Generalized bent functions and class group of imaginary quadratic fields

FENG Keqin (冯克勤)

Department of Mathematical Sciences, Tsinghua University, Beijing 100084, China (email: kfeng@math.tsinghua.edu.cn)

Received May 10, 2000

Abstract Several new results on non-existence of generalized bent functions are presented. The results are related to the class number of imaginary quadratic fields.

Keywords: generalized bent functions, imaginary quadratic fields.

1 Preliminaries

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

$$\left| \sum_{x \in \mathbb{Z}_q^n} \zeta_q^{f(x) - x \cdot y} \right| = q^{n/2} \tag{1.1}$$

holds for every $y \in \mathbb{Z}_q^n$ where $x \cdot y$ stands for the dot product. We call $[n, q]$ the type of such GBF f. GBFs have been used in many fields such as code-division multiple-access communication systems and cryptography. For more background information of GBF and its applications, see ref. [1] and references therein.

Bent functions (for $q = 2$) are initiated by Rothaus[2] in 1976 and generalized by Kumar et al.[1] in 1985. For $q = 2$, Rothaus proved that there exists a bent function with type $[n, 2]$ if and only if n is even. The GBFs with type $[n, q]$ have been constructed in ref. [1] for even n or $q \not\equiv 2 \pmod 4$. From now on we assume that

(*) n is odd and $q = 2N$, $2 \nmid N \geqslant 3$.

So far there is no GBF being constructed in the case (*), but several non-existence results of GBF have been presented under the following extra conditions:

(A)[1] there exists an integer $s \geqslant 1$ such that

$$2^s \equiv -1 \pmod N, \tag{1.2}$$

(B)[3] $(n, q) = (1, 14)$,

(C)[4] $n = 1$ and $N = p^l$ where $l \geqslant 1$, p is a prime number such that $p \equiv 7 \pmod 8$ and $p \neq 7$,

(D)[5] $n = 1$, $N = p_1^{e_1} \cdots p_g^{e_g}$ where $g \geqslant 1$, $p_1, \cdots, p_g$ are distinct prime numbers, $e_i \geqslant 1$ $(1 \leqslant i \leqslant g)$ and for each $i (1 \leqslant i \leqslant g)$ there exists $s_i \geqslant 1$ such that

$$p_i^{s_i} \equiv -1 \left(\bmod \frac{N}{p_i^{e_i}} \right).$$

(D) is a generalization of (B) and (C). In this paper we present some new results on the non-existence of GBF with type $[n, q]$ for $2 \nmid n \geqslant 3$.

To show that our results (Theorems 3.1 and 4.1) are new ones, we need a closed form of condition (1.2). Such a closed form was presented in ref. [4] as follows. Let

$$N = \prod_{i=1}^{l} p_i^{e_i}$$

be the decomposition of an odd integer N where $p_i (1 \leqslant i \leqslant l)$ are distinct prime numbers and $e_i \geqslant 1 (1 \leqslant i \leqslant l)$. By the Chinese Remainder Theorem, condition (1.2) means that

$$2^s \equiv -1 \pmod{p_i^{e_i}} \ (1 \leqslant i \leqslant l). \tag{1.3}$$

We denote by $I(p)$ the 2-part of the order of $2 \pmod p$. It is easy to see that condition (1.3) is equivalent to the condition that

$$I(p_i) \ (1 \leqslant i \leqslant l) \text{ are the same even integers.} \tag{1.4}$$

It is easy to see that $I(p^e) = 2, 4, 1$ for $p \equiv 3, 5, 7 \pmod 8$, respectively, so that condition (1.2) contains exactly the following five cases:

(A_1) $N = \prod_{i=1}^{l} p_i^{e_i}$, $p_i \equiv 1 \pmod 8$ $(1 \leqslant i \leqslant l)$ and $I(p_i)$ $(1 \leqslant i \leqslant l)$ are the same even integers.

(A_2) $N = \prod_{i=1}^{l} p_i^{e_i}$, $p_i \equiv 3 \pmod 8$ $(1 \leqslant i \leqslant l)$,

(A_3) $N = \prod_{i=1}^{l} p_i^{e_i}$, $p_i \equiv 5 \pmod 8$ $(1 \leqslant i \leqslant l)$,

(A_4) $N = \prod_{i=1}^{l} p_i^{e_i} \cdot \prod_{j=1}^{s} p_j'^{f_j}$, $p_i \equiv 3 \pmod 8$ $(1 \leqslant i \leqslant l)$, $p_j' \equiv 1 \pmod 8$ and $I(p_j') = 2$ $(1 \leqslant j \leqslant s)$,

(A_5) $N = \prod_{i=1}^{l} p_i^{e_i} \cdot \prod_{j=1}^{s} p_j'^{f_j}$, $p_i \equiv 5 \pmod 8$ $(1 \leqslant i \leqslant l)$, $p_j' \equiv 1 \pmod 8$ and $I(p_j') = 4$ $(1 \leqslant j \leqslant s)$.

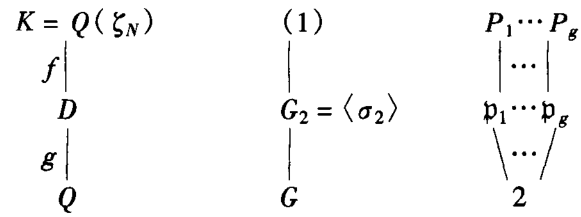
In sec. 3 we will present some new results on the non-existence of GBF in the case of $N = p^e p'^{e'}$.

At the end of this section, we explain the meaning of algebraic number theory of condition (1.3). Let K be the cyclotomic number field $\mathbb{Q}(\zeta_N)$. The Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^\times$ by

$$G \simeq (\mathbb{Z}/N\mathbb{Z})^\times, \ \sigma_a \mapsto a \pmod N, \ (a, N) = 1, \tag{1.5}$$

where σ_a is the isomorphism determined by $\sigma_a(\zeta_N) = \zeta_N^a$. Let D be the decomposition field of 2 in K and $G_2 = \mathrm{Gal}(K/D)$ be the decomposition group of 2 in K. Then G_2 is the cyclic subgroup of G generated by σ_2. Therefore $f = |G_2| = [K:D]$ is the order of σ_2 in G or, by the isomorphism (1.5), f is the order of $2 \pmod N$. And $g = [D:\mathbb{Q}] = [K:\mathbb{Q}]/[K:D] = \frac{\varphi(N)}{f}$ where $\varphi(N)$ stands for the Euler function. For an algebraic number field F, we denote by O_F the ring of integers in F. Then 2 splits completely in $D: 2O_D = \mathfrak{p}_1 \cdots \mathfrak{p}_g$, and each $\mathfrak{p}_i$ is inertia in K.

By isomorphism (1.5), condition (1.3) means that σ_{-1}(the complex conjugation) belongs to $G_2 = \langle \sigma_2 \rangle$ which is also equivalent to the fact that D is a real field. All the results in the next two sections belong to the case $\sigma^{-1} \notin G_2$.



2 Two lemmas

In this and next two sections we fix the following notations.

n is an odd positive integer,

N is an odd positive integer, $N \geqslant 3$,

$q = 2N$,

$K = \mathbb{Q}(\zeta_N)$, $\zeta_N = e^{\frac{2\pi i}{N}}$,

$G = \mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_a : 1 \leqslant a \leqslant N-1,\ (a, N) = 1\}$,

D is the decomposition field of 2 in K,

$G_2 = \mathrm{Gal}(K/D) = \langle \sigma_2 \rangle$ stands for the decomposition group of 2 in K,

$f = [K:D] = |G_2|$ stands for the order of $2 \pmod N$,

O_F the ring of integers in an algebraic number field F,

$g = [D:\mathbb{Q}] = \frac{\varphi(N)}{f}$ stands for the number of prime ideals in O_K above 2.

Suppose that there exists a GBF with type $[n, q]$, $q = 2N$. Since N is odd, condition (1.1) implies that there exists $\xi \in O_K = \mathbb{Z}[\zeta_N]$ such that $\xi \bar{\xi} = q^n = 2^n N^n$ where $\bar{\xi} = \sigma_{-1}(\xi)$ is the complex conjugation of ξ. The first result we use in this paper is

Lemma 2.1[5]. Let $N = \prod_{i=1}^{l} p_i^{e_i}$ where $l \geqslant 1$, $p_1, \cdots, p_l$ are distinct prime numbers, $e_i \geqslant 1$ $(1 \leqslant i \leqslant l)$, and for each i $(1 \leqslant i \leqslant l)$ there exists a positive integer s_i such that

$$p_i^{s_i} \equiv -1 \left(\bmod \frac{N}{p_i^{e_i}}\right).$$

If we have $\xi \in O_K$ such that $\xi \bar{\xi} = 2^n N^n$, then we have $\alpha \in O_K$ such that $\alpha \bar{\alpha} = 2^n$.

Remark. The condition of Lemma 2.1 is trivial for $l = 1$ (so N is a power of an odd prime number). For $l \geqslant 2$, we denote by I_{ij} the 2-part of multiplicative order of $p_i \pmod{p_j}$. It is easy to see that the condition of Lemma 2.1 is equivalent to the saying that for each i $(1 \leqslant i \leqslant l)$, I_{ij} $(1 \leqslant j \leqslant l,\ j \neq i)$ are the same even integers (depending on i only).

The second result we need in this paper says that number α in Lemma 2.1 can be found in a smaller field.

Lemma 2.2. If $\alpha \bar{\alpha} = 2^n$ for some $\alpha \in O_K$, then there exists $\beta \in O_K$ such that $\beta^2 \in O_D$ and $\beta \bar{\beta} = 2^n$. Moreover, $\beta \in O_D$ if f is odd.

Proof. We follow the idea in the proof of the Lemma 2 in ref. [4], but make some simplifications. Since σ_2 fixes all prime ideals of O_K above 2, from $\alpha \bar{\alpha} = 2$ we know that

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

Therefore $\sigma_2(\alpha) = \alpha\varepsilon$ where $\varepsilon \in U_k$ (the unit group of O_K). For each $\sigma \in G$,

$$\sigma(\alpha)\overline{\sigma(\alpha)} = \sigma(\alpha\bar{\alpha}) = 2^n, \quad \sigma\sigma_2(\alpha) = \sigma(\alpha\varepsilon) = \sigma(\alpha)\sigma(\varepsilon).$$

Thus

$$2^n = \sigma\sigma_2(\alpha)\overline{\sigma\sigma_2(\alpha)} = \sigma(\alpha)\sigma(\varepsilon)\overline{\sigma(\alpha)\sigma(\varepsilon)} = 2^n\sigma(\varepsilon)\overline{\sigma(\varepsilon)},$$

which means that $|\sigma(\varepsilon)| = 1$ for all $\sigma \in G$. Thus ε is a root of 1 in K, namely $\varepsilon = \pm\delta$ and $\delta = \zeta_N^i$ for some integer i. Let $\beta = \alpha\delta^{-1}$. Then $\beta\bar{\beta} = \alpha\bar{\alpha} = 2^n$ and

$$\sigma_2(\beta) = \sigma_2(\alpha)\sigma_2(\delta)^{-1} = \alpha\varepsilon\delta^{-2} = \pm\alpha\delta^{-1} = \pm\beta.$$

Therefore $\sigma_2(\beta^2) = \beta^2$ which means that $\beta^2 \in O_D$. Moreover, we have $D \subseteq D(\beta) \subseteq K$ and $[D(\beta):D] \leqslant 2$. If $f = [K:D]$ is odd, then $D(\beta) = D$ so that $\beta \in O_D$. This completes the proof of Lemma 2.2.

3 Non-existence result for case $N = p^l$, $p \equiv 7 \pmod 8$

Now we present some new result on non-existence of GBF for $n > 1$.

Theorem 3.1. Let $N = p^l$ where $l \geqslant 1$ $p \equiv 7 \pmod 8$, let f be the order of $2 \pmod{p^l}$, $s = \frac{g}{2}\left(= \frac{\varphi(p^l)}{2f} \text{ is odd}\right)$, let m be the smallest odd integer such that $x^2 + py^2 = 2^{m+2}$ has integral solution (x, y), and let n be an odd positive integer. If $n < m/s$, then there is no GBF with type $[n, p]$ $(q = 2N)$.

Proof. Suppose that there exists a GBF with type $[n, p]$. From (1.1) we know that $\beta\bar{\beta} = q^n = 2^nN^n = 2^np^{ln}$ for some $\beta \in O_K$. By Lemmas 2.1 and 2.2 we know that $\beta\bar{\beta} = 2^n$ for some $\beta \in O_D$. Let $E = \mathbb{Q}(\sqrt{-p})$ be the unique quadratic subfield of D. Then $[D:E] = \frac{g}{2} = s$ is odd. Let $\gamma = N_{D/E}(\beta)$. Then $\gamma\bar{\gamma} = N_{D/E}(\beta\bar{\beta}) = 2^{sn}$ and $\gamma \in O_E$ so that $\gamma = \frac{1}{2}(A + B\sqrt{-p})$ where $A, B \in \mathbb{Z}$. Therefore we have $A^2 + pB^2 = 4\gamma\bar{\gamma} = 2^{sn+2}$. By the definition of m we know $m \leqslant sn$. Therefore there is no GBF with type $[n, p]$ if $m > sn$. This completes the proof of Theorem 1.

Remark 1. Let p be a fixed odd prime number. For all $l \geqslant 1$, we denote by f_l the order of $2 \pmod{p^l}$ and $g_l = \varphi(p^l)/f_l$. It is easy to see that if $2^{p-1} \not\equiv 1 \pmod{p^2}$, then $f_l = p^{l-1}f_1$ and $g_l = \frac{\varphi(p^l)}{f_l} = \frac{p^{l-1}(p-1)}{p^{l-1}f_1} = g_1$ for all $l \geqslant 1$. It is a well-known fact that the formula $2^{p-1} \not\equiv 1 \pmod{p^2}$ holds for all odd prime numbers $p < 6 \times 10^9$ except $p = 1093$ and 3511 (see Ribenboim's book[6] for instance). Therefore we have $g_l = g_1$ for all $l \geqslant 1$ so that it is enough to compute $g = g_1$ for such a prime number p.

Remark 2. The definition of m is elementary; it has a clear algebraic number theory meaning. Since m is the smallest odd integer such that the equation $x^2 + py^2 = 2^{m+2}$ has integral solution $(x, y) = (A, B)$, we know that both of A and B should be odd, so that $\delta = \frac{1}{2}(A + B\sqrt{-p}) \in O_E$ $(E = \mathbb{Q}(\sqrt{-p}))$ and $\delta\bar{\delta} = 2^m$. We know that 2 splits in O_E as $2O_E = \mathfrak{p}\bar{\mathfrak{p}}$. The minimum property of m implies that $\delta O_E = \mathfrak{p}^m$ or of $\bar{\mathfrak{p}}^m$. Therefore $\mathfrak{p}^m$ is a principal ideal, so that m is a factor of the class number $h(-p)$ of $E = \mathbb{Q}(\sqrt{-p})$. By Gauss' genus theory we know that $h(-p)$ is odd for $p \equiv 7 \pmod 8$. On the other hand, we have $2^{m+2} = A^2 + pB^2 > p$ which gives a lower bound of m, $m > \frac{\log p}{\log 2} - 2$. Particularly we have $m \geqslant 3$ if $p \equiv 7 \pmod 8$ and $p \neq 7$. Therefore if $h(-p)$ is a prime number, then $m = h(-p)$.

Example 1. There are 11 pirme numbers $p \equiv 7 \pmod 8$ within 200. The following table shows the values of g, $h(-p)$ and m for these primes.

p	7	23	31	47	71	79	103	127	151	191	199
$g=2s$	2	2	6	2	2	2	2	18	10	2	2
$h(-p)$	1	3	3	5	7	5	5	5	7	13	9
m	1	3	3	5	7	5	5	5	7	13	0

For all $23 \leqslant p \leqslant 191$, $p \equiv 7 \pmod 8$ and $h(-p)$ are prime number so that $m = h(-p)$. For $p = 199$, $m \mid 9 = h(-199)$ and $m > \frac{\log 199}{\log 2} - 2 > 3$; thus $m = 9$.

For $p = 23, 47, 71, 79, 103, 191$, we have $s = \frac{g}{2} = 1$, so that there is no GBF with type $[n, 2p^l]$ for all $l \geqslant 1$ if n is odd and less than m.

From the above observation Theorem 1 has following corollaries.

Corollary 1. Suppose that $p \equiv 7 \pmod 8$, $p \geqslant 7$, $2^{p-1} \not\equiv 1 \pmod{p^2}$ and the order f of $2 \pmod p$ is $\frac{p-1}{2}$. Then there is no GBF with type $[n, 2p^l]$ for all $l \geqslant 1$ if n is odd and less than m where m is defined in Theorem 1.

Corollary 2. Suppose that $p \equiv 7 \pmod 8$, $p > 7$, $2^{p-1} \not\equiv 1 \pmod{p^2}$ and the class number $h(-p)$ of $\mathbb{Q}(\sqrt{-p})$ is a prime number. Then there is no GBF with type $[n, 2p^l]$ for all $l \geqslant 1$ if n is odd and less than $h(-p)/s$ where $s = \frac{p-1}{2f}$ and f is the order of $2 \pmod p$.

4 Non-existence result: $N = p^l p'^{l'}$

In this section we consider the case $N = p^l p'^{l'}$, where $l, l' \geqslant 1$, p and p' are distinct prime numbers, and do not belong to cases (A_1)—(A_5) in sec. 1. But we assume that N satisfies the condition of Lemma 2.1; that is, there exist positive integers s and s' such that

$$p^s \equiv -1 \pmod{p'^{l'}}, \quad p'^{s'} \equiv -1 \pmod{p^l}.$$

It is easy to see that this condition is equivalent to the following condition:

(*) both of the order of $p \pmod{p'}$ and the order of $p' \pmod p$ are even.

Theorem 4.1. Suppose that $N = p^l p'^{l'}$ where $l, l' \geqslant 1$, $p \equiv 3 \pmod 4$, $p' \equiv 5 \pmod 8$, and primes p and p' satisfy condition (*) (which is equivalent to $\left(\frac{p}{p'}\right) = -1$). Let f be the order of $2 \pmod N$, and $g = \frac{\varphi(N)}{f}$. Then g is even and $s = g/2$ is odd.

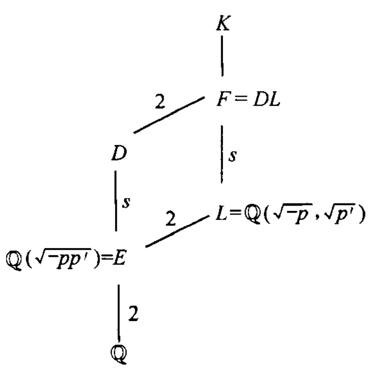
(1) In the case $p \equiv 3 \pmod 8$. Let $E = \mathbb{Q}(\sqrt{-pp'})$. Then $2O_E = P\overline{P}$ where P and $\overline{P}$ are distinct prime ideals in O_E. Let m be the smallest positive integer such that the equation $p'y^2 + pz^2 = 2^{m+2}$ has an integral solution (y, z). Then m is odd and the order of ideal class $[P]$ in the class group of E is $2m$. Moreover, there is no GBF with type $[n, 2N]$ if $2 \nmid n < m/s$.

(2) In the case $p \equiv 7 \pmod 8$. Let $E = \mathbb{Q}(\sqrt{-p})$. Then $2O_E = P\overline{P}$. Let m be the smallest odd integer such that the equation $x^2 + pz^2 = 2^{m+2}$ has an integral solution (x, z). Then m is the order of $[P]$ in the class group of E. Moreover, there is no GBF with type $[n, 2N]$ if $2 \nmid n < m/s$.

Proof. Let t and t_1 be the orders of $2 \pmod{p^l}$ and $\pmod{p'^{l'}}$, respectively. From $p \equiv 3 \pmod 4$ and $p' \equiv 5 \pmod 8$ we know that $t_1 = 4t'$ where t' is odd. Therefore $f = [t, 4t'] = 4a$ and a is odd, so that $s = \frac{g}{2} = \frac{\varphi(N)}{2f}$ is odd. Let D be the decomposition field of 2 in $K = \mathbb{Q}(\zeta_N)$. Then $[D:\mathbb{Q}] = g = 2s$.

Suppose that there exists GBF with type $[n, 2N]$ where $2 \nmid n \geqslant 1$. Then we have $\xi \in O_K$ such that $\xi\bar{\xi} = (2N)^n$. Since N satisties condition (*), by Lemma 2.1 we have $\alpha \in O_K$ such that $\alpha\bar{\alpha} = 2^n$. Then by Lemma 2.2 we have $\beta \in O_K$ such that $\beta^2 \in O_D$ and $\beta\bar{\beta} = 2^n$.

(1) Consider the case $p \equiv 3 \pmod 8$ first. Since $E = \mathbb{Q}(\sqrt{-pp'})$ is a subfield of K and 2 splits in E, we know that $E \subset D$ and $[D:E] = s$. From $\beta^2 \in O_D$ we know that β belongs to the unique quadratic extension F of D in K. By the Galois correspondence, $\mathrm{Gal}(K/F)$ is the cyclic subgroup of $G = \mathrm{Gal}(K/\mathbb{Q})$ generated by $\sigma_2^2 = \sigma_4$ from which we know that $L = \mathbb{Q}(\sqrt{-p}, \sqrt{p'})$ is a subfield of F and $F = DL$, $[F:L] = s$. Let $\gamma = N_{F/L}(\beta) \in O_L$. Then $\gamma\bar{\gamma} = N_{F/L}(\beta\bar{\beta}) = N_{F/L}(2^n) = 2^{ns}$ and $\gamma^2 = N_{F/L}(\beta^2) = N_{D/E}(\beta^2) \in O_E$.



It is well known that $\left\{1,\ \alpha = \frac{1+\sqrt{p'}}{2},\ \beta = \frac{1+\sqrt{-p}}{2},\ \alpha\beta\right\}$ is an integral basis of O_L (see exercise 42(d) of ref. [3], page 52 for instance). Therefore

$$\gamma = A + B\alpha + C\beta + D\alpha\beta \quad (A, B, C, D \in \mathbb{Z})$$
$$= \frac{1}{4}(X + Y\sqrt{p'} + Z\sqrt{-p} + W\sqrt{-pp'}),$$

where

$$X = 4A + 2B + 2C + D,\ Y = 2B + D,\ Z = 2C + D,\ W = D,$$

implying that $D = W$, $C = \frac{1}{2}(Z - W)$, $B = \frac{1}{2}(Y - W)$, $A = \frac{1}{4}(X - Y - Z + W)$ and

$$X \equiv Y \equiv Z \equiv W \pmod 2,\ X + W \equiv Y + Z \pmod 4. \tag{4.1}$$

The equality $\overline{\gamma}\gamma = 2^{ns}$ becomes

$$2^{ns+4} = X^2 + p'Y^2 + pZ^2 + pp'W^2 + 2(XY + pZW)\sqrt{p'};$$

that is, (X, Y, Z, W) satisfies congruences (4.1) and equations

$$\begin{cases} X^2 + p'Y^2 + pZ^2 + pp'W^2 = 2^{ns+4}, \\ XY = -pZW. \end{cases} \tag{4.2}$$

Note that $\gamma^2 \in O_E = \mathbb{Z} + \left[\frac{1 + \sqrt{-pp'}}{2}\right]\mathbb{Z}$. If $\gamma \in O_E$, then $Y = Z = 0$ and $X^2 + pp'W^2 = 2^{4+ns}$ which implies that $\left(\frac{2}{p}\right) = \left(\frac{2}{p}\right)^{4+ns} = 1$ since $2 \nmid ns$. But $\left(\frac{2}{p}\right) = -1$ for $p \equiv 3 \pmod 8$. Therefore $\gamma \notin O_E$ and $\gamma \in O_L$, so that $L = E(\gamma)$ ($\gamma^2 \in E$). Let σ be the non-trivial automorphism in Gal(L/E). Then $\sigma(\gamma) = -\gamma$ which means that $X - Y\sqrt{p'} - Z\sqrt{-p} + W\sqrt{-pp'} = -X - Y\sqrt{p'} - Z\sqrt{-p} - W\sqrt{-pp'}$. So we have $X = W = 0$. And congruence (4.1) becomes $Y \equiv Z \equiv 0 \pmod 2$, and (4.2) becomes $p'Y^2 + pZ^2 = 2^{4+ns}$. Let $y = \frac{Y}{2} \in \mathbb{Z}$, $z = \frac{Z}{2} \in \mathbb{Z}$. Then

$$p'y^2 + pz^2 = 2^{ns+2},\ y \equiv z \pmod 2. \tag{4.3}$$

Let m be the smallest positive integer such that the equation $p'y^2 + pz^2 = 2^{m+2}$ has integral solution $(y, z) = (A, B)$. From $-1 = \left(\frac{p'}{p}\right) = \left(\frac{2}{p}\right)^m = (-1)^m$ we know that m is odd. The minimality of m implies that $2 \nmid AB$, and

$$2^m p = \left(\frac{Bp + A\sqrt{-pp'}}{2}\right)\left(\frac{Bp - A\sqrt{-pp'}}{2}\right).$$

We have $2O_E = P\overline{P}$ and $pO_E = P'^2$. From minimality of m we know that $\left(\frac{Bp + A\sqrt{-pp'}}{2}\right)O_E = P^m P'$ or $\overline{P}^m P'$. Therefore $[P]^m[P'] = 1$. It is well known that $[P']$ is an ideal class of order 2. Therefore the order of $[P]$ is $2m$. From (3.3) and the minimality of m we have $sn \geqslant m$. Therefore there is no GBF with type $[n, 2N]$ if $2 \nmid n < \frac{m}{s}$.

(2) Next we consider the case $p \equiv 7 \pmod 8$. In this case we take $E = \mathbb{Q}(\sqrt{-p})$. By similar argument as in (1), we know that there exists

$$\gamma = \frac{1}{4}(X + Y\sqrt{p'} + Z\sqrt{-p} + W\sqrt{-pp'}) \in O_L,$$

$$\gamma^2 \in O_E = \mathbb{Z} + \left[\frac{1 + \sqrt{-p}}{2}\right]\mathbb{Z},\ \gamma\overline{\gamma} = 2^{ns}.$$

If $\gamma \notin O_E$, then $L = E(\gamma)$ ($\gamma^2 \in O_E$) and $X = Z = 0$. Therefore $\overline{\gamma\gamma} = 2^{ns}$ means that $2^{ns+4} = p'(Y^2 + pW^2)$ which is impossible. Thus $\gamma \in O_E$ which implies $Y = W = 0$, $X^2 + pZ^2 = 2^{ns+4}$ and $X \equiv Z \equiv 0 \pmod 2$. Let $x = \frac{X}{2} \in \mathbb{Z}$, $z = \frac{Z}{2} \in \mathbb{Z}$. Then

$$x^2 + pz^2 = 2^{ns+2}. \tag{4.4}$$

Let m be the smallest odd integer such that the equation $x^2 + pz^2 = 2^{m+2}$ has integral solution $(x, z) = (A, C)$. Then $2 \nmid AC$ and $\left(\frac{A + C\sqrt{-p}}{2}\right)\left(\frac{A - C\sqrt{-p}}{2}\right) = 2^m$. From $2O_E = P\overline{P}$ and the minimality of m we have $\left(\frac{A + C\sqrt{-p}}{2}\right)O_E = P^m$ or $\overline{P}^m$ so that m is the order of $[P]$. From (4.4) we know that $ns \geqslant m$. Therefore there is no GBF with type $[n, 2N]$ if $2 \nmid n < \frac{m}{s}$. This completes the proof of Theorem 2.

Remark. We denote the class number of $Q(\sqrt{-d})$ by $h(-d)$ (there is a big table in the ref. [2] for class number of imaginary quadratic fields). For $p \equiv 3 \pmod 8$ we have $h(-pp') = 2t$, $2 \nmid t$ and $m \mid t$. Particularly, if t is a prime number, then $m = t = h(-pp')/2$. For $p \equiv 7 \pmod 8$ and $p > 7$, $m \mid h(-p)$, $m > 1$ and $2 \nmid h(-p)$. If $h(-p)$ is prime number, then $m = h(-p)$.

Example 2. Computation shows that all (p, p') in the following table satisfies conditions (*) (which is equivalent to $\left(\frac{p'}{p}\right) = -1$) and $p \equiv 3 \pmod 8$, $p' \equiv 5 \pmod 8$. The values of s and $h(-pp')$ are listed in the table. If $h(-pp')/2$ is prime, then $m = h(-pp')/2$. Otherwise m can be determined by definition and the fact that $m \mid h(-pp')/2$.

(p,p')	(67,5)	(83,5)	(11,13)	(59,13)	(67,13)	(83,13)	(11,29)	(19,29)	(43,29)	(19,37)
s	1	1	1	1	1	1	1	1	3	1
$h(-pp')$	18	10	10	22	22	34	10	26	26	14
m	9	5	5	11	11	17	5	13	13	7

(p,p')	(59,37)	(3,53)	(19,53)	(67,53)	(83,53)	(11,61)	(43,61)	(59,61)	(67,61)
s	1	1	1	1	1	1	3	1	1
$h(-pp')$	42	10	30	58	50	30	22	66	30
m	21	5	15	29	25	15	11	33	5

By Theorem 4.1 we know that there is no GBF with types $[3, 2\cdot 43^l \cdot 29^{l'}]$ and $[3, 2\cdot 43^l \cdot 61^{l'}]$ for all $l, l' \geqslant 1$. For remaining cases in the table we have $s = 1$, so that there is no GBF with type $[n, 2p^l p'^{l'}]$ if $2 \nmid n < m$ (for $n = 1$ the result is known[5]).

Example 3. Computation shows that all (p, p') ($p \equiv 7 \pmod 8$, $p' \equiv 5 \pmod 8$) in the following table satisfy condition (*) (namely $\left(\frac{p'}{p}\right) = -1$). For all cases $s = 1$ and $h(-p)$ is prime so that $m = h(-p)$.

(p, p')	(47, 5) (47, 13) (47,29)	(71, 13) (71,53) (71,61)	(79,29) (79,37) (79,53) (79,61)
$m = h(-p)$	5	7	5

By Theorem 4.1 we know that there is no GBF with type $[n, 2p^l p'^{l'}]$ if $2 \nmid n < h(-p)$ and (p, p') belongs to the table (for $n = 1$ the result is known[5]).

Acknowledgements This work was supported by the Fundamental Research Foundation of China (Grant No. G1999075101).

References

1. Kumar, P. V., Scholtz, R. A., Welch, L. R., Generalized bent functions and their properties, J. of Comb. Theory, Ser. A, 1985, 40: 90—107.
2. Rothaus, O. S., On bent functions, J. Comb. Theory, Ser. A, 1976, 20: 300—305.
3. Marcus, D. A., Number Fields, New York: Springer-Verlag, 1977.
4. Akyildiz, E., Guloglu, I. S., Ikeda, M., A note of generalized bent functions, Pure and Applied Alg., 1996, 106: 1.
5. Ikeda, M., A remark on the non-existence of generalized bent functions, Nunber Theory and Its Applications (Ankara 1996), 109—119, LN in Pure and Applied Math., 204, New York: Marcel Dekker, 1999.
6. Ribenboim, P., The Book of Prime Number Records, 2nd ed., New York: Springer-Verlag, 1989.