ELSEVIER
Journal of Pure and Applied Algebra 106 (1996) 1–9
JOURNAL OF PURE AND APPLIED ALGEBRA

A note of generalized bent functions

Ersan Akyildiz,*[1] Ismail Ş. Güloğlu[1], Masatoshi İkeda[2]

Department of Mathematics, Institute for Basic Sciences, Tübitak Marmara Research Center, Gebze-Kocaeli, Turkey

Communicated by J.D. Stasheff; received 22 August 1994

Abstract

Kumar et al. (1985) introduced the concept of generalized bent functions $f: \mathbb{Z}_q^n \to Z_q$ where q is a positive integer > 1, and gave constructions for such functions for every possible value of q and n other than n odd and $q \equiv 2 \pmod 4$. Furthermore, they have shown the non-existence in the remaining case under certain sufficient conditions. The main purpose of this paper is to understand the extent of the set of parameters for which no generalized bent functions exist. In particular, the non-existence of Bent functions on $\mathbb{Z}_{2^r}$ with $p \equiv 7 \pmod 8$ and $r \geq 1$ is examined. The result obtained generalizes recent works of Bi (1991) and Pei (1993).

1. Introduction

A function $f: Z_q^n \to Z_q$ with a positive integer q is called a generalized bent function if the equality

$$|(1/q^{n/2}) \sum_{x \in Z_q^n} \zeta_q^{f(x) - x \cdot y}| = 1$$

holds for every $\boldsymbol{x} \in Z_q^n$, where ζ_q stands for any complex primitive qth root of unity, and $\boldsymbol{x} \cdot \boldsymbol{y}$ for the dot product. This type of functions have been introduced by Kumar et al. [3], and it has been shown that there is no such function if n is odd, $q = 2N$ with an odd N (i.e. $q \equiv 2 \bmod 4$), and if either ($\star$) $N = 1$, or ($\star\star$) there is an integer s satisfying $2^s \equiv -1 \bmod N$. Further a method of constructing this type of functions has been given under the assumption that either n is even, or $q \not\equiv 2 \bmod 4$. By the way there is another condition equivalent to ($\star\star$) due to Kumar et al. Namely, C_N being

*Corresponding author.
[1] Present address: Department of Mathematics, Middle East Technical University, 6531 Ankara, Turkey.
[2] Present address: Department of Mathematics, Institute for Basic Sciences, Tübitak, Marmara Research Center, Gebze – Kocaeli, Turkey.

SSDI 0022-4049(94)00006-2

the cyclotomic field generated by a primitive Nth root of unity for the odd integer N above, the condition $(\star\star)$ is equivalent to that the decomposition group of 2 in C_N/Q contains the automorphism $\sigma^\star$ inducing the complex-conjugation on C_N.

As is seen, there is a gap in what Kumar et al. have done. In fact it is not clear whether or not there exist generalized bent functions if $q = 2N$ with an odd N, but none of the conditions $(\star)$ or $(\star\star)$ is satisfied. Actually Pei [4] has shown by computation that there is no generalized bent function on Z_{14}, a very special case we are interested in. The aim of this note is to point out some facts about this question: we first observe for what combinations of prime powers the condition $(\star\star)$ is actually satisfied, then we examine the existence of generalized bent functions for some case where the condition $(\star\star)$ is not satisfied.

2. The condition $(\star\star)$ and its equivalents

Let $N = \prod_{i=1}^{r} p_i^{e_i}$ be an odd integer > 1 with its factorization into primes p_i with $i = 1, \ldots, r$. In order to formulate further restatements of the condition $(\star\star)$ we need some notations and auxiliary remarks.

(1) As before C_N denotes the cyclotomic field $Q(\zeta_N)$. C_N then is the composite of $C_{p_i^{e_i}} = Q(\zeta_{p_i^{e_i}})$ for $i = 1, \ldots, r$, and $Gal(C_N/Q) \cong \prod_{i=1}^{r} Gal(C_{p_i^{e_i}}/Q)$ under the map Res defined by $\mathrm{Res}(\sigma) = \prod_{i=1}^{r} \mathrm{Res}_i(\sigma)$ for every $\sigma \in \mathrm{Gal}(C_N/Q)$ where Res_i stands for the restriction to $C_{p_i^{e_i}}$. 2 is unramified in C_N/Q, and the order of the decomposition group G_2 of 2 in $Gal(C_N/Q)$ is equal to the order f of $2 \bmod N$. G_2 is cyclic and generated by the Frobenius automorphism φ_N of 2 in C_N/Q. The restriction $\mathrm{Res}_i(\varphi_N) = \varphi_i$ is the Frobenius automorphism of 2 in $C_{p_i^{e_i}}$ for each i, and φ_i generates the decomposition group $G_2^{(i)}$ of 2 in $Gal(C_{p_i^{e_i}}/Q)$ whose order is equal to the order f_i of $2 \bmod p_i^{e_i}$.

(2) Let T be the maximal 2-subfield of C_N, i.e. the largest subfield of C_N whose degree over Q is a power of 2. As in the case of C_N, T is the composite of $T_i = T \cap C_{p_i^{e_i}}$, furthermore $Gal(T/Q) \cong \prod_{i=1}^{r} Gal(T_i/Q)$ under the map induced by the restriction. The decomposition group $\bar{G}_2$ of 2 in $\mathrm{Gal}(T/Q)$ is generated by the Frobenius automorphism $\bar{\varphi}_N$ which is equal to $\mathrm{Res}_T(\varphi_N)$ so that the order of $\bar{G}_2$ is equal to the 2-contribution of f. Similarly the decomposition group $\bar{G}_2^{(i)}$ of 2 in $Gal(T_i/Q)$ is generated by the Frobenius automorphism $\bar{\varphi}_i$ which is equal to $\mathrm{Res}_{T_i}(\varphi_i) = \mathrm{Res}_{T_i}(\varphi_N)$, and the order of $\bar{G}_2(i)$ is equal to the 2-contribution in f_i for each i. Note that, since $Gal(C_{p_i^{e_i}}/Q)$ is cyclic, $Gal(T_i/Q)$ is a cyclic 2-group so that the lattice of its subgroups is a chain.

(3) Let S be the maximal subfield of C_N of odd degree over Q. Then C_N is the composite of T and S, furthermore $Gal(C_N/Q) \cong Gal(T/Q) \times Gal(S/Q)$ by the map induced by the restriction. Note that $Gal(T/Q) \cong Gal(C_N/S)$, and the latter is the (unique) 2-Sylow subgroup of $Gal(C_N/Q)$. By the way for each i, $C_{p_i^{e_i}}$ is the composite of T_i with $S_i = S \cap C_{p_i^{e_i}}$, the largest subfield of $C_{p_i^{e_i}}$ of odd degree over Q.

(4) Let $\sigma^\star$ be the automorphism in $Gal(C_N/Q)$ inducing the complex conjugation on C_N. Since $\sigma^\star$ is of order 2, it is contained in the unique 2-Sylow subgroup $Gal(C_N/S)$ of

$Gal(C_N/Q)$. This implies that S is fixed by $\sigma^\star$ elementswise, i.e. S is a real subfield of C_N. This further implies that none of T_i $(i = 1, \ldots, r)$ is real, because otherwise $C_{p_i^{e_i}} = T_i \cdot S_i$ will be a real field for some i. Hence $\sigma_i^\star = \mathrm{Res}_{T_i}(\sigma^\star)$ is non-trivial and of order 2 in $Gal(T_i/Q)$.

After these observations we now prove the following:

Lemma 1. *Let $N = \prod_{i=1}^{r} p_i^{e_i}$ be an odd integer > 1 with its factorization into primes p_i with $i = 1, \ldots, r$. Then the following statements are equivalent to each other.*

(a) *There is an integer s satisfying $2^s \equiv -1 \bmod N$.*

(b) *The 2-contribution in the order $\bar{f}_i$ of $2 \bmod p_i$ is equal to the power 2^t with an integer $t \geq 1$ independent of i for $i = 1, \ldots, r$.*

(c) *The decomposition groups of 2 in $Gal(T_i/Q)$ $(i = 1, \ldots, r)$ are all non-trivial, and of the same order, where T_i stands for the maximal 2-subfield of the cyclotomic field $C_{p_i^{e_i}}$.*

(d) *The decomposition group of 2 in $Gal(C_N/Q)$ contains the automorphism $\sigma^\star$ inducing the complex conjugation on C_N.*

Although the equivalence of (a) and (d) has already been shown by Kumar et al. [3], for the sake of completeness, we prove the equivalence of the statements cyclically.

Proof of Lemma 1. (a) $\Rightarrow$ (b): First note that the order f_i of $2 \bmod p_i^{e_i}$ is the product of the order $\bar{f}_i$ in $2 \bmod p_i$ and a power of p_i. Hence the 2-contribution in f_i coincides with that in $\bar{f}_i$ for every $i = 1, \ldots, r$. Therefore, for our purpose, it suffices to show that all f_i $(i = 1, \ldots, r)$ have the same non-trivial 2-contribution. For this end, assume that f be the order of $2 \bmod N$, and $2^s \equiv -1 \bmod N$ for an integer s. Now write $s = fg \pm s_0$ with integers g and s_0 satisfying $0 \leq s_0 \leq f/2$. Then $2^{s_0} \equiv -1 \bmod N$. Note that $s_0 \neq 0$, because, otherwise we arrive at the impossible congruence $1 \equiv -1 \bmod N$. Now $2^{s_0} \equiv -1 \bmod N$ implies $2^{2s_0} \equiv 1 \bmod N$. Since $0 \leqq 2s_0 \leq f$, this implies that $f = 2s_0$. Hence $f = 2^t f'$ with an integer $t \geq 1$ and an odd f'. By the way, from the observation above, we obtain $2^{f/2} = 2^{s_0} \equiv -1 \bmod N$ so that $2^{f/2} \equiv -1 \bmod p_i^{e_i}$ for every $i(= 1, \ldots, r)$. Now let f_i be the order of $2 \bmod p_i^{e_i}$. Since $2^s \equiv -1 \bmod N$, we have $2^s \equiv -1 \bmod p_i^{e_i}$ for each i. Therefore, first expressing $s = f_i g_i \pm s_i$ with $g_i, s_i \in Z$ such that $0 \leq s_i \leq f_i/2$, then doing the same thing as above, we obtain $f_i = 2^{t_i} f_i'$ with $t_i \geq 1$ and odd f_i'. Further we have $2^{f_i/2} = 2^{s_i} \equiv -1 \bmod p_i^{e_i}$ for each i. Since f is the least common multiple of f_i for $i = 1, \ldots, r$ we have $t_i \leq t$. Now if $t_i < t$ for some i, say $i = 1$, then, $f = f_1 h$ with an even h. This further implies that $2^{f/2} = (2^{f_1/2})^h \equiv (-1)^h = 1 \bmod p_1^{e_1}$ contradicting the fact mentioned above. Hence $t_i = t$ for $i = 1, \ldots, r$. This completes the proof of (a) $\Rightarrow$ (b).

(b) $\Rightarrow$ (c): This follows from remark (2) above.

(c) $\Rightarrow$ (d): For each i, $Gal(T_i/Q)$ is a cyclic 2-group, and $\langle \sigma_i^\star \rangle$ is the unique minimal subgroup of $Gal(T_i/Q)$ by remark (4). Hence $\sigma_i^\star$ is a power of $\bar{\varphi}_i$, because the latter is not trivial by assumption. On the other hand all $\bar{\varphi}_i$ are of the same order, say 2^t with $t \geq 1$, by assumption, and $\sigma_i^\star$ is of order 2. Hence $\sigma_i^\star = \varphi_i^{2^{t-1}}$ for every $i = 1, \ldots, r$. This then implies that $\mathrm{Res}_T(\sigma^\star) = \mathrm{Res}_T(\varphi_i^{2^{t-1}})$ by remarks (2)–(4). But this means that

$\sigma^\star(\varphi_N)^{-2^{r-1}} \in Gal(C_N/T)$. Since $Gal(C_N/T)$ ($\cong Gal(S/Q)$) is of odd order, there is odd integer, say $2m+1$, making $(\sigma^\star(\varphi_N)^{-2^{r-1}})^{2m+1} =$ identity. But we are working in an abelian group, and $\sigma^\star$ is of order 2, hence the last equality implies that $\sigma^\star$ is a power of φ_N, i.e. $\sigma^\star$ is in the decomposition group of 2.

(d) $\Rightarrow$ (a): Because N is odd, the action of the Frobenius automorphism φ_N is completely described by $\zeta_N^{\varphi_N} = \zeta_N^2$. Now $\sigma^\star = \varphi_N^s$ for some integer s by assumption. Hence $\zeta_N^{-1} = \zeta_N^{\sigma^\star} = \zeta_N^{\varphi_N^s} = \zeta_N^{2^s}$, i.e. $2^s \equiv -1 \bmod N$. This argument is due to Kumar et al. □

3. Odd integers satisfying (★★)

We now observe for what combinations of odd primes the condition (★★) is satisfied. For this purpose we classify odd primes according to their residues mod 8. Namely let Π_v be the set of all odd primes $\equiv v \bmod 8$ for $v = 1, 3, 5, 7$ respectively. Then from the general theory of cyclotomic fields we have the following:

(0) For any odd prime p, the Galois group $Gal(C_p/Q)$ is a cyclic group of order $p-1$ where C_p denotes the cyclotomic fields $Q(\zeta_p)$ generated by a primitive pth root of unity ζ_p. Hence $Gal(T_p/Q)$ for the maximal 2-subfield T_p of C_p is a cyclic 2-group so that the lattice of its subgroups is a chain. Note that T_p is the maximal 2-subfield of C_{p^r} for any $r \geq 1$.

(1) If $p \in \Pi_1$, then the 2-contribution in $p-1$ is 2^r with $r \geq 3$, hence $[T_p : Q] = 2^r$. Since C_p contains the quadratic field $Q(\sqrt{p})$ (see [2, p. 529]), T_p contains $Q(\sqrt{p})$ as its unique minimal subfield. Moreover $(p/2) = 1$ by the second supplement to the quadratic reciprocity law (see [2], pp. 73, 90), hence 2 is decomposed in $Q(\sqrt{p})$. This means that the decomposition group of 2 in $Gal(T_p/Q)$ is a proper subgroup of $Gal(T_p/Q)$, but may be trivial.

(2) If $p \in \Pi_3$, then the 2-contribution in $p-1$ is exactly 2, hence $[T_p : Q] = 2$. On the other hand, C_p contains $Q(\sqrt{-p})$ (see [2, p. 529]), hence $T_p = Q(\sqrt{-p})$. Because $(-p/2) = -1$ (see [2, pp. 78, 90]), 2 is inert in T_p (i.e. $\langle 2 \rangle$ remains as a prime ideal of T_p). This means that the decomposition group of 2 in T_p/Q coincides with $Gal(T_p/Q)$, and is of order 2.

(3) If $p \in \Pi_5$, the 2-contribution in $p-1$ is exactly 4, hence $[T_p : Q] = 4$. Furthermore C_p contains the quadratic field $Q(\sqrt{p})$ (see [2, p. 529]), hence T_p contains $Q(\sqrt{p})$ as its unique minimal subfield. On the other hand, $(p/2) = -1$ (see [2, pp. 78, 90]), hence 2 is inert in $Q(\sqrt{p})$. Since $Q(\sqrt{p})$ is the unique minimal subfield of T_p, 2 is inert in the whole extension T_p/Q. This means that the decomposition group of 2 in T_p/Q is $Gal(T_p/Q)$, and is of order 4.

(4) If $p \in \Pi_7$, the 2-contribution in $p-1$ is exactly 2, hence $[T_p : Q] = 2$. Since C_p contains $Q(\sqrt{-p})$ (see [2, p. 529]), we have $T_p = Q(\sqrt{-p})$. Because $(-p/2) = 1$ (see [2, pp. 78, 90]), 2 is decomposed in T_p/Q. This means that the decomposition group of 2 in T_p/Q is trivial.

From these facts we have the following:

Proposition 1. *The condition* (★★) *is satisfied for an odd integer* $N > 1$ *iff either* (I) N *is a product of powers of primes* $p_i \in \Pi_1$ *with* $i = 1, \ldots, r$ *such that, for each* p_i, *the order of the decomposition group of* 2 *in* T_{p_i}/Q *is of order* 2^t *with an integer* $t \geq 1$ *independent of* i, *or* (II) N *is a product of powers of primes in* Π_3, *or* (III) N *is a product of powers of primes in* Π_5, *or* (IV) N *is a product of powers of primes in* Π_3 *together with powers of primes* $p_1, \ldots, p_r \in \Pi_1$ *such that, for each* p_i, *the decomposition group of* 2 *in* T_{p_i}/Q *is of order* 2, *or* (V) N *is a product of powers of primes in* Π_5 *together with powers of primes* $p_1, \ldots, p_r \in \Pi_1$ *such that the decomposition group of* 2 *in* T_{p_i}/Q *is of order* 4 *for each* $i = 1, \ldots, r$.

Thus the condition (★★) is not satisfied, for example, for any integer N which is the product of a non-trivial power of a prime in Π_3 and a non-trivial power of a prime in Π_5, e.g. $N = 15$, or for any non-trivial power of a prime in Π_7. By the way, the cases (II) and (III) cover the Theorem 1 in [4].

4. The equation $\alpha\bar{\alpha} = 2$

In this section we examine the existence of generalized bent functions on Z_{2p^r} for $p \in \Pi_7$ and $r \geq 1$.

Let f be a generalized bent function $Z_{2p^r} \to Z_{2p^r}$ for $p \in \Pi_7$ and $r \geq 1$. Then the algebraic integer $\alpha(y) = \sum_{x \in Z_{2p^r}} \zeta_{2p^r}^{f(x)-xy}$ in the cyclotomic field $C_{p^r} = Q(\zeta_{2p^r}) = Q(\zeta_{p^r})$ satisfies $\alpha(y)\overline{\alpha(y)} = 2p^r$ for every $y \in Z_{2p^r}$. Hence the non-existence of generalized bent function follows if there is no integral solution of the equation $\alpha\bar{\alpha} = 2p^r$ in C_{p^r}. Now by Pei's argument in [4, p. 168], this is further reduced to the question whether or not the equation $\alpha\bar{\alpha} = 2$ is integrally solvable in C_{p^r}. So we are going to examine the solvability of the latter equation.

Before starting the discussion it will be in place to make some auxiliary remarks. Note that we always work with $p \equiv 7 \bmod 8$.

(1) $Gal(C_{p^r}/Q)$ is a cyclic group of order $(p-1)p^{r-1}$. Let σ be a generator of $Gal(C_{p^r}/Q)$. $Gal(C_{p^r}/Q)$ is the direct product of the unique subgroup of order $p-1$ ($\cong Gal(C_p/Q)$) and the p-Sylow subgroup. Further $Gal(C_p/Q)$ in turn is the direct product of the unique subgroup of order 2 and the unique subgroup of order $n = (p-1)/2$ where n is odd. Hence $Gal(C_{p^r}/Q)$ has a unique subgroup of order 2 which corresponds to the maximal real subfield R of C_{p^r}. $Gal(C_{p^r}/R)$ then is generated by $\sigma^\star = \sigma^{np^{r-1}}$ which fixes R elementwise. Hence $\sigma^\star$ induces the complex-conjugation on C_{p^r}: $\omega^{\sigma^\star} = \bar{\omega}$ for all $\omega \in C_{p^r}$. Note that $\bar{\omega}^{\sigma'} = (\omega^{\sigma^\star})^{\sigma'} = (\omega^{\sigma'})^{\sigma^\star} = \overline{(\omega^{\sigma'})}$ for every $\sigma' \in Gal(C_{p^r}/Q)$ and every $\omega \in C_{p^r}$ because $Gal(C_{p^r}/Q)$ is abelian.

(2) C_p, hence C_{p^r} with $r \geq 1$, contains the imaginary quadratic field $Q(\sqrt{-p}) = E$ (see Section 3, remark (4)). $Gal(C_{p^r}/E) = \langle \sigma^2 \rangle$ is of order np^{r-1}. Now 2 is unramified in C_{p^r}/Q, and it is decomposed in E/Q as was mentioned in Section 3, remark (4). Hence the decomposition group of 2 in $Gal(C_{p^r}/Q)$ is contained in $Gal(C_{p^r}/E)$. Setting

$f = |G_2|$, we then have $np^{r-1} = fg$ with f and g both being odd, and $G_2 = \langle \sigma^{2g} \rangle$. For the factor group $Gal(C_{p^r}/Q)/G_2$ we have the natural isomorphism $Gal(C_{p^r}/Q)/G_2 \cong Gal(D/Q)$ where D is the decomposition field of 2 in C_{p^r}/Q, i.e. the subfield of C_{p^r} elementwise fixed by the action of G_2. The factor group $Gal(C_{p^r}/Q)/G_2$ is generated by the coset (or the element in $Gal(D/Q)$) $\tau = \sigma \bmod G_2$. In particular, $\tau^\star = \tau^g = \sigma^g \bmod G_2$. On the other hand, $\sigma^\star = \sigma^{np^{r-1}} = \sigma^{fg} = \sigma^g \bmod G_2$, because f is odd, and $G_2 = \langle \sigma^{2g} \rangle$. Combining these we have $\tau^\star = \tau^g = \sigma^\star \bmod G_2$ which means that $\tau^\star$ induces the complex-conjugation on D: $\omega^{\tau^\star} = \bar{\omega}$ for all $\omega \in D$.

(3) The principal ideal $\langle 2 \rangle$ in D generated by 2 is factorized into prime ideals of D mutually conjugate with respect to $Gal(D/Q)$: $\langle 2 \rangle = \prod_{v=0}^{2g-1} \wp^{\tau^v} = \prod_{r=0}^{g-1} \wp^{\tau^r} \prod_{r=0}^{g-1} \bar{\wp}^{\tau^r}$ where $\wp$ is a prime ideal of D lying over 2, and $\bar{\wp} = \wp^{\tau^\star} = \wp^{\tau^u}$. Note that all prime factors appearing in the factorization above are different from each other, i.e. 2 splits completely in D. For each prime factor of 2 above there is a unique prime ideal of C_{p^r}, hence for the principal ideal 2 in C_{p^r} generated by 2 we have $\langle 2 \rangle = \prod_{r=0}^{2g-1} \mathscr{P}^{\tau^r} = \prod_{r=0}^{g-1} \mathscr{P}^{\tau^r} \prod_{r=0}^{g-1} \bar{\mathscr{P}}^{\tau^r}$, where $\mathscr{P}$ is the (unique) prime ideal lying over $\wp$. Further note that $\mathscr{P}^{\tau^r}$ in the factorization denotes the image of $\mathscr{P}$ by any element in the coset τ^r of $Gal(C_{p^r}/Q)/G_2$ for each r ($= 0, 1, \ldots, g-1$). The well-definedness of this notation is based on the fact that $\mathscr{P}$ remains invariant under the action of elements in G_2. The restriction of the factorization of $\langle 2 \rangle$ in C_{p^r} (or in D) down to E gives the factorization of $\langle 2 \rangle$ ($=$ the principal ideal in E generated by 2) in E: $\langle 2 \rangle = P\bar{P}$ where $P = E \cap \mathscr{P} = E \cap \wp$.

(4) Note that $C_p \not\subseteq D$ where D stands for the decomposition field of 2 in C_{p^r}/Q. In fact, $C_p \cap D$ is the decomposition field of 2 in C_p/Q so that $f_0 = [C_p : C_p \cap D]$ is the order of $2 \bmod p$ which cannot be 1.

(5) The following simple fact will be used in the proof of Lemma 2 several times: Let p be any prime, F a field of characteristic $\neq p$, and K a subfield of F. Further assume that, for a non-zero element $\omega \in F$, $\omega^p \in K$, but $\omega^p \notin K^p = \{\alpha^p \mid \alpha \in K\}$. Then $[K(\omega) : K] = p$. Under the same assumption as above, if furthermore a primitive pth root of unity is in K, then $[K(\omega) : K]$ is either 1 or p according as $\omega^p \in K^p$ or not. In particular, this is the case for $p = 2$.

We now prove the following:

Lemma 2. *If $\alpha\bar{\alpha} = 2$ for an algebraic integer $\alpha \in C_{p^r}$, then there is an algebraic integer $\beta \in D$, the decomposition field of 2 in C_{p^r}/Q, such that $\beta\bar{\beta} = 2$, and $\alpha = \beta\xi$ with a root of unit ξ in C_{p^r}.*

Proof. $\alpha\bar{\alpha} = 2$ implies $\langle \alpha \rangle \langle \bar{\alpha} \rangle = \langle 2 \rangle$ as ideals in C_{p^r}. Hence $\langle \alpha \rangle$ is the product of some prime factors of $\langle 2 \rangle$. Let $\sigma_1 = \sigma^{2g}$ be the generator of G_2. Since each prime factor of $\langle 2 \rangle$ remains invariant under the action of σ_1, we obtain $\langle \alpha^{\sigma_1} \rangle = \langle \alpha \rangle$, hence $\alpha^{\sigma_1} = \alpha\varepsilon$ with a unit ε in C_{p^r}. Next apply any $\sigma' \in Gal(C_{p^r}/Q)$ to $\alpha\bar{\alpha} = 2$ to obtain $\alpha^{\sigma'}\bar{\alpha}^{\sigma'} = 2$ which further implies $|\alpha^{\sigma'}| = \sqrt{2}$, in particular $|\alpha^{\sigma'}| = |\alpha|$ for every $\sigma' \in Gal(C_{p^r}/Q)$. Now, first applying σ' to $\alpha^{\sigma_1} = \alpha\varepsilon$, then taking the absolute value of each term, we have $|\alpha| = |\alpha^{\sigma_1\sigma}| = |\alpha^{\sigma}||\varepsilon^{\sigma'}| = |\alpha||\varepsilon^{\sigma'}|$ hence $|\varepsilon^{\sigma'}| = 1$ for every

$\sigma' \in Gal(C_{p^r}/Q)$. This means that ε is a root of unity. Since every root of unity in C_{p^r} is of order dividing $2p^r$, the order of ε is either $2p^t$ or p^t with $0 \le t \le r$. Note further that the order of ε is equal to the smallest positive integer n such that $\alpha^n \in D$. In fact, $\alpha^n \in D$ implies that $\alpha^n = (\alpha^n)^{\sigma_1} = (\alpha^{\sigma_1})^n = (\alpha\varepsilon)^n = \alpha^n\varepsilon^n$, hence $\varepsilon^n = 1$. This shows that n is not smaller than the order of ε. Conversely, if $o(\varepsilon)$ is the order of ε, $\alpha^{\sigma_1} = \alpha\varepsilon$ implies $(\alpha^{o(\varepsilon)})^{\sigma_1} = \alpha^{o(\varepsilon)}$ so that $\alpha^{o(\varepsilon)}$ is in D. Hence n is not greater than $o(\varepsilon)$. Thus we have shown $n = o(\varepsilon)$. Now let Γ be the set of all integral solutions of the equation $x\bar{x} = 2$ in C_{p^r}. Clearly Γ is not empty, because our α is in it. As was shown above, with each $\gamma \in \Gamma$, there is associated a root of unity ζ_γ satisfying $\gamma^{\sigma_1} = \gamma\zeta_\gamma$. We are going to prove the assertion in the lemma by induction on the order $o(\zeta_\gamma)$. Before doing this we better insert a remark on $o(\zeta_\gamma)$; $o(\zeta_\gamma)$ is not of the form $2p^t$ $(0 \le t \le r)$. In fact, if $\sigma(\zeta_\gamma) = 2p^t$, then $(\gamma^{p^t})^2 \in D$, hence $[D(\gamma^{p^t}):D]$ is either 1 or 2 according as $(\gamma^{p^t})^2 \in D^2$ or not. On the other hand, $D(\gamma^{p^t})/D$ is a sub-extension of C_{p^r}/D, hence $[D(\gamma^{p^t}):D]$ divides $f = [C_{p^r}:D]$ where f is an odd integer. Hence $[D(\gamma^{p^t}):D]$ must be 1, and $(\gamma^{p^t})^2 \in D^2$. There is then an element $\delta \in D$ such that $\gamma^{p^t} = \pm\delta$, i.e. $\gamma^{p^t} \in D$ contradicting the fact that $o(\zeta_\gamma) = 2p^t$ is the smallest positive integer making $\gamma^{o(\zeta_\gamma)} \in D$. Now we apply induction on $o(\zeta_\gamma)$ to prove our assertion in the lemma. If $o(\zeta_\gamma) = 1$, then $\gamma \in D$, so our assertion is trivially true. Next assume that $o(\zeta_\gamma) = N > 1$, and that our assertion has already been proved for all $\gamma' \in \Gamma$ with $o(\zeta_{\gamma'}) < N$. By the remark above, N is of the form p^t with $0 < t \le r$ which means that ζ_γ is a primitive p^t-th root of unity. Now if $(\gamma^{p^{t-1}})^p \notin D^p$, then by the remark (5) above, $[D(\gamma^{p^{t-1}}):D] = p$. On the other hand, $(\gamma^{p^{t-1}})^{\sigma_1} = \gamma^{p^{t-1}}\zeta_\gamma^{p^{t-1}}$. Note that $\zeta_\gamma^{p^{t-1}}$ is a primitive pth root of unity, because ζ_γ is a primitive p^t-th root of unity. Since $D(\gamma^{p^{t-1}})$ is a Galois extension of Q, it contains $(\gamma^{p^{t-1}})^{\sigma_1}$, hence also $\zeta_\gamma^{p^{t-1}}$, a primitive pth root of unity. Hence $D(\gamma^{p^{t-1}})$ contains C_p. Thus if $(\gamma^{p^{t-1}}) \notin D^p$, then $[D(\gamma^{p^{t-1}}):D] = p$ must be divisible by $[C_pD:D]$ where $[C_pD:D] = [C_p:C_p \cap D]$ is a divisor of $p-1$ $(= [C_p:Q])$, and greater than 1 by remark (4) above. This contradiction shows that $(\gamma^{p^{t-1}})^p \in D^p$. Therefore there is an element $\delta \in D$ such that $\gamma^{p^{t-1}} = \delta^p$, i.e. $\gamma^{p^{t-1}} = \delta\zeta_p$ with a pth root of unity ζ_p. Now find a p^t-th root of unity, say η, satisfying $\eta^{p^{t-1}} = \zeta_p$. This is possible, because $t \le r$. Then $\gamma' = \gamma\eta^{-1}$ satisfies $\gamma'\bar{\gamma}' = 2$ as γ does, furthermore $(\gamma')^{p^{t-1}} = \gamma^{p^{t-1}} \cdot \eta^{-p^{t-1}} = \delta\zeta_p \cdot \zeta_p^{-1} = \delta \in D$. Hence by induction assumption, there is an algebraic integer $\beta \in D$ satisfying $\beta\bar{\beta} = 2$ such that $\gamma' = \beta\xi'$ with a root of unity $\xi' \in C_{p^r}$. Then $\gamma = \beta\xi'\eta$ where $\xi = \xi'\eta$ is a root of unity in C_{p^r}. This completes the proof of the lemma. □

Lemma 3. *If there is an integral solution of $x\bar{x} = 2$ in the decomposition field D of 2 in C_{p^r}, then the equation $x\bar{x} = 2$ has an integral solution in $E = Q(\sqrt{-p})$.*

Proof. The principal ideal $\langle 2\rangle$ in D generated by 2 splits completely in D: $\langle 2\rangle = \prod_{v=0}^{2g-1} \wp^{\tau^v} = (\prod_{v=0}^{g-1} \wp^{\tau^v})(\prod_{v=0}^{g-1} \bar{\wp}^{\tau^v})$. Hence $\alpha\bar{\alpha} = 2$ with an algebraic integer $\alpha \in D$ implies that

$$\langle\alpha\rangle = \wp^{\tau^{i_1}} \cdots \wp^{\tau^{i_h}} \bar{\wp}^{\tau^{j_1}} \cdots \bar{\wp}^{\tau^{j_k}},$$

$$\langle\bar{\alpha}\rangle = \wp^{\tau^{j_1}} \cdots \wp^{\tau^{j_k}} \bar{\wp}^{\tau^{i_1}} \cdots \bar{\wp}^{\tau^{i_h}}, \tag{1}$$

where $h + k = g$, $I_\alpha = \{i_1 < i_2 < \cdots < i_h\}$ and $J_\alpha = \{j_1 < j_2 < \cdots < j_k\}$ are subsets of $\{0, 1, \ldots, g-1\}$ mutually disjoint, and $I_\alpha \cup J_\alpha = \{0, 1, \ldots, g-1\}$. Note that one of I_α and J_α may be empty in which case the non-empty one coincides with the whole set $\{0, 1, \ldots, g-1\}$. We call h and k the number of $\wp$'s and the number of $\bar{\wp}$'s in the factorization Eq. (1) of α, respectively. Note that, since $h + k = g$ is odd, the difference $\delta(\alpha) = h - k$ is also odd. Hence, in particular, $\delta(\alpha) \neq 0$ for every integral solution α of $x\bar{x} = 2$ in D. Now we claim that there is an integral solution α_0 of the equation satisfying $\delta(\alpha_0) = 1$. For this purpose we first choose any integral solution β of the equation, and examine the change of $\delta(\beta)$ under the action of τ on β. Let $\delta(\beta) = h_1 - k_1$, i.e. $\langle\beta\rangle = \wp^{\tau^{i_1}} \cdots \wp^{\tau^{i_{h_1}}} \bar{\wp}^{\tau^{j_1}} \cdots \bar{\wp}^{\tau^{j_{k_1}}}$. If $g - 1 \in I_\beta = \{i_1 < \cdots < i_{h_1}\}$ then $i_{h_1} = g - 1$, hence $(\wp^{\tau^{i_{h_1}}})^\tau = \wp^{\tau^g} = \bar{\wp}$. On the other hand, J_β is either empty, or for every $j \in J, j + 1 < g$. Hence the number of $\bar{\wp}$ in the decomposition for β^τ increases by 1, while the number of $\wp$'s decreases by 1. Hence $\delta(\beta^\tau) = \delta(\beta) - 2$. If $g - 1 \notin I_\beta$, then $g - 1 \in J_\beta$, and a similar observation as above shows that $\delta(\beta^\tau) = \delta(\beta) + 2$. In this way we see that at each step of application of τ, $\delta(\beta)$ increases or decreases by 2. Now returning to our purpose, take any integral solution α of $x\bar{x} = 2$. Without loss of generality we may assume $\delta(\alpha) > 0$, because otherwise we may use $\bar{\alpha}$ in place of α. If $\delta(\alpha) = 1$, we are done. If $\delta(\alpha) \geq 3$, look at the sequences of integral solutions α, α^τ, α^{τ^2}, ... Note that $\alpha\bar{\alpha} = 2$ implies $\alpha^\tau \overline{\alpha^\tau} = 2$. Since, for $\alpha^{\tau^g} = \bar{\alpha}$, $\delta(\alpha^{\tau^g}) = -\delta(\alpha)$, there is a power τ^{v_0} such that $\delta(\alpha^{\tau^{v_0}}) > 0$, but $\delta(\alpha^{\tau^{v_0+1}}) < 0$. Then, from the observation above, we see that $\delta(\alpha^{\tau^{v_0}}) = 1$. Thus we have seen the existence of an integral solution α_0 satisfying $\delta(\alpha_0) = 1$. Now take the norm $N_{D/E}$ of $\langle\alpha_0\rangle$ to obtain $N_{D/E}\langle\alpha_0\rangle = (\prod_{v=1}^{h_0} N_{D/E}\,\wp^{\tau^{i_v}})(\prod_{\mu=1}^{k_0} N_{D/E}\,\bar{\wp}^{\tau^{j_\mu}})$. Since the relative degree of $\wp$ (and of $\bar{\wp}$) in D/E is 1 (because P and $\bar{P}$ split completely in D/E), we have $N_{D/E}\,\wp^{\tau^{i_v}} = P$ and $N_{D/E}\,\bar{\wp}^{\tau^{i_v}} = \bar{P}$ for every v and μ. Hence $N_{D/E}\langle\alpha_0\rangle = P^{h_0}\bar{P}^{k_0}$ where $\delta(\alpha_0) = h_0 - k_0$ with the number h_0 of $\wp$'s and the number k_0 of $\bar{\wp}$'s. Because $h_0 - k_0 = 1$ from the choice of α_0, we have further $N_{D/E}\langle\alpha_0\rangle = (P\bar{P})^{k_0}P = \langle 2\rangle^{k_0}P$. Let $\gamma = N_{D/E}\alpha_0 (\in E)$, then $\langle\gamma\rangle = N_{D/E}\langle\alpha_0\rangle = 2^{k_0}P$, which implies $\langle\gamma/2^{k_0}\rangle = P$ is integral, hence $\gamma = 2^{k_0}\beta$ with an algebraic integer $\beta \in E$, and $\bar{\gamma} = 2^{k_0}\bar{\beta}$. Now $\langle 2^{2k_0}\beta\bar{\beta}\rangle = \langle 2^{k_0}\rangle P\langle 2^{k_0}\rangle \bar{P} = \langle 2^{2k_0+1}\rangle$ yields that $\langle\beta\bar{\beta}\rangle = \langle 2\rangle$, or $\beta\bar{\beta} = 2\varepsilon$ with a unit ε in E. Because $p \geq 7$, the only units in the imaginary quadratic field $E = Q(\sqrt{-p})$ are ± 1. Hence $\beta\bar{\beta} = \pm 2$. Since $\beta\bar{\beta} = -2$ is impossible, we arrive at $\beta\bar{\beta} = 2$ which proves the lemma. □

Using the lemmas above we obtain the following.

Proposition 2. *The equation $x\bar{x} = 2$ is solvable with algebraic integer in C_{p^r} $(r \geq 1)$ for a prime $p \equiv 7 \bmod 8$ if and only if $p = 7$.*

Proof. By Lemmas 2 and 3, if there is an integral solution of $x\bar{x} = 2$ in C_{p^r} for $p \in \Pi_7$, it must have an integral solution in $E = Q(\sqrt{-p})$. Since $p \equiv 7 \bmod 8$, every algebraic integer in E is of the form $a + b(1 + \sqrt{-p})/2$ with $a, b \in Z$. Assume now that

$\beta = a + b(1 + \sqrt{-p})/2$ satisfy $\beta\bar{\beta} = 2$. This then yields $4a^2 + 4ab + b^2(1 + p) = (2a + b)^2 + b^2p = 8$. The only solutions of the last equation are: $2a + b = \pm 1$, $b = \pm 1$, and $p = 7$. This proves the "only if" part of the proposition. Conversely if $p = 7$, $\beta = (1 + \sqrt{-7})/2$ satisfies $\beta\bar{\beta} = 2$ showing that there actuall exist integral solutions of $x\bar{x} = 2$ in C_7 $(r \geq 1)$. This completes the proof. □

Corollary 1. *There is no generalized bent function on* Z_{2p^r} $(r \geq 1)$ *for any prime* $p \equiv 7 \bmod 8$ *different from* 7.

Corollary 2. *There is no generalized bent function* Z_{2p} *for any prime* $p \equiv 7 \bmod 8$.

Proof. For $p \neq 7$, this is a special case of Corollary 1, as for $p = 7$, our assertion has already been proved in [4]. □

The last corollary covers the cases observed in [1].

References

[1] K. Bi, A note on non-existence of generalized bent functions, Thesis at Institute of Mathematics, Academia Sinica, 1991.
[2] H. Hasse, Number Theory (Springer, Berlin, 1980).
[3] P.V. Kumar, R.A. Scholtz and L.R. Welch; Generalized bent functions and their properties, J. Combin. Theory Ser. A 40 (1985) 90–107.
[4] D. Pei, On non-existence of generalized bent functions, Lecture Notes in Pure and Applied Mathematics, Vol. 141 (1993) 165–172.