p_2})$, $(\alpha\bar{\alpha})\mathcal{O}_T = (P\bar{P})^e Q\bar{Q} = (2^e p_2)\mathcal{O}_T$. Therefore, $x^2 + p_1 p_2 y^2 = 2^{e+2} p_2$, $2 \nmid e$. From the minimal property of λ we get that λ is just e, the half of the order of $[P]$.

Example 4 Let $m = p_1^{a_1} p_2^{a_2}$ $(a_1, a_2 \geq 1)$ where $p_1 = 19 \equiv 3 \pmod 8$, $p_2 = 29 \equiv 5 \pmod 8$, then $\left(\frac{p_2}{p_1}\right) = \left(\frac{29}{19}\right) = -1$, $r' = 18 \cdot 19^{a_1 - 1}$, $g_1 = 1$, $r'' = 28 \cdot 29^{a_2 - 1}$, $g_2 = 1$ and so $g = g_1 g_2 \cdot gcd\{r', r''\} = 2$, $s = \frac{g}{2} = 1$. The equation $19x^2 + 29y^2 = 2^{l+2}$ has no solution $(x, y) \in \mathbb{Z}^2$ for $l = 1, 3, 5, 7, 9$ and 11, but $2^{13+2} = 32768 = 19 \cdot 21^2 + 29 \cdot 29^2$. We get $\lambda = 13$ and , by Theorem 4, there is no $(19^{a_1} 29^{a_2}, n)$-GBF and $(2 \cdot 19^{a_1} 29^{a_2}, n)$-GBF and for any $a_1, a_2 \geq 1$ and $n = 1, 3, 5, 7, 9, 11$.

6 Conclusion

In this paper we deal with the existence problem of generalized bent function $f : \mathbb{Z}_2^n \to \mathbb{Z}_m$, called a (m, n)-GBF. In Sect. 2 we proved that there is a (m, n)-GBF if $2 \mid gcd\{m, n\}$ or $4 \mid m$. For the remaining cases we presented a series of nonexistence results in Sects. 3–5 including the following results.

There is no (m, n)-GBF for any odd integer $n \geq 1$ if one of the following conditions on m is satisfied (p, $p_1, \ldots, p_s$ denote odd prime numbers, a, $a_1, \ldots, a_s \geq 1$).

(A). $m = p^a$ (Corollary 2);

(B). $m = 2p^a$, $p \equiv 3, 5 \pmod 8$, or $p \equiv 1 \pmod 8$ and $ord_2(p)$ is even (Corollary 3);

(C). $m = 2p_1^{a_1} p_2^{a_2}$, $p_1 \equiv 3 \pmod 8$, $p_2 \equiv 5 \pmod 8$ and $\left(\frac{p_2}{p_1}\right) = 1$ (Theorem 4);

(D). $m = 2p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$, $p_1, \ldots, p_s$ are distinct and $p_1 \equiv p_2 \equiv \ldots \equiv p_s \equiv 3 \pmod 8$, or $p_1 \equiv p_2 \equiv \ldots \equiv p_s \equiv 5 \pmod 8$ (Corollary 2);

In Sect. 4, the decomposition field M of 2 in $K = \mathbb{Q}(\zeta_m)$ is real. For all cases in Sect. 5, $[M, \mathbb{Q}] = 2s$, $2 \nmid s$ and M contains an imaginary quadratic subfield T. The nonexistence results are derived by using field-descent method from K to M (Lemma 5), then from M to T by norm mapping, and by using some knowledge on the decomposition law of prime numbers in $\mathcal{O}_T$ and the structure of the class group of T. Next step we may consider the case that $[M, \mathbb{Q}] = 4s$, $2 \nmid s$ and M contains an imaginary quadratic subfield T. In this case we would use specific knowledge on integral basis of $\mathcal{O}_T$, the decomposition law in $\mathcal{O}_T$ and the structure of the class group of T. The derived conditions on nonexistence of GBF would be more complicated if the Galois group $G(T/\mathbb{Q})$ is cyclic.

Acknowledgements The authors are very grateful to the three anonymous reviewers and the editors for all their helpful and constructive comments that much improved the quality of the paper. K. Feng is supported by NSFC with No. 11471178, NSFC with No. 11571007 and the National Lab. on Information Science and Technology of Tsinghua University. R. Feng is supported by NSFC with No. 61370187.

References

1. Feng K.: Generalized bent functions and class group of imaginary quadratic fields. Sci. China Ser. A **44**, 562–570 (2001).

2. Ireland K., Rosen M.I.: A Classical Introduction to Modern Number Theory, GTM 84. Springer, New York (1990).
3. Kumar P.V., Scholtz R.A., Welch L.R.: Generalized bent functions and their roperties. 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. Li N., Tang X., Helleseth T.: New classes of generalized Boolean bent functions over $\mathbb{Z}_4$. In: Caire G., Effros M., Loeliger H.-A., Vardy A. (eds.) Proceedings of 2012 IEEE International Symposium on Information Theory, 841C845 (2012).
6. Pizer A.: On the 2-part of the class number of imaginary quadratic number fields. J. Number Theory **8**(2), 184–192 (1976).
7. Rothaus O.S.: On bent functions. J. Comb. Theory Ser. A **20**(3), 300–305 (1976).
8. Schmidt K.-U.: Quaternary constant-amplitude codes for multicode CDMA. IEEE Trans. Inf. Theory **55**(4), 1824–1832 (2009).
9. Schmidt K.-U.: $\mathbb{Z}_4$-valued quadratic forms and quaternary sequence families. IEEE Trans. Inf. Theory **55**(12), 5803–5810 (2009).
10. Solé P., Tokareva N.: Connections between quaternary and binary bent functions. http://eprint.iacr.org/2009/544.
11. Stănică P., Martinsen T.: Octal bent generalized Boolean functions. arXiv:1102.4812.
12. Stănică P., Martinsen T., Gangopadhyay S., Singh B.K.: Bent and generalized bent Boolean functions. Des. Codes Cryptogr. **69**(1), 77–94 (2013).
13. Tokareva N.N.: Generalizations of bent functions. A survey. J. Appl. Ind. Math. **5**(1), 110–129 (2011).
14. Washington L.C.: Introduction to Cyclotomic Fields, GTM 83. Springer, New York (1997).