Nonexistence Results on Generalized Bent Functions $\mathbb{Z}_q^m \to \mathbb{Z}_q$ with Odd m and $q \equiv 2 \pmod 4$

Ka Hin Leung [*]
Department of Mathematics
National University of Singapore
Kent Ridge, Singapore 119260
Republic of Singapore

Bernhard Schmidt
Division of Mathematical Sciences
School of Physical & Mathematical Sciences
Nanyang Technological University
Singapore 637371
Republic of Singapore

Abstract

Let p be an odd prime, let a be a positive integer, let m be an odd positive integer, and suppose that a generalized bent function from $\mathbb{Z}_{2p^a}^m$ to $\mathbb{Z}_{2p^a}$ exists. We show that this implies $m \neq 1$, $p \leq 2^{2m} + 2^m + 1$, and $\mathrm{ord}_p(2) \leq 2^{m-1}$. We obtain further necessary conditions and prove that $p = 7$ if $m = 3$ and $p \in \{7, 23, 31, 73, 89\}$

[*] Research is supported by grant R-146-000-158-112, Ministry of Education, Singapore

if $m = 5$. Our results are based on new tools for the investigation of cyclotomic integers of prescribed complex modulus, including "minimal aliases" invariant under automorphisms, and bounds on the ℓ_2-norms of their coefficient vectors. These methods have further applications, for instance, to relative difference sets, circulant Butson matrices, and other kinds of bent functions.

1 Introduction

The term "bent function" has been used with various different meanings in the literature (an account of which can be found in [25]). So we first need to clarify in what setting we are exactly interested in.

Let q and m be positive integers and let ζ_q be a primitive complex qth root of unity. A function $f : \mathbb{Z}_q^m \to \mathbb{Z}_q$ is called a **generalized bent function (GBF)** if

$$\left|\sum_{x\in\mathbb{Z}_q^m} \zeta_q^{f(x)-v\cdot x}\right|^2 = q^m \text{ for all } v \in \mathbb{Z}_q^m. \tag{1}$$

Here $x \cdot v$ denotes the usual dot product.

Research on GBFs started with the work of Rothaus [19, 20] and Dillon [6], initially focussing on the case $q = 2$. Significant further results on GBFs can be found in [7, 9, 11, 18], for instance. A survey of GBFs and related objects is given in [25].

Bent functions are a highly active research field due to their numerous applications in information theory, cryptography and coding theory. In fact, the defining condition (1) ensures that bent functions are "maximally nonlinear", which is desirable property for cryptographic purposes. The importance of nonlinear functions in cryptography is emphasized in the recent survey [3]. The relevance of bent functions in coding theoretic applications is apparent from work such as [23, 24].

The main existence result for GBFs was obtained by Kumar, Scholtz, and Welch [11]. They proved that GBFs from $\mathbb{Z}_q^m$ to $\mathbb{Z}_q$ exist whenever m is even or $q \not\equiv 2 \pmod 4$. On the other hand, not a single GBF from $\mathbb{Z}_q^m$ to $\mathbb{Z}_q$ with m odd and $q \equiv 2 \pmod 4$ is known. In fact, several nonexistence results for GBFs from $\mathbb{Z}_q^m$ to $\mathbb{Z}_q$ with m odd and $q \equiv 2 \pmod 4$ have been obtained in the literature, cf. [7, 9, 11, 18]. The aim of this paper is to strengthen these nonexistence results. More precisely, we study the case where m is odd and $q = 2p^a$ for an odd prime p and positive integer a.

Since the structure of this paper is quite complicated, we give an overview of our strategy here. Let p^a be an odd prime power, let m be an odd positive integer, and suppose that a GBF from $\mathbb{Z}_{2p^a}^m$ to $\mathbb{Z}_{2p^a}$ exists. This implies (see Corollary 37) that there is a cyclotomic integer $X \in \mathbb{Z}[\zeta_{p^a}]$ with

$$|X|^2 = 2^m. \tag{2}$$

Now there are two important observations concerning equation (2):

(a) 2^m is relatively small compared to p in most cases we are interested in.

(b) 2^m is a nonsquare.

A highly useful consequence of (a) is that the *length* of X (the smallest positive integer $\ell(X)$ such that X is an integer linear combination of $\ell(X)$ roots of unity) also is relatively small (Theorem 22). We quantify this correspondence between the modulus of X and its length in Section 4. These results heavily make use of ideas we describe in Section 3: On the one hand, Cassels' $\mathcal{M}$-function [5] gives us a basic connection between the modulus and length of X. On the other hand, we introduce the new notion of *minimal aliases*, that enables us to use Galois automorphisms to significantly improve the results based on the $\mathcal{M}$-function. In fact, the crucial Proposition 19 shows that there are minimal aliases that are invariant under maps induced by suitable Galois automorphisms.

Curiously, (b) (2^m is a nonsquare) allows us to considerably strengthen the necessary conditions for the existence of solutions of (2). This is the subject of Section 5. The main idea of this work is to switch from $|X|^2 = n$ (n nonsquare) to a group ring equation $YY^{(-1)} = n + K$, where K is a "kernel contribution" that arises from this switching. If n is small compared to p, we can show that K vanishes and thus get a contradiction by applying the trivial character $YY^{(-1)} = n$. At the end of Section 5, we will indicate how this idea can be used to study other structures such as relative difference sets, circulant Butson matrices, and other kinds of bent functions.

In Section 6, we strengthen the results of Section 5 in the case $n = 2^m$. The strategy is to use the Galois automorphisms that leave the prime ideals containing 2 invariant to obtain lower and upper bounds on the ℓ_2 norm of coefficient vector of X. This, in turn, provides additional information on what happens when we switch from (2) to a group ring equation (see Lemma 30). This group ring equation is the basis for the results in Section 6 following Lemma 30.

Finally, in Section 7, we apply our results on equation (2) to GBFs. Of course, if (2) has no solution, then there does not exist any GBF from $\mathbb{Z}_{2p^a}^m$ to $\mathbb{Z}_{2p^a}$. This is the straightforward consequence of the results of the previous sections. In turns out, however, that there is a more powerful way to make use of our results on equation (2): Even if there are solutions, we can prove nonexistence of corresponding GBFs as long as these solutions satisfy a certain intriguing parity condition (see (35)). This enables us to further improve our nonexistence results by providing sufficient conditions for (35) to be satisfied.

2 Group Rings and Characters

It turns out that group rings and characters of abelian groups provide a convenient setting for the study of GBFs. Let G be a finite (multiplicatively written) group of order v, let R be a ring, and let $R[G]$ denote group ring of G over R. Every $X \in R[G]$ can be written as $X = \sum_{g\in G} a_g g$ with $a_g \in R$. The a_g's are called the **coefficients** of X. We identify a subset S of G with the group ring element $\sum_{g\in S} g$. Let 1_G denote the identity element of G and let r be an integer. To simplify notation, we write r for the group ring element $r1_G$. The **support** of $X = \sum_{g\in G} a_g g$ is defined as

$$\mathrm{supp}(X) = \{g \in G : a_g \neq 0\}.$$

Some additional notation for the case $R = \mathbb{Z}[\zeta_q]$ is needed. Let t be an integer coprime to q. For $X = \sum_{g\in G} a_g g \in \mathbb{Z}[\zeta_q][G]$, we write $X^{(t)} = \sum a_g^\sigma g^t$ where σ is the automorphism of $\mathbb{Q}(\zeta_q)$ determined by $\zeta_q^\sigma = \zeta_q^t$.

The group of complex characters of G is denoted by $\hat{G}$. The **trivial character** of G is the character χ_0 with $\chi_0(g) = 1$ for all $g \in G$. It is well known that $\hat{G}$ is a group isomorphic to G, with multiplication in $\hat{G}$ defined by $\chi\tau(g) = \chi(g)\tau(g)$ for $\chi\tau \in \hat{G}$, $g \in G$. For $X = \sum_{g\in G} a_g g \in \mathbb{C}[G]$ and $\chi \in \hat{G}$, we write $\chi(X) = \sum_{g\in G} a_g \chi(g)$. For a subgroup U of G, we write $U^\perp = \{\chi \in \hat{G} : \chi(g) = 1 \text{ for all } g \in U\}$. If $\chi \in U^\perp$, we say that χ is **trivial on $\boldsymbol{U}$**. We have $|U^\perp| = |G|/|U|$. The following is a standard result, see [2, Chapter VI, Lemma 3.5], for instance.

Result 1 (Fourier inversion formula)**.** *Let G be a finite abelian group and $X = \sum_{g\in G} a_g g \in \mathbb{C}[G]$. Then*

$$a_g = \frac{1}{|G|} \sum_{\chi\in\hat{G}} \chi(Xg^{-1}) \textit{ for all } g \in G.$$

We now describe how bent functions can be characterized in terms of group ring equations. Let $G = \mathbb{Z}_q^m$ and let $f : G \to \mathbb{Z}_q$ be any function. Then f corresponds to an element D_f of the group ring $\mathbb{Z}[\zeta_q][G]$ via

$$D_f = \sum_{x\in G} \zeta_q^{f(x)} x.$$

Moreover, every $v \in G$ determines a character χ_v of G by

$$\chi_v(x) = \zeta_q^{-v\cdot x} \text{ for all } x \in G.$$

It well known and straightforward to verify that every complex character of G is equal to some χ_v, $v \in G$. Note that

$$\chi_v(D_f) = \sum_{x\in G} \zeta_q^{f(x)} \chi_v(x) = \sum_{x\in G} \zeta_q^{f(x)-v\cdot x} = F(v) \text{ for all } v \in G, \tag{3}$$

where $F(v)$ is defined as in Result 3. From (1) and (3), we see that f is a GBF if and only if

$$|\chi(D_f)|^2 = q^m \text{ for all } \chi \in \hat{G}. \tag{4}$$

Thus we get the following.

Proposition 2. *Let m and q be positive integers, let $f : \mathbb{Z}_q^m \to \mathbb{Z}_q$ be a function, and set $D_f = \sum_{x \in \mathbb{Z}_q^m} \zeta_q^{f(x)} x$. Then f is a GBF if and only if*

$$D_f D_f^{(-1)} = q^m. \tag{5}$$

Proof. We have shown that f is a GBF if and only if (4) holds. Note that $|\chi(D_f)|^2 = \chi(D_f D_f^{(-1)})$ for all characters χ of $\mathbb{Z}_q^m$. Using Result 1, we conclude that (4) holds if and only if (5) is satisfied. □

The following is well known, cf. [9, p. 376], and straightforward to verify.

Result 3. *Suppose f is a GBF from $\mathbb{Z}_q^m$ to $\mathbb{Z}_q$. Write $F(v) = \sum_{x \in \mathbb{Z}_q^m} \zeta_q^{f(x) - x \cdot v}$ for $v \in \mathbb{Z}_q^m$. We have*

$$\sum_{v \in \mathbb{Z}_q^m} F(v)\overline{F(v+w)} = 0 \textit{ for all } w \in \mathbb{Z}_q^m \setminus \{0\}.$$

In view of (3), Result 3 can be reformulated as follows.

Proposition 4. *Let m and q be positive integers, $G = \mathbb{Z}_q^m$, let $f : G \to \mathbb{Z}_q$ be a bent function, and set $D_f = \sum_{x \in G} \zeta_q^{f(x)} x$. Then*

$$\sum_{\tau \in \hat{G}} \tau(D_f)\overline{\tau\chi(D_f)} = 0 \textit{ for all } \chi \in \hat{G} \setminus \{\chi_0\}.$$

3 Number Theoretic Preliminaries

To study group ring equations, a powerful technique we often use is number theory. We first record some well known results that we will use later. As before, write $\zeta_n = \exp(2\pi i/n)$. Elements of the ring $\mathbb{Z}[\zeta_n]$ are called **cyclotomic integers**.

Notation 5. Throughout the rest of this paper, we assume that p is odd prime, that a is a positive integer, and we write $\zeta = \zeta_{p^a}$. Moreover, "$^-$" denotes complex conjugation.

See [4, Section 2.3, Thm. 2] for a proof of the following result of Kronecker.

Result 6. *Any nonzero algebraic integer all of whose conjugates have absolute value at most 1 is a root of unity.*

Part (a) of the next result is proved in [16, p. 76] and part (b) in [10, pp. 196–197].

Result 7. *Write $R = \mathbb{Z}[\zeta]$.*

(a) The ideal pR factors as $pR = ((1-\zeta)R)^{(p-1)p^{a-1}}$ and $(1-\zeta)R$ is a prime ideal of R. Moreover, $\overline{(1-\zeta)R} = (1-\zeta)R$.

(b) Let q be a prime different from p. The ideal qR factors as $qR = \mathfrak{p}_1 \cdots \mathfrak{p}_s$ where $s = (p-1)/\mathrm{ord}_p(q)$ and the $\mathfrak{p}_i$'s are distinct prime ideals. Moreover, $\overline{\mathfrak{p}_i} = \mathfrak{p}_i$ if and only if $\mathrm{ord}_p(q)$ is even.

Corollary 8. *Write $\Theta = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) \zeta_p^x$ where $\left(\frac{x}{p}\right)$ is the Legendre symbol. Suppose that $X \in \mathbb{Z}[\zeta]$ satisfies $|X|^2 = p^b m$ where b and m are positive integers. Then $X = \Theta^b A$ for some $A \in R$ with $|A|^2 = m$.*

Proof. Write $R = \mathbb{Z}[\zeta]$ and $\mathfrak{p} = (1-\zeta)R$. Then $\mathfrak{p}$ is a prime ideal of R and $pR = \mathfrak{p}^{(p-1)p^{a-1}}$ by Result 7. Moreover, $\overline{\mathfrak{p}} = \mathfrak{p}$ by Result 7 (a). As $|X|^2 = p^b m$, we have $X\overline{X}R = \mathfrak{p}^{b(p-1)p^{a-1}}(mR)$. Since $\overline{\mathfrak{p}} = \mathfrak{p}$, this implies $X \in \mathfrak{p}^{b(p-1)p^{a-1}/2}$. We have $\Theta\overline{\Theta} = p$ (see [10, Prop. 8.2.2]) and thus $\Theta R = \mathfrak{p}^{(p-1)p^{a-1}/2}$. As $X \in \mathfrak{p}^{b(p-1)p^{a-1}/2} = \Theta^b R$, we conclude that $X = \Theta^b A$ for some $A \in R$. Note that $|A|^2 = |X|^2/|\Theta|^{2b} = p^b m/p^b = m$. □

The next result is a special case of [14, Thm. 4.7].

Result 9. *Suppose that $X \in \mathbb{Z}[\zeta]$ satisfies $|X|^2 = 2^{2n}$ for some positive integer n. If $\mathrm{ord}_p(2) \geq 2^{n+1}$, then X is trivial, that is, $X = 2^n \eta$ for some root of unity η.*

The following is a consequence of [21, Thm. 3.5].

Result 10. *Suppose that $X \in \mathbb{Z}[\zeta]$ satisfies $|X|^2 = q^b$, where $q \neq p$ is a prime and b is a positive integer. If $q^{\mathrm{ord}_p(q)} \not\equiv 1 \pmod{p^2}$, then $X\zeta^j \in \mathbb{Z}[\zeta_p]$ for some integer j.*

Note that Result 10 indeed follows from [21, Thm. 3.5], as $q^{\mathrm{ord}_p(q)} \not\equiv 1 \pmod{p^2}$ implies $F(p^a, q^b) = p$, where the function F is defined in [21].

Cassels [5] introduced the following useful notion.

Definition 11 ($\mathcal{M}$-function)**.** *For $X \in \mathbb{Z}[\zeta_n]$, let*

$$\mathcal{M}(X) = \frac{1}{\varphi(n)} \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})} (X\overline{X})^{\sigma},$$

where φ denotes the Euler totient function.

Note that $\mathcal{M}(X) \geq 1$ for all nonzero $X \in \mathbb{Z}[\zeta_n]$ by the inequality of geometric and arithmetic means, since $\prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})} (X\overline{X})^{\sigma} \geq 1$. The following is a consequence of [5, (3.4), (3.16)].

Result 12. *Let $X \in \mathbb{Z}[\zeta_n]$, let q be a prime divisor of n, and write $n = q^b n'$ with $(q, n') = 1$. If $b = 1$, then $X = \sum_{i=0}^{q-1} X_i \zeta_q^i$ with $X_i \in \mathbb{Z}[\zeta_{n'}]$ and*

$$\mathcal{M}(X) = \frac{1}{q-1} \sum_{1 \leq i < j \leq q}^{q-1} \mathcal{M}(X_i - X_j). \tag{6}$$

On the other hand, if $b > 1$, then $X = \sum_{i=0}^{q^{b-1}-1} X_i \zeta_n^i$ with $X_i \in \mathbb{Z}[\zeta_{qn'}]$ and

$$\mathcal{M}(X) = \sum_{i=0}^{q^{b-1}-1} \mathcal{M}(X_i). \tag{7}$$

Proposition 13. *Let $U = \{\zeta_p^j : j = 0, \ldots, p-1\}$ be the subgroup of order p of $\langle \zeta \rangle$.*

(a) Let N be a set of integers with $|N| = p^{a-1}$ such that the elements of N are pairwise incongruent modulo p^{a-1}. Then $B = \{\zeta^i : i \in N\}$ is an integral basis of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}(\zeta_p)$.

(b) A subset T of $\{1, \zeta, \ldots, \zeta^{p^a-1}\}$ is linearly independent over $\mathbb{Q}$ if and only if T does not contain a coset of U.

Proof.
(a) Note that $|B| = p^{a-1}$. As the degree of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}(\zeta_p)$, is $\varphi(p^a)/\varphi(p) = p^{a-1} = |B|$, it suffices to show $\mathrm{span}(B) = \mathbb{Z}[\zeta]$, where $\mathrm{span}(B)$ denotes the set of all linear combinations of elements of B with coefficients from $\mathbb{Z}[\zeta_p]$. Let $j \in \mathbb{Z}$ be arbitrary. By the definition of N, there is $i \in N$ with $i \equiv j \pmod{p^{a-1}}$, that is, $j = i + kp^{a-1}$ for some $k \in \mathbb{Z}$. Thus $\zeta^j = \zeta^i \zeta_p^k \in \mathrm{span}(B)$. Hence we have $\{1, \zeta, \ldots, \zeta^{p^a-1}\} \subset \mathrm{span}(B)$. This implies $\mathrm{span}(B) = \mathbb{Z}[\zeta]$.

(b) If T contains a coset of U, then T is linearly dependent, as $\sum_{j=0}^{p-1} \zeta_p^j = 0$. Write $T = \{\zeta^j : j \in A\}$ with $A \subset \{0, \ldots, p^a - 1\}$. If T is linearly dependent, then there are integers a_i, not all zero, such that $\sum_{j \in A} a_j \zeta^j = 0$. As the minimal polynomial of ζ over $\mathbb{Q}$ is $1 + x^{p^{a-1}} + \cdots + x^{(p-1)p^{a-1}}$, this implies

$$\sum_{j \in A} a_j x^j = g(x)(1 + x^{p^{a-1}} + \cdots + x^{(p-1)p^{a-1}}) \tag{8}$$

for some nonzero polynomial $g(x) \in \mathbb{Z}[x]$ of degree less than p^{a-1}. Let $k = \min\{j \in A : a_j \neq 0\}$. Then A contains $\{k, kp^{a-1}, \ldots, k(p-1)p^{a-1}\}$ by (8) and thus T contains $U\zeta^k$. □

Definition 14. Let n be a positive integer, let G be a cyclic group of order n, and let g be a fixed generator of G. For $Z = \sum_{i=0}^{n-1} a_i g^i \in \mathbb{Z}[G]$, write $Z(\zeta_n) = \sum_{i=0}^{n-1} a_i \zeta_n^i$. We say that Z is **minimal** if

$$|\mathrm{supp}(Z)| = \min\{|\operatorname{supp}(Y)| : Y \in \mathbb{Z}[G],\ Y(\zeta_n) = Z(\zeta_n)\}.$$

If $X \in \mathbb{Z}[\zeta_n]$ and $Z(\zeta_n) = X$, then Z is called an **alias** of X. The **length** of X is $|\mathrm{supp}(Z)|$, where Z is a minimal alias of X. We denote the length of X by $\ell(X)$.

Remark 15. If H is a subgroup of $G = \langle g \rangle$ of order m, we consider the group ring $\mathbb{Z}[H]$ as imbedded in $\mathbb{Z}[G]$. In particular, every $A \in \mathbb{Z}[H]$ can be written in the form $A = \sum_{i=0}^{m-1} a_i g^{in/m}$ with $a_i \in \mathbb{Z}$ and we have $A(\zeta_n) = \sum_{i=0}^{m-1} a_i \zeta_n^{in/m} \in \mathbb{Z}[\zeta_m]$.

Lemma 16. *Let G be a cyclic group of order p^a and let P be its subgroup of order p.*

(a) The map $\mathbb{Z}[G] \to \mathbb{Z}[\zeta], Y \mapsto Y(\zeta)$ is a ring homomorphism with kernel $\{PY : Y \in \mathbb{Z}[G]\}$.

(b) Let S be subset of $G \setminus \{1\}$ and let c, d be integers. If $Y = c + dS \in \mathbb{Z}[G]$ is minimal, then $|S \cap Ph| \leq (p-1)/2$ for all $h \in G$.

Proof.
(a) This follows from that fact that the minimal polynomial of ζ over $\mathbb{Q}$ is $1 + x^{p^{a-1}} +$

$\cdots + x^{(p-1)p^{a-1}}$.

(b) Suppose $|S \cap Ph| \geq (p+1)/2$. Set $Z = c + d(S - Ph)$. Then $Z(\zeta) = Y(\zeta)$, as $P(\zeta) = 0$. However, $|\operatorname{supp}(Z)| < |\operatorname{supp}(Y)|$, contradicting the minimality of Y. □

Lemma 17. *Let t be a positive integer with $\gcd(t,p) = 1$ and let G be a cyclic group of order p. Let σ be the automorphism of $\mathbb{Q}(\zeta_p)$ determined by $\zeta_p^\sigma = \zeta^t$. If $X^\sigma = X$ for $X \in \mathbb{Z}[\zeta_p]$, then $Z^{(t)} = Z$ for every alias $Z \in \mathbb{Z}[G]$ of X.*

Proof. Let g be a generator of G and suppose that $Z = \sum_{i=0}^{p-1} a_i g^i$ is an alias of X. Then $Z(\zeta_p) = X$ and thus $Z^{(t)}(\zeta_p) = Z(\zeta_p)^\sigma = Z(\zeta_p)$, since $X^\sigma = X$ by assumption. Using Lemma 16, we conclude $Z^{(t)} = Z + \alpha G$ with $\alpha \in \mathbb{Z}$. As the sum of the coefficients of $Z^{(t)}$ is the same as the sum of the coefficients of Z, we have $\alpha = 0$ and thus $Z^{(t)} = Z$. □

Lemma 18. *Let $G = \langle g \rangle$ be a cyclic group of order p^a, and let $P = \langle g^{p^{a-1}} \rangle$ be the subgroup of order p of G. Let N be a set of integers with $|N| = p^{a-1}$ such that the elements of N are pairwise incongruent modulo p^{a-1}.*

(a) Every $Z \in \mathbb{Z}[G]$ can be written in the form $Z = \sum_{j \in N} Z_j g^j$ with $Z_j \in \mathbb{Z}[P]$, and Z is minimal if and only if each Z_j is minimal.

(b) Every $X \in \mathbb{Z}[\zeta]$ can be written in the form $X = \sum_{j \in N} X_j \zeta^j$ with $X_j \in \mathbb{Z}[\zeta_p]$, and we have $\ell(X) = \sum_{j \in N} \ell(X_i)$.

Proof. (a) Since the elements g^j, $j \in N$, represent every coset of P in G, we see that Z indeed can be written as $Z = \sum_{j \in N} Z_j g^j$ with $Z_j \in \mathbb{Z}[P]$. If Z is minimal, then each Z_j must be minimal by the definition of minimality. Suppose that all Z_j's are minimal and that Z is not minimal. Then there exists $Y \in \mathbb{Z}[G]$ with $Y(\zeta) = Z(\zeta)$ and $|\operatorname{supp}(Y)| < |\operatorname{supp}(Z)|$. Write $Y = \sum_{j \in N} Y_j g^j$ with $Y_j \in \mathbb{Z}[P]$. We have

$$\sum_{j \in N} Z_j(\zeta)\zeta^j = Z(\zeta) = Y(\zeta) = \sum_{j \in N} Y_j(\zeta)\zeta^j. \tag{9}$$

By Proposition 13 (a), the set $\{\zeta^j : j \in N\}$ is linearly independent over $\mathbb{Q}(\zeta_p)$. Moreover, $Z_j(\zeta), Y_j(\zeta) \in \mathbb{Z}[\zeta_p]$. Thus $Z_j(\zeta) = Y_j(\zeta)$ for all j by (9). As $|\operatorname{supp}(Y)| < |\operatorname{supp}(Z)|$, we have $|\mathrm{supp}(Y_j)| < |\mathrm{supp}(Z_j)|$ for some j, contradicting the minimality of Z_j. This completes the proof of part (a).

(b) Let $X \in \mathbb{Z}[\zeta]$. We indeed have $X = \sum_{j\in N} X_j \zeta^j$ with $X_j \in \mathbb{Z}[\zeta_p]$, as $\{\zeta^j : j \in N\}$ is an integral basis of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}(\zeta_p)$ by Proposition 13 (a). Let Z be a minimal alias of X and write $Z = \sum_{j\in N} Z_j g^j$ with $Z_j \in \mathbb{Z}[P]$. Then each Z_j is minimal by part (a) and $\sum_{j\in N} X_j\zeta^j = X = Z(\zeta) = \sum_{j\in N} Z_j(\zeta)\zeta^j$. Thus $Z_j(\zeta) = X_j$, which implies that Z_j is a minimal alias of X_j and $\ell(X_j) = |\mathrm{supp}(Z_j)|$ for all j. Hence

$$\ell(X) = |\mathrm{supp}(Z)| = \sum_{j\in N} |\mathrm{supp}(Z_j)| = \sum_{j\in N} \ell(X_j).$$

□

Proposition 19. *Let t be an integer with $\gcd(t,p) = 1$ and let G be a cyclic group of order p^a. Write $\mathrm{ord}_{p^a}(t) = f$ and suppose that f divides $p-1$. Let σ be the automorphism of $\mathbb{Q}(\zeta)$ determined by $\zeta^\sigma = \zeta^t$. If $X^\sigma = X$ for $X \in \mathbb{Z}[\zeta]$, then there is a minimal alias $Z \in \mathbb{Z}[G]$ of X with*

$$Z^{(t)} = Z.$$

Proof. For $x \in \mathbb{Z}$ let $r(x)$ be the integer such that $r(x) \equiv x \pmod{p^{a-1}}$ and $0 \le r(x) < p^{a-1}$. Note that the map $x \mapsto r(xt)$ is a permutation of $\{0,\dots,p^{a-1}-1\}$, since $\gcd(t,p) = 1$. Note that all orbits of $x \mapsto r(xt)$ on $\{1,\dots,p^{a-1}-1\}$ have length f, since $f|(p-1)$ by assumption. Let $\mathcal{O}_0,\dots,\mathcal{O}_\ell$ be the orbits of $x \mapsto r(xt)$ on $\{0,\dots,p^{a-1}-1\}$ where $\ell = (p^{a-1}-1)/f$, $\mathcal{O}_0 = \{0\}$, and $|\mathcal{O}_i| = f$ for all $i > 0$. For each i, let x_i be a fixed element of $\mathcal{O}_i$, and set

$$N = \{0\} \cup \{x_i t^s : 1 \le i \le \ell,\ 0 \le s \le f-1\}.$$

Then $|N| = 1 + \ell f = p^{a-1}$ and the elements of N are pairwise incongruent modulo p^{a-1}. Moreover, $\{\zeta^{tj} : j \in N\} = \{\zeta^j : j \in N\}$, since $t^f \equiv 1 \pmod{p^a}$. Note that $\{\zeta^j : j \in N\}$ is an integral basis of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}(\zeta_p)$ by Proposition 13 (a). Hence there are unique $X_j \in \mathbb{Z}[\zeta_p]$ with $X = \sum_{j\in N} X_j\zeta^j$. As $X^\sigma = X$ by assumption and $N^\sigma = N$, we have

$$\sum_{j\in N} X_{jt}\zeta^{jt} = \sum_{j\in N} X_j\zeta^j = X = X^\sigma = \sum_{j\in N} X_j^\sigma \zeta^{jt},$$

where the index jt in X_{jt} is taken modulo p^a. This implies $X_j^\sigma = X_{jt}$ for all j and thus $(X_{x_i})^{\sigma^s} = X_{x_i t^s}$ for all i, s. We conclude

$$X = \sum_{j \in N} X_j \zeta^j = X_0 + \sum_{i=1}^{\ell} \sum_{s=0}^{f-1} X_{x_i t^s} \zeta^{x_i t^s} = X_0 + \sum_{i=1}^{\ell} \sum_{s=0}^{f-1} \left(X_{x_i} \zeta^{x_i} \right)^{\sigma^s}. \tag{10}$$

Let g be a generator of G and let $P = \langle g^{p^{a-1}} \rangle$ be the subgroup of G of order p. Let $Z_0 \in \mathbb{Z}[P]$ be a minimal alias of X_0 and, for $i = 1, \ldots, \ell$, let $Z_i \in \mathbb{Z}[P]$ be a minimal alias of X_{x_i}. Define

$$Z = Z_0 + \sum_{i=1}^{\ell} \sum_{s=0}^{f-1} Z_i^{(t^s)} g^{x_i t^s}.$$

We claim that Z is a minimal alias of X. Note that $Z_i^{(t^s)}$ is minimal for all i and s, since Z_i is minimal. Furthermore, the elements of $\{0\} \cup \{x_i t^s : 1 \le i \le \ell,\ 0 \le s \le f-1\}$ are pairwise incongruent modulo p^{a-1}. Hence Z is minimal by Lemma 18 (a). Moreover, we have

$$Z(\zeta) = Z_0(\zeta) + \sum_{i=1}^{\ell} \sum_{s=0}^{f-1} Z_i(\zeta)^{(t^s)} \zeta^{x_i t^s} = X_0 + \sum_{i=1}^{\ell} \sum_{s=0}^{f-1} \left(X_{x_i} \zeta^{x_i} \right)^{\sigma^s} = X$$

by (10), where we have used that Z_0 is an alias of X_0 and Z_i is an alias of X_{x_i} for $i = 1, \ldots, \ell$. Hence Z is an alias of X.

It remains to show $Z^{(t)} = Z$. Note that $X_0^\sigma = X_0$, as $X_j^\sigma = X_{jt}$ for all j. As Z_0 is an alias of X_0, we have $Z_0^{(t)} = Z_0$ by Lemma 17. Hence

$$Z^{(t)} = Z_0^{(t)} + \sum_{i=1}^{\ell} \sum_{s=1}^{f} Z_i^{(t^s)} g^{x_i t^s} = Z_0 + \sum_{i=1}^{\ell} \sum_{s=0}^{f-1} Z_i^{(t^s)} g^{x_i t^s} = Z,$$

since $Z_i^{(t^f)} = Z_i^{(t^0)}$ and $g^{x_i t^f} = g^{x_i t^0}$ for all i. □

4 $\mathcal{M}$-Function and Length of Cyclotomic Integers

We now prove a basic result relating the length of cyclotomic integers to the $\mathcal{M}$-function.

Lemma 20. *Let $\langle g\rangle$ be a cyclic group of order p and suppose that $\sum_{i=0}^{p-1} a_i g^i$ is a minimal alias of $X \in \mathbb{Z}[\zeta_p]$. Then*

$$\mathcal{M}(X) \geq \frac{1}{p-1}\left((p-\ell(X))\sum_{i=0}^{p-1} a_i^2 + \ell(X)\max\{0, \ell(X)-p/2\}\right). \tag{11}$$

In particular,

$$\mathcal{M}(X) \geq \max\left\{\frac{p\ell(X)}{2(p-1)}, \frac{\ell(X)(p-\ell(X))}{p-1}\right\}. \tag{12}$$

Proof. Write $k = \ell(X)$ and $K = \{i : a_i \neq 0\}$. Since $\sum_{i=0}^{p-1} a_i g^i$ is a minimal alias of X, we have $|K| = k$. Moreover, we claim that

$$|\{i : a_i = a_j\}| \leq \min\{k, p-k\} \text{ for all } j \in K. \tag{13}$$

Note that $|\{i : a_i = a_j\}| \leq k$ for $j \in K$, as $0 = a_i \neq a_j$ for $i \notin K$. Moreover, if $|\{i : a_i = a_j\}| > p-k$, then $|\{i : a_i - a_j \neq 0\}| < k$ and X would have length less than k, as $\sum_{i=0}^{p-1}(a_i - a_j)g^i$ is an alias of X. This contradicts $k = \ell(X)$ and proves (13).

Using (6), we get

$$(p-1)\mathcal{M}(X) = \sum_{i<j}\mathcal{M}(a_i - a_j) = \frac{1}{2}\sum_{i\in K}\sum_{j\in K}\mathcal{M}(a_i - a_j) + \sum_{i\in K}\sum_{j\notin K}\mathcal{M}(a_i - a_j). \tag{14}$$

Since $a_j = 0$ for $j \notin K$ and $\mathcal{M}(a_i) = a_i^2$ for all i, we conclude

$$\sum_{i\in K}\sum_{j\notin K}\mathcal{M}(a_i - a_j) = (p-k)\sum_{i\in K} a_i^2 = (p-k)\sum_{i=0}^{p-1} a_i^2 \tag{15}$$

Note that $\mathcal{M}(a_i - a_j) \geq 1$ if $a_i \neq a_j$. Hence, in view of (13), we get

$$\sum_{i\in K}\mathcal{M}(a_i - a_j) \geq k - \min\{k, p-k\} = \max\{0, 2k-p\}.$$

and thus

$$\sum_{i,j\in K}\mathcal{M}(a_i - a_j) \geq k\max\{0, 2k-p\}. \tag{16}$$

Combining (14-16) proves (11).

It remains to prove (12). Note that $\mathcal{M}(X) \geq k(p-k)/(p-1)$ by (11), since $\sum a_i^2 \geq k$. Hence it suffices to show $\mathcal{M}(X) \geq p\,k/(2(p-1))$. Using (11) and $\sum a_i^2 \geq k$, we obtain

$$\begin{aligned}\mathcal{M}(X) &\geq \frac{1}{p-1}\left((p-k)\sum_{i=0}^{p-1} a_i^2 + k\max\{0, k-p/2\}\right)\\ &\geq \frac{2k(p-k)+k(2k-p)}{2(p-1)} = \frac{pk}{2(p-1)}.\end{aligned}$$

□

Corollary 21. *Let $\langle g\rangle$ be a cyclic group of order p^a and suppose that $Z = \sum_{i=0}^{p^a-1} a_i g^i$ is a minimal alias of $X \in \mathbb{Z}[\zeta]$. Then*

$$\mathcal{M}(X) \geq \frac{1}{p-1}\left((p-\ell(X))\sum_{i=0}^{p^a-1} a_i^2 + \ell(X)\max\{0, \ell(X) - \frac{p}{2}\}\right). \tag{17}$$

In particular,

$$\mathcal{M}(X) \geq \max\left\{\frac{p\ell(X)}{2(p-1)}, \frac{\ell(X)(p-\ell(X))}{p-1}\right\}. \tag{18}$$

Proof. Write $X = \sum_{j=0}^{p^{a-1}-1} X_j\zeta^j$ with $X_j \in \mathbb{Z}[\zeta_p]$. By Lemma 18 (b), we have $\ell(X) = \sum_{j=0}^{p^{a-1}-1} \ell(X_j)$. Furthermore, $\mathcal{M}(X) = \sum_{j=0}^{p^{a-1}-1} \mathcal{M}(X_j)$ by (7).

For $j = 0, \ldots, p^{a-1}-1$, write $Z_j = \sum_{k=0}^{p-1} a_{p^{a-1}k+j} g^{p^{a-1}k}$. Note that $Z = \sum_{j=0}^{p^{a-1}-1} Z_j g^j$. and thus Z_j is a minimal alias of X_j for all j by Lemma 18. Hence $\ell(X_j) = |\operatorname{supp}(Z_j)|$ for all j. Moreover, $|\operatorname{supp}(Z_j)| \leq \sum_{k=0}^{p-1} a_{p^{a-1}k+j}^2$ and thus we get

$$\begin{aligned}\sum_{j=0}^{p^{a-1}-1} (p-\ell(X_j))\sum_{k=0}^{p-1} a_{p^{a-1}k+j}^2 &= \sum_{j=0}^{p^{a-1}-1} [(p-\ell(X)) + (\ell(X)-\ell(X_j))]\sum_{k=0}^{p-1} a_{p^{a-1}k+j}^2\\ &= (p-\ell(X))\sum_{i=0}^{p^a-1} a_i^2 + \sum_{j=0}^{p^{a-1}-1} (\ell(X)-\ell(X_j))\sum_{k=0}^{p-1} a_{p^{a-1}k+j}^2\\ &\geq (p-\ell(X))\sum_{i=0}^{p^a-1} a_i^2 + \sum_{j=0}^{p^{a-1}-1} (\ell(X)-\ell(X_j))\ell(X_j).\end{aligned} \tag{19}$$

As $\mathcal{M}(X) = \sum_{j=0}^{p^{a-1}-1} \mathcal{M}(X_j)$, we have

$$(p-1)\mathcal{M}(X) \geq \sum_{j=0}^{p^{a-1}-1} \left((p - \ell(X_j)) \sum_{k=0}^{p-1} a_{p^{a-1}k+j}^2 + \ell(X_j) \max\{0, \ell(X_j) - \frac{p}{2}\} \right)$$

by (12). Together with (19), this implies

$$\begin{aligned}(p-1)\mathcal{M}(X) &\geq (p - \ell(X)) \sum_{i=0}^{p^a-1} a_i^2 + \sum_{j=0}^{p^{a-1}-1} (\ell(X) - \ell(X_j))\ell(X_j) \\ &\quad + \sum_{j=0}^{p^{a-1}-1} \ell(X_j) \max\{0, \ell(X_j) - \frac{p}{2}\} \\ &= (p - \ell(X)) \sum_{i=0}^{p^a-1} a_i^2 + \sum_{j=0}^{p^{a-1}-1} \ell(X_j) \left(\ell(X) - \ell(X_j) + \max\{0, \ell(X_j) - \frac{p}{2}\} \right) \\ &\geq (p - \ell(X)) \sum_{i=0}^{p^a-1} a_i^2 + \ell(X) \max\{0, \ell(X) - \frac{p}{2}\},\end{aligned}$$

where the last inequality holds due to $\sum_{j=0}^{p^{a-1}-1} \ell(X_j) = \ell(X)$ and this proves (17). Now (18) follows from (17) in the same way as (12) follows from (11). □

5 Elements of $\mathbb{Z}[\zeta]$ for which $|X|^2$ is a Nonsquare

The key to our results on GBFs from $\mathbb{Z}_{2p^a}^m$ to $\mathbb{Z}_{2p^a}$ is to study solutions of $|X|^2 = n$ where n is a nonsquare integer and $X \in \mathbb{Z}[\zeta]$.

Theorem 22. *Let $G = \langle g \rangle$ be a cyclic group of order p^a. Let n be nonsquare integer not divisible by p and let $q_1, \ldots, q_s$ be the distinct prime divisors of n. Write $f = \gcd\{\mathrm{ord}_p(q_1), \ldots, \mathrm{ord}_p(q_s)\}$ and let t be an integer with $\mathrm{ord}_{p^a}(t) = f$. Let σ be the automorphism of $\mathbb{Q}(\zeta)$ determined by $\zeta^\sigma = \zeta^t$. Suppose $X \in \mathbb{Z}[\zeta]$ satisfies $|X|^2 = n$. Then we have the following.*

(a) f is odd.

(b) We have $\ell(X) < 2n$ and there is a positive integer u such that $\ell(X) \in \{uf, uf+1\}$

(c) *$f \leq n$ or $p \leq \frac{f^2-n}{f-n}$.*

(d) *There is an integer i such that $(X\zeta^i)^\sigma = X\zeta^i$.*

(e) *There is a minimal alias Z of $X\zeta^i$ with $Z^{(t)} = Z$ and we can write $Z = c_0 + \sum_{j=1}^u c_j\Gamma_j$, where $c_0, \ldots, c_u \in \mathbb{Z}$, $c_j \neq 0$ for $j > 0$, and the Γ_j's are distinct orbits of $g \mapsto g^t$ on $G \setminus \{1\}$. Moreover, $|\Gamma_j| = f$ for all j.*

Proof. Let K be the subfield of $\mathbb{Q}(\zeta)$ fixed by σ. By [14, Lemma 4.6], we have $X\zeta^i \in K$ for some integer i (note that [13, Lemma 4.6] is stated for the case that $|X|^2$ is a square, but its proof shows that the statement is also true if $|X|^2$ is a nonsquare). Hence $(X\zeta^i)^\sigma = X\zeta^i$ and this proves part (d). Replacing X by $X\zeta^i$, if necessary, we can assume $X^\sigma = X$, that is, $X \in K$.

If f is even, then K is real and thus $X^2 = |X|^2 = n$. Since n is a nonsquare, this implies that $\mathbb{Q}(X) = \mathbb{Q}(\sqrt{n})$ is a quadratic subfield of $\mathbb{Q}(\zeta)$. But the unique quadratic subfield of $\mathbb{Q}(\zeta)$ is $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$ and it is straightforward to show $\sqrt{n} \notin \mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$, as $\gcd(p, n) = 1$ and n is a nonsquare. Hence f is odd.

By Proposition 19, there is a minimal alias $Z \in \mathbb{Z}[G]$ of X such that $Z^{(t)} = Z$. Moreover, $Z^{(t)} = Z$ implies that Z can be written in the form $c_0 + \sum_{i=1}^u c_i\Gamma_i$ for some nonnegative integer u, where $c_0, \ldots, c_u \in \mathbb{Z}$, $c_i \neq 0$ for $i > 0$, and the Γ_i's are distinct orbits of $g \mapsto g^t$ on $G \setminus \{1\}$. If $u = 0$, then $n = |X|^2 = |Z(\zeta)|^2 = c_0^2$. This is impossible, as n is a nonsquare by assumption. As $\mathrm{ord}_{p^a}(t) = f = \mathrm{ord}_p(t)$, we have $|\Gamma_i| = f$ for all i. This proves part (e).

Note that $\ell(X) = |\operatorname{supp}(Z)| \in \{uf, uf+1\}$ by part (e). If $u = 0$, then $X = c_0 \in \mathbb{Z}$ and $n = |X|^2$ is a square, contradicting our assumptions. Therefore, $u \geq 1$. By Corollary 21, we have $n = \mathcal{M}(X) > \frac{\ell(X)}{2}$ and thus $\ell(X) < 2n$. This completes the proof of part (b) of Theorem 22.

To prove part (c), suppose $f > n$. Then $u = 1$, since $uf + 1 \leq 2n$. Thus $\ell(X) \in \{f, f+1\}$. Note that $f < p/2$, as f is an odd divisor of $p-1$. As the function $x(p-x)$ is increasing for $x < p/2$ and $\ell(X) \in \{f, f+1\}$, we have $\ell(X)(p - \ell(X)) \geq f(p-f)$. Using

Corollary 21, we conclude

$$n = \mathcal{M}(X) \geq \frac{\ell(X)(p-\ell(X))}{p-1} \geq \frac{f(p-f)}{p-1}.$$

This implies $p \geq (f^2-n)/(f-n)$, which completes the proof of part (c). □

Theorem 23. *Let n be a nonsquare integer. Let $G = \langle g \rangle$ be a cyclic group of order p^a and let P be the subgroup of G of order p. Assume there is $X \in \mathbb{Z}[\zeta]$ with $|X|^2 = n$. Then, for every alias $Z \in \mathbb{Z}[G]$ of X, there is $Y \in \mathbb{Z}[G]$ such that*

$$ZZ^{(-1)} = n + PY. \tag{20}$$

Moreover, we have $\ell(X) < 2n$ and

$$p \leq n^2+n+1. \tag{21}$$

Proof. Let $Z \in \mathbb{Z}[G]$ be an alias of X. Then $Z(\zeta)\overline{Z(\zeta)} = X\overline{X} = n$. Using Lemma 16, we conclude that $ZZ^{(-1)} = n + PY$ for some $Y \in \mathbb{Z}[G]$, which proves (20).

Now suppose $p > n^2+n+1$. Note that $n \geq 2$, as n is a nonsquare. If $n = 2$, then $p > 2^2+2+1 = 7$ and hence $p \geq 11 > 4n$. If $n \geq 3$, then $p > n^2+n+1 \geq 3n+n+1 = 4n+1$. Hence we have $p > 4n$ in any case.

Recall that $X\overline{X} = |X|^2 = n$ by assumption and thus $(X\overline{X})^\sigma = n$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Since $|\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})| = \varphi(p^a)$, we conclude

$$\mathcal{M}(X) = \frac{1}{\varphi(p^a)} \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})} (X\overline{X})^\sigma = \frac{|\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})|\, n}{\varphi(p^a)} = n.$$

We have $\mathcal{M}(X) = |X|^2 = n$ by assumption and $\ell(X) < 2n$ by Theorem 22 (b). Write $s = \ell(X)$. Note that $s < 2n < p/2$, as $p > 4n$. Write $f(x) = x(p-x)$ and note that

$$f(n+1) = (n+1)(p-n-1) = n(p-1) + p - n^2 - n - 1 > n(p-1), \tag{22}$$

as we assume $p > n^2+n+1$. On the other hand, $n = \mathcal{M}(X) \geq s(p-s)/(p-1)$ by Corollary 21 and thus $f(s) = s(p-s) \leq n(p-1)$. As $f(n+1) > n(p-1)$ by (22) and f is increasing for $x < p/2$, we conclude $s \leq n$.

Finally, let Z be a minimal alias of X and let Y be the element of $\mathbb{Z}[G]$ satisfying (20). If $PY = 0$, then $ZZ^{(-1)} = n$ and thus $|Z|^2 = n$, contradicting the assumption that n is nonsquare. Hence $PY \neq 0$ and consequently $|\operatorname{supp}(n+PY)| \geq p-1$. On the other hand, we have $|\operatorname{supp}(Z)| = \ell(X) = s \leq n$, as Z is minimal. This implies $|\operatorname{supp}(ZZ^{(-1)})| \leq n^2$. Using (20), we conclude $n^2 \geq |\operatorname{supp}(ZZ^{(-1)})| = |\operatorname{supp}(n+PY)| \geq p-1$, which contradicts the assumption $p > n^2 + n + 1$. This proves (21). □

As promised in the introduction, we will now explain how our methods can be used to study other combinatorial structures. For instance, suppose p and q are distinct primes and p is odd. Assume that a relative (pq, p, pq, q) difference set exists in an abelian group (see [2] for the necessary background on relative difference sets). It can be shown that that this implies that there is $X \in \mathbb{Z}[\zeta_p]$ with $|X|^2 = q$. Hence Theorems 22 and 23 immediately provide necessary conditions for the existence of such relative difference set. In particular, we have $p \leq q^2 + q + 1$ by Theorem 23. Similarly, if a circulant Butson matrix $\mathrm{BH}(pq, p)$ exists (see [12] for information on Butson matrices), then there also is $X \in \mathbb{Z}[\zeta_p]$ with $|X|^2 = q$ and we get the same conclusions. Finally, our results can be applied to other types of bent functions and, for example, immediately give new necessary conditions for the existence of the functions studied in [15].

6 Elements of $\mathbb{Z}[\zeta]$ with $|X|^2 = 2^m$ and Odd m

In this section, we study the structure of elements $X \in \mathbb{Z}[\zeta]$ which satisfy $|X|^2 = 2^m$. We first summarize the results that can be deduced from the theorems in Section 5.

Corollary 24. *Suppose there exists $X \in \mathbb{Z}[\zeta]$ with $|X|^2 = 2^m$, where m is odd. Write $f = \operatorname{ord}_p(2)$. We have the following.*

(a) $p \leq 2^{2m} + 2^m + 1$ and f is odd.

(b) $f < 2^m$ or $p \leq \frac{f^2 - 2^m}{f - 2^m}$.

(c) If $p > 2^{2(m-2)} + 2^{m-2} + 1$, then $X \not\equiv 0 \pmod 2$.

(d) $f < 2^{m+1}$.

(*e*) *$\ell(X) \in \{uf, uf+1\}$ for some positive integer u and $\ell(X) < 2^{m+1}$.*

(*f*) *$p \equiv 7 \pmod 8$ or $p \equiv 1, 9, 17, 25, 33, 41, 49, 57 \pmod{64}$.*

Proof. Parts (a), (b), and (e) follow directly from Theorems 22 and 23. For part (c), suppose $X \equiv \ 0 \pmod 2$. The $2^m = |X^2| \equiv 0 \pmod 4$ and thus $m \geq 3$, as m is odd. Furthermore, $Y = X/2 \in \mathbb{Z}[\zeta]$ and $|Y|^2 = 2^{m-2}$. Hence $p \leq 2^{2m-2} + 2^{m-1} + 1$ by Theorem 23. This proves part (c). By Theorem 22 (b), we have $f \leq \ell(X) < 2^{m+1}$, which proves part (d). To prove part (f), note that $f = \mathrm{ord}_p(2)$ is odd by part (a). Hence 2 is a square mod p and thus $p \equiv \pm 1 \pmod 8$. Suppose $p \equiv 1 \pmod 8$. As f is odd, 2 is biquadratic residue mod p and thus p is square mod 64 by a result of Gauß[8]. This completes the proof. □

Using conditions (a), (b), and (d) in Corollary 24, it is straightforward to deduce the following.

Corollary 25. *Suppose there exists $X \in \mathbb{Z}[\zeta]$ with $|X|^2 = 2^m$.*

(*a*) *If $m = 1$, then $p = 7$.*

(*b*) *If $m = 3$, then $p \in \{7, 23, 31, 73\}$.*

(*c*) *If $m = 5$, then $p \in \{7, 23, 31, 47, 71, 73, 79, 89, 103, 127, 151, 223, 233, 337, 601\}$.*

(*d*) *If $m = 7$, then*

$$p \in \{7, 23, 31, 47, 71, 73, 79, 89, 103, 127, 151, 167, 191, 199, 223, 233, 239, 263, 271, 311, 337, 359, 367, 383, 431, 439, 463, 479, 487, 503, 601, 631, 727, 881, 911, 919, 937, 1103, 1801, 2089, 2143, 2351, 2593, 2687, 3191, 3391, 4177, 4513, 6361, 6553, 8191, 9719, 11119, 11447, 13367, 14951\}.$$

We get the following directly from Result 10.

Corollary 26. *Let m be a positive integer and suppose that $X \in \mathbb{Z}[\zeta]$ is a solution of $|X|^2 = 2^m$. If $2^{\mathrm{ord}_p(2)} \not\equiv 1 \pmod{p^2}$, then $X\zeta^i \in \mathbb{Z}[\zeta_p]$ for some integer i.*

Throughout this section, we fix the following notation. Suppose that $X \in \mathbb{Z}[\zeta]$ satisfies $|X|^2 = 2^m$, where m is odd. By Theorem 22 (e), replacing X by $X\zeta^i$ for some integer i, if necessary, we can assume that there is a minimal alias

$$Z = c_0 + \sum_{i=1}^{u} c_i \Gamma_i \tag{23}$$

of X, where $u > 0$, $c_0, \dots, c_u \in \mathbb{Z}$, $c_i \neq 0$ for $i > 0$, the Γ_i's are distinct orbits of $g \mapsto g^2$ on $G \setminus \{1\}$ and $|\Gamma_i| = f$ for all i. Here we use the same notation as before. In particular, $G = \langle g \rangle$ is cyclic group of order p^a and P is the subgroup of G of order p. Note that $Z^{(2)} = Z$. Moreover,

$$ZZ^{(-1)} = 2^m + PY \tag{24}$$

for some $Y \in \mathbb{Z}[G]$ by Theorem 23. In the following list, we summarize the most important notation required for the rest of this section.

(1) $f = \mathrm{ord}_p(2)$.

(2) $X \in \mathbb{Z}[\zeta]$ with $|X|^2 = 2^m$, where $m \geq 3$ is odd.

(3) Z is a minimal alias of X satisfying (23), (24), and $Z^{(2)} = Z$.

(4) $S = c_0^2 + f \sum_{i=1}^{u} c_i^2$. Note that S is the coefficient of the identity in $ZZ^{(-1)}$.

To get a deeper understanding of the situation, we first find a bound on the ℓ_2-norm of the coefficient vector of Z, that is, on $S = c_0^2 + f \sum_{i=1}^{u} c_i^2$.

Lemma 27. *If $p > 2^{m+1}$, then $S \leq 2^{m+1}$.*

Proof. Write $s = \ell(X)$. Note that $s < 2^{m+1}$ by Corollary 24 (e). First, we assume $s \leq (p-1)/2$. As $Z = c_0 + \sum_{i=1}^{u} c_i \Gamma_i$ is minimal, it follows from Corollary 21 that

$$2^m = \mathcal{M}(X) \geq \frac{S(p-s)}{p-1} \geq \frac{S}{2}.$$

Therefore, $S \leq 2^{m+1}$.

Next, we assume $s \geq (p+1)/2$. By Corollary 21, we have

$$2^m = \mathcal{M}(X) \geq \frac{s(2s-p) + 2S(p-s)}{2(p-1)}.$$

Therefore,

$$2S \leq \frac{2^{m+1}(p-1) - s(2s-p)}{p-s}. \tag{25}$$

We aim to find an upper bound for the right hand side subject to $(p+1)/2 \leq s \leq 2^{m+1}$. Write $f(s) = [2^{m+1}(p-1) - s(2s-p)]/(p-s)$. Then

$$f'(s) = \frac{2^m(p-1) + p^2 + 2s^2 - 4ps}{(p-s)^2}.$$

Note that $g(s) = 2^m(p-1) + p^2 + 2s^2 - 4ps$ is a quadratic function of s with minimum at $s = p$ and that $g((p+1)/2) = 2^m(p-1) - (p^2+2p-1)/2 < 0$, as $p > 2^{m+1}$ by assumption. This implies $g(s) < 0$ and thus $f'(s) < 0$ for $(p+1)/2 \leq s < p$. Since $(p+1)/2 \leq s < 2^{m+1} < p$, we conclude

$$f(s) \leq f\left(\frac{p+1}{2}\right) = \frac{2^{m+1}(p-1) - (p+1)/2}{(p-1)/2} = 2^{m+2} - \frac{p+1}{p-1} < 2^{m+2}. \tag{26}$$

Combining (25) and (26), we get $S \leq 2^{m+1}$. □

Recall that $ZZ^{(-1)} = 2^m + PY$ by (24). As $ZZ^{(-1)} = (ZZ^{(-1)})^{(-1)}$, this implies $(PY)^{(-1)} = PY$. Similarly, $Z^{(2)} = Z$ and (24) imply $(PY)^{(2)} = PY$. For convenience, we write $PY = \lambda P + PY'$ with $\lambda \in \mathbb{Z}$ and $Y' \in \mathbb{Z}[G]$ such that P and $\operatorname{supp}(PY')$ are disjoint. We thus have

$$ZZ^{(-1)} = 2^m + PY = 2^m + \lambda P + PY'. \tag{27}$$

Observe that $(PY')^{(2)} = PY'$ and $(PY')^{(-1)} = PY'$, as $(PY)^{(2)} = PY$ and $(PY)^{(-1)} = PY$.

Corollary 28. *We have $S = 2^m + \lambda$. Moreover, if $p > 2^{m+1}$, then $\lambda \leq 2^m$.*

Proof. Comparing the coefficient of identity on both sides of (27), we find $S = 2^m + \lambda$. The second statement thus follows from Lemma 27. □

Lemma 29. *We have*

$$S^2 \geq |2^m + \lambda| + |\lambda|(p-1) + |\text{supp}(PY')|\,. \tag{28}$$

Proof. Write $Z = \sum_{g \in G} a_g g$ and $ZZ^{(-1)} = \sum_{g \in G} b_g g$ with $a_g, b_g \in \mathbb{Z}$. Note that $S = \sum_{g \in G} a_g^2$. As $ZZ^{(-1)} = \sum_{g,h \in G} a_g a_h g h^{-1}$, we conclude

$$\sum_{g \in G} |b_g| \leq \sum_{g,h \in G} |a_g a_h| = \left(\sum_{g \in G} |a_g| \right)^2 \leq \left(\sum_{g \in G} a_g^2 \right)^2 = S^2. \tag{29}$$

On the other hand, as $ZZ^{(-1)} = 2^m + \lambda P + PY'$, we have

$$\sum_{g \in G} |b_g| \geq |2^m + \lambda| + |\lambda|(p-1) + |\text{supp}(PY')|\,. \tag{30}$$

Combining (29) and (30), we get (28). □

Lemma 30. *Suppose that* $2^f \not\equiv 1 \pmod{p^2}$ *or* $p > 2^{2m-4}$*. Then*

$$ZZ^{(-1)} = 2^m + \lambda P \tag{31}$$

for some integer λ*. In particular,* $2^m + \lambda p$ *is a perfect square. Moreover, if* $p > 2^m$*, then* $\lambda > 0$*.*

Proof. If $a = 1$, then (31) immediately follows from (24). Hence we can assume $a > 1$.

First suppose $2^f \not\equiv 1 \pmod{p^2}$. Then $X\zeta^j \in \mathbb{Z}[\zeta_p]$ for some integer j by Corollary 26. Recall that $Z(\zeta) = X$, as Z is an alias of X. Hence $Zg^j(\zeta) = X\zeta^j \in \mathbb{Z}[\zeta_p]$. Note that Zg^j is minimal, since Z is minimal. Let N be defined as in Lemma 18 and write $Zg^j = \sum_{i \in N} Z_i g^i$. Since $Zg^j(\zeta) = \sum_{i \in N} Z_i(\zeta)\zeta^i \in \mathbb{Z}[\zeta_p]$ and $\{\zeta^i : i \in N\}$ is linearly independent over $\mathbb{Z}[\zeta_p]$, we conclude that $Z_i(\zeta) = 0$ for all i with $i \not\equiv 0 \pmod{p^{a-1}}$. Since Zg^j is minimal, each Z_i is minimal by Lemma 18 (a). As $Z_i(\zeta) = 0$ for $i \not\equiv 0 \pmod{p^{a-1}}$, this implies $Z_i = 0$ for all $i \not\equiv 0 \pmod{p^{a-1}}$. We conclude that $Zg^j = \sum_{i \in N} Z_i g^i \in \mathbb{Z}[P]$. Thus $2^m + PY = ZZ^{(-1)} = (Zg^j)(Zg^j)^{(-1)} \in \mathbb{Z}[P]$, where Y is defined as in (24). This implies $Y \in \mathbb{Z}[P]$ and thus $PY = |Y|P$. Hence (31) holds (with $\lambda = |Y|$). This completes the proof of (31) in the case $2^f \not\equiv 1 \pmod{p^2}$.

Using Corollary 25, it is straightforward to check that $2^f \not\equiv 1 \pmod{p^2}$ whenever $m \le 5$. Hence we can assume $m \ge 7$.

Now suppose $p > 2^{2m-4}$. Then $p > 2^{m+3}$, as $m \ge 7$. Moreover, $\lambda \le 2^m$ by Corollary 28. In view of (27), to prove (31), we need to show $Y' = 0$. Suppose $Y' \ne 0$. Then, as $PY' \cap P = \emptyset$, there is $g \in G \setminus P$ with $gP \subset \mathrm{supp}(PY')$. Recall that $f = \mathrm{ord}_p(2)$ is odd. Thus $\mathrm{ord}_p(-2) = 2f$. Since $(PY')^{(2)} = PY'$ and $(PY')^{(-1)} = PY'$, we conclude $g^{(-2)^j}P \subset \mathrm{supp}(PY')$ for $j = 0, \dots, 2f-1$.

Next, we show that the cosets $g^{(-2)^j}P$, $j = 0, \dots, 2f-1$, are pairwise disjoint. Note that $\mathrm{ord}_{p^{a-1}}(-2)$ is divisible by $2f$, since $\mathrm{ord}_p(-2) = 2f$ and $a > 1$. Assume $g^{(-2)^j}P \cap g^{(-2)^{j'}}P \ne \emptyset$ for some j, j' with $0 \le j, j' \le 2f-1$, $j \ne j'$. Then there are $r, s \in \{0, \dots, p-1\}$ with $g^{(-2)^j + rp^{a-1}} = g^{(-2)^{j'} + sp^{a-1}}$. This implies $(-2)^j \equiv (-2)^{j'} \pmod{p^{a-1}}$, which contradicts the fact that $\mathrm{ord}_{p^{a-1}}(-2)$ is divisible by $2f$. Hence the cosets $g^{(-2)^j}P$, $j = 0, \dots, 2f-1$, are indeed pairwise disjoint.

As $g^{(-2)^j}P \subset \mathrm{supp}(PY')$ for $j = 0, \dots, 2f-1$, we conclude $|\mathrm{supp}(PY')| \ge 2fp$. Using Lemma 29, we find

$$(2^m + \lambda)^2 = S^2 \ge |2^m + \lambda| + |\lambda|(p-1) + 2fp.$$

Recall that $p > 2^{m+3}$ and $\lambda \le 2^m$. Since

$$2^{m+1}\lambda + \lambda^2 \le |\lambda|(2^{m+1} + \lambda) \le |\lambda| 2^{m+2} \le |\lambda|(p-1) \le |\lambda|(p-1) + (2^m + \lambda),$$

it follows that $2^{2m} > 2pf$. As $p > 2^{2m-4}$ and f is odd, we conclude $f \le 7$. On the other hand, we have $p > 2^{2m-4} \ge 2^{10}$, as we assume $m \ge 7$. This implies $f = \mathrm{ord}_p(2) > 10$, a contradiction. Therefore, $Y' = 0$. This completes the proof (31).

Note that $2^m + \lambda p = |Z|^2$ is a perfect square by (31). It remains to show that $\lambda > 0$ if $p > 2^m$. If $\lambda = 0$, then $|Z|^2 = 2^m$, which is impossible, as m is odd. Thus $\lambda \ne 0$. If $\lambda < 0$, then $0 \le |Z|^2 = 2^m + \lambda p \le 2^m - p$ and thus $p \le 2^m$. Hence $p > 2^m$ indeed implies $\lambda > 0$. □

Our next goal is to determine all possible values of λ. For a prime r and an integer n, let $\nu_r(n)$ be the r-adic valuation of n, i.e., $r^{\nu_r(n)}$ is the largest power of r dividing n.

Lemma 31. *Suppose that $ZZ^{(-1)} = 2^m + \lambda P$ with $\lambda \in \mathbb{Z}$. Then the following hold.*

(*a*) *If q is an odd prime divisor of λ, then $q \equiv \pm 1 \pmod 8$.*

(*b*) *Either $\nu_2(\lambda)$ is even or $\nu_2(\lambda) = m$.*

(*c*) *If $1 \leq \lambda \leq 29$, then $\lambda \in \{1, 4, 7, 16, 17\}$ unless $m = 3$ and $\lambda = 8$.*

(*d*) *If λ is odd, then $\lambda \equiv p \pmod 8$.*

(*e*) $c_0^2 + f \sum_{i=1}^{u} c_i^2 = 2^m + \lambda$ *and* $\left(c_0 + f \sum_{i=1}^{u} c_i\right)^2 = 2^m + \lambda p.$

Proof. Let q be an odd prime divisor of λ. By applying the trivial character of G to $ZZ^{(-1)} = 2^m + \lambda P$, we obtain $|Z|^2 = 2^m + \lambda p$. As m is odd, this implies that 2 is a square modulo q. Using the second supplement to quadratic reciprocity, we get part (a).

Write $\lambda = 2^t \mu$ where μ is odd. Note that $t = \nu_2(\lambda)$. If $t > m$, then $\nu_2(2^m + \lambda p) = 2^m$, which contradicts $|Z|^2 = 2^m + \lambda p$, as m is odd. Hence $t \leq m$. If $t < m$, then $t = \nu_2(2^m + \lambda p) = \nu_2(|Z|^2)$ and thus t is even. This proves part (b).

Part (c) follows from part (a) and (b). Finally, as $m \geq 3$, we have $|Z|^2 \equiv \lambda p \pmod 8$, and this implies (d), since $x^2 \equiv 1 \pmod 8$ for all odd integers x.

Finally, recall that $Z = c_0 + \sum_{i=1}^{u} c_i \Gamma_i$ and $|\Gamma_i| = f$ for all i. Hence part (e) follows by comparing the coefficient identity on both sides of $ZZ^{(-1)} = 2^m + \lambda P$ and applying the trivial character to this equation. □

Lemma 32. *If $m \geq 7$ and $p \geq 2^{2m-4} + 2^{m-2} + 1$, then $\lambda \in \{1, 4, 7, 16\}$.*

Proof. Suppose that $m \geq 7$ and $p \geq 2^{2m-4} + 2^{m-2} + 1$. Then $p > 2^{m+3}$ and thus $\lambda > 0$ by Lemma 30. By Lemma 27 and Corollary 28, we have $S = 2^m + \lambda \leq 2^{m+1}$ and hence $\lambda \leq 2^m$. Moreover, $(2^m + \lambda)^2 \geq 2^m + \lambda p$ by Lemma 29. We thus have $g(\lambda) \geq 0$ where

$$g(t) := t^2 + (2^{m+1} - p)t + 2^{2m} - 2^m.$$

Note that $g(t)$ is decreasing for $t \leq (p - 2^{m+1})/2$ and that $\lambda \leq 2^m < (2^{m+3} - 2^{m+1})/2 < (p - 2^{m+1})/2$. Hence, if we have $g(t) < 0$ for some $t \in \mathbb{R}$, then $t > \lambda$. For $m \geq 9$, we have

$$\begin{aligned} g(17) &= 17^2 + 17(2^{m+1} - p) + 2^{2m} - 2^m \\ &< 17^2 + (16+1)(2^{m+1} - 2^{2m-4} - 2^{m-2}) + 2^{2m} - 2^m \\ &= 17^2 + 2^{m+5} - 2^{2m} - 2^{m+2} + 2^{m+1} - 2^{2m-4} - 2^{m-2} + 2^{2m} - 2^m \\ &< 17^2 + 2^{m+1} - 2^{m+2} = 17^2 - 2^{m+1} < 0. \end{aligned}$$

On the other hand, if $m = 7$, then

$$g(23) = 23^2 + 23(2^8 - p) + 2^{14} - 2^7 < 23^2 + 23(2^8 - 2^{10}) + 2^{14} - 2^7 < 0.$$

Therefore, $\lambda < 17$ if $m \geq 9$ and $\lambda < 23$ if $m = 7$. In view of Lemma 31 (c), it only remains to prove $(m, \lambda) \neq (7, 17)$. Thus suppose $m = 7$ and $\lambda = 17$. As $(2^m + \lambda)^2 \geq 2^m + \lambda p$, we have

$$p \leq \frac{(2^7 + 17)^2 - 2^7}{17} < 1230.$$

Hence $2^{10} + 2^5 + 1 \leq p \leq 1229$. Recall $|Z|^2 = 2^m + \lambda p$. It can be checked that, for p in the above range, $2^7 + 17p$ is a perfect square only when $p = 1129$. However, if $p = 1129$, then $f = 564$, which contradicts Corollary 24 (a). □

For $m = 3$ and 5, it is possible to use our results to find all possible solutions of $X\bar{X} = 2^m$ in $\mathbb{Z}[\zeta]$ (recall that we write $\zeta = \zeta_{p^a}$). We will only treat those cases which are needed for application in Section 7. As the necessary computations are tedious and straightforward, we give the details only for one case. We say that $A, B \in \mathbb{Z}[\zeta]$ are **equivalent** if $B = \pm\zeta^i A^\tau$ for some integer i and some $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$.

Corollary 33. *If $m = 1$, then $p = 7$ and X is equivalent to $\zeta_7 + \zeta_7^2 + \zeta_7^4$. If $m = 3$, then $p \in \{7, 23, 31, 73\}$ and X is equivalent to one of the following.*

$$2\left(\sum_{i=0}^{2} \zeta_7^{2^i}\right), \; -2 + \sum_{i=0}^{2} \zeta_7^{2^i}, \; 2 + \sum_{i=0}^{10} \zeta_{23}^{2^i}, \; \sum_{i=1}^{15} \zeta_{31}^{i^2}, \; 1 + \sum_{i=0}^{4} \left(\zeta_{31}^{5\cdot 2^i} + \zeta_{31}^{7\cdot 2^i} + \zeta_{31}^{11\cdot 2^i}\right), \; \sum_{i=0}^{8} \zeta_{73}^{2^i}.$$

Proof. By Corollary 25, we have $p = 7$ if $m = 1$ and $p \in \{7, 23, 31, 73\}$ if $m = 3$. Suppose $m = 3$ and $p = 23$. Note that $f = \mathrm{ord}_{23}(2) = 11$ and $2^f \not\equiv 1 \pmod{23^2}$. Hence we can assume $X \in \mathbb{Z}[\zeta_{23}]$ by Proposition 26. Recall that Z is a minimal alias of X. As in the proof of Lemma 30, we see that $Z \in \mathbb{Z}[P]$ where P is a group of order 23. By Corollary 28 and Lemma 30, we have $1 \leq \lambda \leq 8$ and $8 + 23\lambda = |Z|^2$. This implies $\lambda \in \{4, 7\}$ and $|Z|^2 \in \{100, 169\}$. Replacing Z by $-Z$, if necessary, we can assume $(\lambda, |Z|) \in \{(4, 10), (7, 13)\}$. Note that $S = c_0^2 + 11\sum_{i=1}^{u} c_i^2 = 2^m + \lambda = 8 + \lambda$. Hence, if $\lambda = 4$, then $u = 1$, $c_0 = -1$, and $c_1 = 1$. Moreover, if $\lambda = 7$, then $u = 1$ and $c_0 = 2$ and $c_1^2 = 1$. As $Z = c_0 + c_1\Gamma_1$ where Γ_1 is an orbit of size 11 of $g \mapsto g^2$ on P, it is straightforward to check that in both cases $X = Z(\zeta_{23})$ is equivalent to $2 + \sum_{i=1}^{10} \zeta_{23}^{i^2}$. The proofs for the other cases are similar. □

The proof of the following result is analogous to that of Corollary 33 and is skipped.

Corollary 34. *Suppose $m = 5$. If $p = 151$, then X is equivalent to*

$$3 + \sum_{i=0}^{14} \zeta_{151}^{23 \cdot 2^i} + \sum_{i=0}^{14} \zeta_{151}^{35 \cdot 2^i}.$$

If $p = 127$, then X is equivalent to $\sum_{i=1}^{9} \sum_{j=0}^{6} \zeta_{127}^{2^j \alpha_i}$ where $\{\alpha_1, \ldots, \alpha_9\}$ is one of the following sets.
$\{1, 3, 9, 27, 28, 71, 94, 116, 121\}, \{1, 3, 9, 27, 28, 73, 81, 94, 121\}, \{1, 3, 9, 27, 66, 71, 73, 109, 116\},$
$\{1, 3, 22, 27, 66, 73, 84, 116, 125\}, \{1, 3, 27, 28, 66, 73, 92, 94, 125\}, \{1, 9, 22, 71, 73, 81, 84, 94, 121\}.$

Remark 35. The six inequivalent solutions $X \in \mathbb{Z}[\zeta_{127}]$ of $|X|^2 = 32$ are in one-two-one correspondence to the six equivalence classes of $(127, 63, 31)$ difference sets, cf. [1, pp. 154–155].

7 Applications to Generalized Bent Functions

Throughout this section, we fix the following notation. Let m be an odd positive integer. Write $H = U \times K$ with $U = \mathbb{Z}_{p^a}^m$ and $K = \mathbb{Z}_2^m$ and note that $H \cong \mathbb{Z}_{2p^a}^m$. Recall that we write $\zeta = \zeta_{p^a}$. We assume that a GBF $f : \mathbb{Z}_{2p^a}^m \to \mathbb{Z}_{2p^a}$ exists. By (5), this implies that there is $D \in \mathbb{Z}[\zeta][H]$ with

$$DD^{(-1)} = 2^m p^{am}. \tag{32}$$

(note that $\mathbb{Z}[\zeta_{2p^a}] = \mathbb{Z}[\zeta]$, since $-\zeta \in \mathbb{Z}[\zeta]$ and $-\zeta$ is a primitive $(2p^a)$th root of unity). Let $\chi : U \to \mathbb{C}^*$ be any character of U. We extend χ to a ring homomorphism $\mathbb{Z}[\zeta][H] \to \mathbb{Z}[\zeta][K]$ by linearity and setting $\chi(g) = g$ for all $g \in K$. Write $D_\chi = \chi(D)$. Then

$$D_\chi D_\chi^{(-1)} = 2^m p^{am}. \tag{33}$$

by (32). Write $D_\chi = \sum_{h\in K} x_h h$ with $x_h \in \mathbb{Z}[\zeta]$ and $\Theta = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right)\zeta_p^x$. By (33), for any character τ on K, we have $|\tau(D_\chi)|^2 = 2^m p^{am}$ and thus $\tau(D_\chi) \equiv 0 \pmod{\Theta^{am}}$ by Corollary 8. Using Result 1, we conclude

$$x_h|K| = \sum_{\tau \in \hat{K}} \tau(D_\chi)\tau(h)^{-1} \equiv 0 \bmod \ (\Theta^{am})$$

for all $h \in K$. Note that $|K| = 2^m$ and Θ are relatively prime in $\mathbb{Z}[\zeta]$, since $|\Theta|^2 = p$ and p is odd. Hence it follows that $x_h \equiv 0 \pmod{\Theta^{am}}$ for all $h \in K$. Thus $E_\chi := D_\chi/\Theta^{am}$ is an element of $\mathbb{Z}[\zeta][K]$. Moreover, note that $E_\chi E_\chi^{(-1)} = 2^m$, as $|\Theta|^2 = p$. Let us summarize what we found so far.

Proposition 36. *Suppose that $D \in \mathbb{Z}[\zeta][H]$ satisfies* (32)*, let χ be a character of U, and write $E_\chi = \chi(D)/\Theta^{am}$. Then $E_\chi \in \mathbb{Z}[\zeta][K]$ and*

$$E_\chi E_\chi^{(-1)} = 2^m. \tag{34}$$

The application of our results in Section 6 to equation (34) immediately gives the following.

Corollary 37. *Suppose that a GBF from $\mathbb{Z}_{2p^a}^m$ to $\mathbb{Z}_{2p^a}$ exists. Then $p \le 2^{2m} + 2^m + 1$ and $p \equiv 7 \pmod 8$ or $p \equiv 1, 9, 17, 25, 33, 41, 49, 57 \pmod{64}$. Moreover, the following hold.*

(*a*) *If $m = 1$, then $p = 7$.*

(*b*) *If $m = 3$, then $p \in \{7, 23, 31, 73\}$.*

(*c*) *If $m = 5$, then $p \in \{7, 23, 31, 47, 71, 73, 79, 89, 103, 127, 151, 223, 233, 337, 601\}$.*

Proof. Let χ be any character of U, let τ_0 be the trivial character of K, and set $X = \tau_0(E_\chi)$. Then $X \in \mathbb{Z}[\zeta]$ and $|X|^2 = 2^m$ by (34). Hence the assertions follows from Corollaries 24 and 25. □

Our next objective is to eliminate more primes from the lists above.

Lemma 38. *Let $W = \{w \in \mathbb{Z}[\zeta] : w\bar{w} = 2^m\}$. Suppose*

$$v + w \not\equiv 0 \pmod 2 \text{ for all } v, w \in W \text{ with } w \neq \pm v. \tag{35}$$

Then for any character χ of U, there exist $w \in W$ and $g \in K$ such that $E_\chi = wg$.

Proof. If $v \equiv 0 \ (\bmod\ 2)$ for $v \in W$, then $w := \zeta v \in W$, $v + w \equiv 0 \ (\bmod\ 2)$, and $w \neq \pm v$. This contradicts (35) and thus we have $v \not\equiv 0 \pmod 2$ for all $v \in W$.

Let τ_0 be the trivial character of K and write $v = \tau_0(E_\chi)$. We claim that

$$\tau(E_\chi) = \pm v \text{ for all } \tau \in \hat{K}. \tag{36}$$

Let τ be a nontrivial character of K and write $w = \tau(E_\chi)$. To prove (36), it suffices to show $w = \pm v$. By (34), we have $v, w \in W$. Let $T = \{g \in K : \tau(g) = 1\}$ and write $E_\chi = \sum_{g \in K} x_g g$ where $x_g \in \mathbb{Z}[\zeta]$. Note that $\tau(g) = -1$ for all $g \in K \setminus T$, as all nontrivial characters of K have order 2. Note that

$$v + w = \sum_{g \in K} x_g + \left(\sum_{g \in T} x_g - \sum_{g \in K \setminus T} x_g \right) = 2 \sum_{g \in T} x_g \equiv 0 \pmod 2.$$

Hence $w = \pm v$ by (35). This proves (36).

Let $A = \{\tau \in \hat{K} : \tau(E_\chi) = v\}$ and $B = \hat{K} \setminus A$. By Result 1 and (36), we get

$$x_g = \frac{1}{|K|} \sum_{\tau \in \hat{K}} \tau(E_\chi)\tau(g) = \frac{v}{2^m} \left(\sum_{\tau \in A} \tau(g) - \sum_{\tau \in B} \tau(g) \right). \tag{37}$$

As $v \not\equiv 0 \ (\bmod\ 2)$, there is a prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\zeta]$ such that $2 \in \mathfrak{p}$ and $v \notin \mathfrak{p}$. For $y \in \mathbb{Z}[\zeta]$, let $\nu_\mathfrak{p}(y)$ denote the largest nonnegative integer k such that $y \in \mathfrak{p}^k$ (with the convention $\nu_\mathfrak{p}(y) = 0$ if $y \notin \mathfrak{p}$). Note that $\nu_\mathfrak{p}(v) = 0$, as $v \notin \mathfrak{p}$. Write $T = \sum_{\tau \in A} \tau(g) - \sum_{\tau \in B} \tau(g)$. We have

$$0 \leq \nu_\mathfrak{p}(x_g) = \nu_\mathfrak{p}(v) + \nu_\mathfrak{p}(T) - \nu_\mathfrak{p}(2^m) = \nu_\mathfrak{p}(T) - m$$

by (37) and thus $\nu_\mathfrak{p}(T) \geq m$. As T is a rational integer, this implies $T \equiv 0 \pmod{2^m}$. Using (37), we conclude $x_g \equiv 0 \pmod v$ for all $g \in K$ and thus $E_\chi \equiv 0 \pmod v$.

Hence $F := E_\chi/v \in \mathbb{Z}[\zeta][K]$ and $FF^{(-1)} = 1$ by (34), as $v\bar{v} = 2^m$ by assumption. Write $F = \sum_{g\in K} y_g g$ with $y_g \in \mathbb{Z}[\zeta]$. As $FF^{(-1)} = 1$, we have $\sum_{g\in K} |y_g|^2 = 1$. This implies $\left|y_g^\ell\right| \leq 1$ for all $g \in K$ and all $\ell \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Hence, by Result 6, there is $g \in G$ such that y_g is a root of unity and $y_h = 0$ for all $h \neq g$. We conclude $F = y_g g$ and thus $E_\chi = Fv = (y_g v)g$, which completes the proof, as $y_g v \in W$. □

Theorem 39. *If condition* (35) *holds, then there is no GBF from* $\mathbb{Z}_{2p^a}^m$ *to* $\mathbb{Z}_{2p^a}$.

Proof. Suppose that condition (35) holds and suppose that a GBF $f : \mathbb{Z}_{2p^a}^m \to \mathbb{Z}_{2p^a}$ exists. Write $H = U \times K$ with $U = \mathbb{Z}_{p^a}^m$ and $K = \mathbb{Z}_2^m$ and note that $H \cong \mathbb{Z}_{2p^a}^m$. Recall that we write $\zeta = \zeta_{p^a}$. By (5), there is $D \in \mathbb{Z}[\zeta][H]$ with $DD^{(-1)} = 2^m p^{am}$. Moreover,

$$\sum_{\tau\in\hat{H}} \tau(D)\overline{\tau\chi(D)} = 0 \tag{38}$$

for every nontrivial character χ of H by Result 3.

Note that every $\tau \in \hat{H}$ uniquely can be written as $\tau = \tau_K \circ \tau_U$ where τ_K is a character of K and τ_U is a character of U, extended to $\mathbb{Z}[\zeta][H]$ by $\tau_U(h) = h$ for all $h \in K$ and linearity. Note that $\tau_U(D) = \Theta^{am} E_{\tau_U}$. As we are assuming that (35) holds, Lemma 38 gives

$$\tau(D) = \tau_K \circ \tau_U(D) = \tau_K\left(\Theta^{am} E_{\tau_U}\right) = \Theta^{am} w(\tau)\tau_K(g(\tau)) \tag{39}$$

for all $\tau \in \hat{H}$, where $w(\tau) \in W$ and $g(\tau) \in K$. Note that $w(\tau)$ and $g(\tau)$ only depend on τ_U, that is, $w(\tau\chi) = w(\tau)$ and $g(\tau\chi) = g(\tau)$ for all $\chi \in U^\perp$. Moreover, $|\tau_K(g(\tau))|^2 = 1$ for all $\tau \in \hat{H}$, as $\tau_K(g(\tau))$ is a root of unity.

Now let χ be any character of H which is trivial on U and nontrivial on K. Note that $\tau_K(g)(\tau\chi)_K(g) = \chi(g)$ for all $g \in H$, as τ_K has order 1 or 2 and $\chi_K(g) = \chi(g)$. Using

(38) and (39), we get

$$\begin{aligned}0 =&\sum_{\tau\in\hat{H}}\tau(D)\overline{\tau\chi(D)}\\ =&\sum_{\tau\in\hat{H}}\Theta^{am}w(\tau)\tau_K(g(\tau))\overline{\Theta^{am}w(\tau\chi)(\tau\chi)_K(g(\tau\chi))}\\ =&|\Theta|^{2am}\sum_{\tau\in\hat{H}}w(\tau)\tau_K(g(\tau))\overline{w(\tau)(\tau\chi)_K(g(\tau))}\\ =&2^m p^{am}\sum_{\tau\in\hat{H}}\tau_K(g(\tau))(\tau\chi)_K(g(\tau)).\\ =&2^m p^{am}\sum_{\tau\in\hat{H}}\chi(g(\tau)).\end{aligned}$$

Let $\hat{H}=\bigcup_{i=1}^{p^a}|U|^{\perp}\tau_i$, $\tau_i\in\hat{H}$, be the decomposition of $\hat{H}$ into cosets of $U^{\perp}$. Since $g(\tau\chi)=g(\tau)$ for all $\chi\in U^{\perp}$ and $|U^{\perp}|=2^m$, we get

$$0=\sum_{\tau\in\hat{H}}\chi(g(\tau))=2^m\sum_{i=1}^{p^a}\chi(g(\tau_i)).$$

and thus $\sum_{i=1}^{p^a}\chi(g(\tau_i))=0$. This is impossible, since p is odd and $\chi(g(\tau_i))=\pm1$. □

Next, we find some conditions to ensure (35) is satisfied.

Lemma 40. *If $f>2^{m-1}$, then condition* (35) *holds.*

Proof. If f is even, then $W=\emptyset$ by Corollary 24 (a). Hence we can assume that f is odd. Suppose that $v\equiv 0 \pmod 2$ for $v\in W$. Then $X=v/2$ satisfies $|X|^2=2^{m-2}$ and thus $f<2^{m-1}$ by Corollary 24 (d), which contradicts our assumption. Hence $v\not\equiv 0 \pmod 2$ for all $v\in W$.

Now suppose that $v+w\equiv 0 \pmod 2$ for $v,w\in W$, that is,

$$v\equiv w \pmod 2. \tag{40}$$

Write $R=\mathbb{Z}[\zeta]$. Recall that f is odd. Thus, by Result 7 (b), the prime ideals of R containing 2 are not invariant under complex conjugation. That is, these prime ideals occur in complex conjugate pairs in the prime ideal factorization of $2R$. Hence $2R = \prod_{i=1}^k(\mathfrak{p}_i\overline{\mathfrak{p}_i})$ by Result 7 (b), where the $\mathfrak{p}_i$'s are distinct prime ideals of R and $k = (p-1)/(2f)$. As $|v|^2 = |w|^2 = 2^m$, we conclude

$$vR = \prod_{i=1}^k(\mathfrak{p}_i^{a_i}(\overline{\mathfrak{p}_i})^{m-a_i}) \text{ and } wR = \prod_{i=1}^k(\mathfrak{p}_i^{b_i}(\overline{\mathfrak{p}_i})^{m-b_i}).$$

with $a_i, b_i \in \mathbb{Z}$ and $0 \le a_i, b_i \le m$. Note that (40) implies that a prime ideal divides vR if and only if divides wR. Hence for each i, we either have (a) $1 \le a_i, b_i \le m-1$, (b) $a_i = 0$ and $b_i = 0$, or (c) $a_i = m$ and $b_i = m$. Note that, in each case,

$$v\bar{w}R = \prod_{i=1}^k(\mathfrak{p}_i^{m+a_i-b_i}(\overline{\mathfrak{p}_i})^{m-a_i+b_i})$$

is divisible by $\mathfrak{p}_i^2\overline{\mathfrak{p}_i}^2$. This implies $v\bar{w} \equiv 0 \pmod 4$.

Set $Y = v\bar{w}/4$. Then $|Y|^2 = 2^{2m-4}$. If Y is nontrivial, then $f < 2^{m-1}$ by Result 9, contradicting our assumption. Hence Y is trivial, that is, $Y = \kappa 2^{m-2}$ for some root of unity κ. This implies

$$v\bar{w}R = 4YR = 4\kappa 2^{m-2}R = 2^mR = \prod_{i=1}^k(\mathfrak{p}_i\overline{\mathfrak{p}_i})^m.$$

Comparing this with the factorization of $v\bar{w}R$ we previously obtained, we conclude $a_i = b_i$ for all i, that is, $vR = wR$. Hence $w = \epsilon v$ for some unit ϵ of $\mathbb{Z}[\zeta]$. As w and v have the same absolute value, we have $|\epsilon| = 1$. Using Result 6, we infer $w = \pm\zeta^i v$ for some integer i and thus $v + w = (1 \pm \zeta^i)v$. Recall that $v \not\equiv 0 \pmod 2$. If $i \not\equiv 0 \pmod{p^a}$, then the ideal $(1 \pm \zeta^i)R$ is coprime to $2R$ and thus $v + w = (1 \pm \zeta^i)v \not\equiv 0 \pmod 2$, which contradicts our assumptions. Hence $i \equiv 0 \pmod{p^a}$ and thus $w = \pm v$, as required. □

For $m = 5$ and $m = 7$, the following lists those primes that survive Corollary 24 and are excluded by Theorem 39 and Lemma 40.

Corollary 41. *Assume the existence of a GBF from $\mathbb{Z}_{2p^a}^m$ to $\mathbb{Z}_{2p^a}$. Then we have the following.*

If $m = 5$, then $p \notin \{47, 71, 79, 103, 223, 233, 337, 601\}$.

If $m = 7$, then $p \notin \{167, 191, 199, 239, 263, 271, 311, 359, 367, 383, 439, 463, 479, 487, 503, 727, 911, 919, 937, 2593, 2687, 3391, 4177, 6553, 11447, 14951\}$.

Let G be a cyclic group of order p^a. Using the notation of Lemma 38, suppose that $w \in W$. It follows from Theorem 22 (e) that there is a minimal alias of w of the form

$$h\left(c_0 + \sum_{i=1}^{u} c_i \Gamma_i\right),$$

where $h \in G$, $c_i \in \mathbb{Z}$ and the Γ_i's are distinct orbits of $x \mapsto x^2$ on $G \setminus \{1\}$. It turns out that condition (35) is satisfied if we always have $c_1 = \cdots = c_u$ and c_1 is odd.

Lemma 42. *We use the notation of Lemma* 38*. Let G be a cyclic group of order p^a and suppose that every $w \in W$ has a minimal alias of the form*

$$h(c \pm S) \tag{41}$$

where $h \in G$, $c \in \mathbb{Z}$, and S is a subset of $G \setminus \{1\}$ with $S^{(2)} = S$ (note that h, c, and S may depend on w). Then condition (35) *is satisfied.*

Proof. Let $v \in W$ and let g be a fixed generator of G. By assumption, v has a minimal alias of the form (41). Replacing v by an equivalent number, if necessary, we can assume that v has a minimal alias of the form $Z = c + S$, where $c \in \mathbb{Z}$ and S is a subset of G with $S^{(2)} = S$. Note that $S \neq \emptyset$, as $|v|^2 = 2^m$ is a nonsquare. Let P be the subgroup of G of order p. By Lemma 16 (b), we have

$$|S \cap Ph| \leq (p-1)/2 \tag{42}$$

for all $h \in G$. Write $S = \sum_{j \in A} g^j$ with $A \subset \{1, \ldots, p^a - 1\}$. Note that $v = Z(\zeta) = c + \sum_{j \in A} \zeta^j$, as Z is an alias of v. Moreover, $\{1\} \cup \{\zeta^j : j \in A\}$ does not contain any coset of $\langle \zeta_p \rangle$ by (42). Hence $\{1\} \cup \{\zeta^j : j \in A\}$ is linearly independent over $\mathbb{Q}$ by Proposition 13 (b). As $S \neq \emptyset$, this implies $v = c + \sum_{j \in A} \zeta^j \not\equiv 0 \pmod 2$. Hence we have shown

$$v \not\equiv 0 \pmod 2 \text{ for all } v \in W. \tag{43}$$

Suppose that $v, w \in W$ satisfy

$$v + w \equiv 0 \pmod{2}. \tag{44}$$

To prove that condition (35) holds, we need to show $w = \pm v$. As before, we can assume that v has a minimal alias of the form $Z = c + S$, where $c \in \mathbb{Z}$ and S is a subset of G with $S^{(2)} = S$. By assumption, w has a minimal alias of the form $g^s(d \pm T)$, where $s, d \in \mathbb{Z}$ and T is a subset of G with $T^{(2)} = T$. Note that (44) holds if and only if $v - w \equiv 0 \pmod{2}$. Hence, replacing w by $-w$, if necessary, we can assume that w has a minimal alias of the form $Y = g^s(d + T)$. Note that $w = \zeta^s(d + T(\zeta))$ by the definition of an alias.

Let σ be the automorphism of $\mathbb{Q}(\zeta)$ determined by $\zeta^\sigma = \zeta^2$. Note that $v^\sigma = Z(\zeta)^\sigma = Z(\zeta) = v$, as $S^{(2)} = S$. Moreover,

$$w^\sigma = Y(\zeta)^\sigma = (\zeta^s)^\sigma(d + T(\zeta)^\sigma) = \zeta^{2s}(d + T(\zeta)) = \zeta^s w,$$

since $T^{(2)} = T$. Using (44), we conclude $0 \equiv (v + w)^\sigma \equiv v + \zeta^s w \pmod{2}$ and thus

$$(1 - \zeta^s)w \equiv 0 \pmod{2}. \tag{45}$$

On the other hand, we have $w \not\equiv 0 \pmod{2}$ by (43). If $\zeta^s \neq 1$, then $1 - \zeta^s$ is coprime to 2 and thus $(1 - \zeta^s)w \not\equiv 0 \pmod{2}$, contradicting (45). We conclude $\zeta^s = 1$ and hence $Y = d + T$.

Recall $S = \sum_{j \in A} g^j$ and write $T = \sum_{j \in B} g^j$ with $B \subset \{1, \dots, p^a - 1\}$. By (42), we have

$$c + d + \left(\sum_{j \in A} \zeta^j + \sum_{j \in B} \zeta^j \right) \equiv Z(\zeta) + Y(\zeta) = v + w \equiv 0 \pmod{2}. \tag{46}$$

Write $A = A_1 \cup A_2$ with $A_1 = A \cap \{ip^{a-1} : i = 1, \dots, p - 1\}$ and $A_2 = A \setminus A_1$. Similarly, write $B = B_1 \cup B_2$. For the convenience, of the reader we summarize some of the notation we have introduced. We have

$$\begin{aligned}
Z &= c + S = c + \sum_{j\in A} g^j,\\
Y &= d + T = d + \sum_{j\in B} g^j,\\
v &= Z(\zeta) = c + \sum_{j\in A_1} \zeta^j + \sum_{j\in A_2} \zeta^j,\\
w &= Y(\zeta) = d + \sum_{j\in B_1} \zeta^j + \sum_{j\in B_2} \zeta^j.
\end{aligned}$$

Note that $\{\zeta^j : j \in A_1\} \cup \{\zeta^j : j \in B_1\} \subset \mathbb{Z}[\zeta_p]$. As $\{\zeta^i : 0 \le i \le p^{a-1} - 1\}$ is linearly independent over $\mathbb{Q}(\zeta_p)$, we infer from (46) that

$$c + d + \left(\sum_{j\in A_1} \zeta^j + \sum_{j\in B_1} \zeta^j \right) \equiv 0 \pmod 2 \text{ and} \tag{47}$$

$$\sum_{j\in A_2} \zeta^j + \sum_{j\in B_2} \zeta^j \equiv 0 \pmod 2. \tag{48}$$

By (42), every coset of $\langle \zeta_p \rangle$ contains at most $(p-1)/2$ elements of $\{\zeta^j : j \in A\}$ and at most $(p-1)/2$ elements of $\{\zeta^j : j \in B\}$. Thus $A_2 \cup B_2$ does not contain any coset of $\langle \zeta_p \rangle$. By Proposition 13 (b), this shows that $\{\zeta^j : j \in A_2 \cup B_2\}$ is linearly independent over $\mathbb{Q}$. Hence (48) implies $A_2 = B_2$. Note that $|A_1| \le (p-1)/2$ and $|B_1| \le (p-1)/2$ by (42), as $\{g^j : j \in A_1\} \subset P$ and $\{g^j : j \in B_1\} \subset P$.

First suppose that $A_1 \cup B_1$ is a proper subset of $\{p^{a-1}, \dots, (p-1)p^{a-1}\}$. Then $\{1\} \cup \{\zeta^j : j \in A_1 \cup B_1\}$ is linearly independent and (47) implies $c + d \equiv 0 \pmod 2$ and $A_1 = B_1$. As we also have $A_2 = B_2$, we conclude $v = c + U$ and $w = d + U$ where $U = \sum_{j\in A} \zeta^j$. Hence

$$c^2 + c(U + \bar{U}) + |U|^2 = |v|^2 = |w|^2 = d^2 + d(U + \bar{U}) + |U|^2.$$

This implies $c = d$ or $c + d = -U - \bar{U}$. If $c = d$, then $v = w$ and we are done. Suppose $c + d = -U - \bar{U}$, that is,

$$\sum_{j\in A_1} (\zeta^j + \zeta^{-j}) + \sum_{j\in A_2} (\zeta^j + \zeta^{-j}) = -c - d. \tag{49}$$

Note that the first sum in (49) is in $\mathbb{Q}(\zeta_p)$ and every root of unity occurring in the second sum has the form $\zeta^{i+kp^{a-1}}$ with $1 \leq i \leq p^{a-1}-1$ and $k \in \mathbb{Z}$. As $\{\zeta^i : 0 \leq i \leq p^{a-1}-1\}$ is linearly independent over $\mathbb{Q}(\zeta_p)$, we infer from (49) that $\sum_{j\in A_1}(\zeta^j + \zeta^{-j}) = -c-d$ (and the second sum in (49) vanishes). Hence $M = \{1\} \cup \{\zeta^j : j \in A_1\} \cup \{\zeta^{-j} : j \in A_1\}$ is linearly dependent. Thus M contains a coset of $\langle \zeta_p \rangle$ by Proposition 13 (b). As $|A_1| \leq (p-1)/2$, this implies $\{\zeta^j : j \in A_1\} \cup \{\zeta^{-j} : j \in A_1\} = \{\zeta_p, \dots, \zeta_p^{p-1}\}$ and thus $-c-d = \sum_{i=1}^{p-1} \zeta_p = -1$. This contradicts the fact that $c+d$ is even.

Now suppose $A_1 \cup B_1 = \{p^{a-1}, \dots, (p-1)p^{a-1}\}$. Then $|A_1| = |B_1| = (p-1)/2$ and $\sum_{j\in A_1} \zeta^j + \sum_{j \in B_1} \zeta^j = -1$. Recall that $A_2 = B_2$. We conclude $v = c + V + W$ and $w = d - 1 - V + W$, where $V = \sum_{j\in A_1} \zeta^j$ and $W = \sum_{j \in A_2} \zeta^j$. Note that if we write $c + V = \sum_{i=0}^{p-1} r_i \zeta_p^i$ with $r_i \in \mathbb{Z}$, then $r_i = 1$ for $|A_1| = (p-1)/2$ indices i and $r_i = 0$ for $(p-1)/2$ indices i, as well as $r_0 = c$. Thus, using (6), we find

$$\begin{aligned}\mathcal{M}(c+V) &= \frac{1}{p-1}\left(\frac{p-1}{2}(c-0)^2 + \frac{p-1}{2}(c-1)^2 + \left(\frac{p-1}{2}\right)^2 (1-0)^2\right) \\ &= \frac{1}{2}\left(c^2 + (c-1)^2 + \frac{p-1}{2}\right).\end{aligned}$$

Combining this with (7), we get

$$\begin{aligned}(p-1)\mathcal{M}(v) &= (p-1)(\mathcal{M}(c+V) + \mathcal{M}(W)) \\ &= \frac{p-1}{2}\left(c^2 + (c-1)^2 + \frac{p-1}{2}\right) + (p-1)\mathcal{M}(W).\end{aligned} \tag{50}$$

Similarly,

$$(p-1)\mathcal{M}(w) = \frac{p-1}{2}\left(d^2 + (d-1)^2 + \frac{p-1}{2}\right) + (p-1)\mathcal{M}(W). \tag{51}$$

As $\mathcal{M}(v) = \mathcal{M}(w) = 2^m$, we infer $c^2 + (c-1)^2 = d^2 + (d-1)^2$ from (50) and (51). This implies $c = d$ or $d = -c + 1$. If $c = d$, then $v + w = (c + V + W) + (d - 1 - V + W) = 2c - 1 + 2W \not\equiv 0 \pmod 2$, which contradicts (44). Hence $d = -c + 1$ and thus $w = d - 1 - V + W = -c - V + W$. Set $X = c + V$. Note that $X \neq 0$, since $|A_1| = (p-1)/2$. Moreover, $v = X + W$ and $w = -X + W$. We have

$$|X|^2 + |W|^2 + X\bar{W} + \bar{X}W = |v|^2 = |w|^2 = |X|^2 + |W|^2 - X\bar{W} - \bar{X}W.$$

This implies $X\bar{W} + \bar{X}W = 0$ and thus $\bar{W} = -(\bar{X}/X)W$. We conclude

$$2^m = |v|^2 = X\bar{X} + W\bar{W} = X\bar{X} - \frac{\bar{X}}{X}W^2. \tag{52}$$

Note that $X \in \mathbb{Q}(\zeta_p)$. Hence (52) shows that the degree of the extension $\mathbb{Q}(\zeta_p)(W)/\mathbb{Q}(\zeta_p)$ divides 2. But the degree of $\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta_p)$ is p^{a-1} and p is odd. As $W \in \mathbb{Q}(\zeta)$, we conclude $W \in \mathbb{Q}(\zeta_p)$. As W only involves roots of unity of the form ζ^i with $i \not\equiv 0 \pmod{p^{a-1}}$, the usual linear independence argument shows that $W = 0$. Hence $w = -X + W = -X = -X - W = -v$ and this completes the proof. □

For $m \leq 5$, the following provides lists of those primes that survive Corollaries 24 and 41, but are excluded by Corollary 33, Theorem 39 and Lemma 42.

Corollary 43. *Assume the existence of a GBF from $\mathbb{Z}_{2p^a}^m$ to $\mathbb{Z}_{2p^a}$. Then we have the following.*

- *(a) If $m = 1$, then $p \neq 7$,*
- *(b) If $m = 3$, then $p \notin \{23, 31, 73\}$,*
- *(c) If $m = 5$, then $p \notin \{127, 151\}$.*

Proof. Suppose $m = 1$ and $p = 7$. Let $v \in W$. Then v is equivalent to $X := \zeta_7 + \zeta_7^2 + \zeta_7^4$ by Corollary 33. Hence $v = \pm\zeta_7^i X^\tau$ for some integer i and $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$. Let t be an integer with $\zeta_7^\tau = \zeta_7^t$ and let $\langle g \rangle$ be a cyclic group of order 7. We have $v = \pm\zeta_7^i(\zeta_7^t + \zeta_7^{2t} + \zeta_7^{4t})$ and thus $Z = \pm g^i(g^t + g^{2t} + g^{4t})$ is an alias of v. It is straightforward to check that Z is minimal and has the form (41). Hence, by Lemma 42, condition (35) is satisfied. Thus there is no GBF from $\mathbb{Z}_{2\cdot 7^a}$ to $\mathbb{Z}_{2\cdot 7^a}$ by Theorem 39. The proofs for the other cases are similar. □

Lemma 44. *If $m \geq 7$, $p > 2^{2m}/9$, and $f > (2^m + 3)/5$, then condition* (35) *is satisfied.*

Proof. Let G be a cyclic group of order p^a and let $w \in W$. We will show that w has a minimal alias of the form (41). By Theorem 22 (e), multiplying w with a root of unity, if necessary, we can assume that there is a minimal alias Z of w with $Z^{(2)} = Z$ such that $Z = c_0 + \sum_{i=1}^{u} c_i\Gamma_i$ for some nonnegative integer u, where $c_0, \dots, c_u \in \mathbb{Z}$, $c_i \neq 0$ for $i > 0$, and the Γ_i's are distinct orbits of $g \mapsto g^2$ on $G \setminus \{1\}$. Replacing w by $-w$, if necessary, we can assume $c_0 \geq 0$. Moreover, $|\Gamma_i| = f$ for all i. By Lemma 30, we have $ZZ^{(-1)} = 2^m + \lambda P$ with $\lambda \in \mathbb{Z}$, where P is the subgroup of G of order p. Moreover, we have $\lambda \in \{1, 4, 7, 16\}$ by Lemma 32. Recall that $S = 2^m + \lambda$ by Corollary 28 and $S^2 \geq 2^m + \lambda p$ for $\lambda > 0$ by Lemma 29. Hence, if $\lambda = 16$, then

$$p \leq 2^{-4}(S^2 - 2^m) = 2^{2m-4} + 2^{m+1} + 16 - 2^{m-4} < 2^{2m}/9,$$

as $m \geq 7$. This contradicts our assumptions. Thus $\lambda \in \{1, 4, 7\}$. Recall that

$$c_0^2 + f\sum_{i=1}^{u} c_i^2 = 2^m + \lambda \text{ and } \left(c_0 + f\sum_{i=1}^{u} c_i\right)^2 = 2^m + \lambda p \tag{53}$$

by Lemma 31 (e) and that f is odd.

We now show that

$$c_i = 1 \text{ for } i = 1, \dots, u \text{ or } c_i = -1 \text{ for } i = 1, \dots, u. \tag{54}$$

Suppose that (54) does not hold. Write $\alpha = \sum_{i=1}^{u} c_i^2$ and $\beta = \sum_{i=1}^{u} c_i$. The assumption that (54) does not hold implies $\alpha \geq 2$ and that there is an i with $|c_i| \geq 2$ or there are i, j with $c_i c_j < 0$. Thus, in any case, we have $\alpha \geq \beta + 2$. Recall that $5f > 2^m + 3$ by assumption. As $5f$ is odd and divisible by 5, this implies $5f \geq 2^m + 7$. Together with (53) we get

$$2^m + 7 \leq 5f = \frac{5(2^m + \lambda - c_0^2)}{\alpha}. \tag{55}$$

Note that

$$2^m + \lambda p \leq (2^m + \lambda)^2 \tag{56}$$

by (28). We have

$$\sum_{i=1}^{u} c_i^2 \leq \frac{2^m + \lambda}{f} < \frac{5(2^m + 7)}{2^m + 3}, \tag{57}$$

as $f > (2^m + 3)/5$ by assumption. This implies $\sum_{i=1}^{u} c_i^2 \leq 5$.

Case 1. $\alpha = 5$. Then $\lambda = 7$, $5f = 2^m + 7$, and $c_0 = 0$ by (55). Using (53) and $\beta \leq \alpha - 2$, we get

$$2^m + 7p = (f\beta)^2 \leq \frac{(2^m+7)^2(\alpha-2)^2}{25} = \frac{9(2^m+7)^2}{25}.$$

Therefore,

$$p < \frac{9}{25}\left(\frac{2^{2m}}{7} + 2^{m+1} + 7\right) < \frac{2^{2m}}{9}.$$

This contradicts our assumptions.

Case 2. $\alpha = 4$. Then $c_0^2 + 4f = 2^m + \lambda$ (53) and thus $\lambda \equiv c_0^2 + 4 \pmod 8$, as f is odd. This implies $\lambda \neq 1, 7$ and thus $\lambda = 4$ and c_0 is even. Note that $\beta \leq \alpha - 2 \leq 2$ and recall that $c_0 \geq 0$. Moreover, $c_0 \leq c_0^2/2$, as c_0 is even. Using a similar calculation as in Case 1, we get

$$2^m + 4p = (c_0 + \beta f)^2 \leq (c_0 + 2f)^2 \leq \left(\frac{c_0^2 + 4f}{2}\right)^2 = \frac{(2^m+4)^2}{4}$$

and thus $p < 2^{2m}/9$, contradicting our assumptions.

Case 3. $\alpha = 3$. Then $c_0^2 + 3f = 2^m + \lambda$. As $\lambda \in \{1, 4, 7\}$ and m is odd, this implies $c_0 \equiv 0 \pmod 3$ and thus $c_0 \leq c_0^2/3$. Using $\beta \leq \alpha - 2 = 1$, we conclude

$$2^m + \lambda p = (c_0 + \beta f)^2 \leq (c_0 + f)^2 \leq \left(\frac{c_0^2 + 3f}{3}\right)^2 = \frac{(2^m+\lambda)^2}{9}.$$

As $\lambda \geq 1$, we conclude

$$p \leq \frac{1}{9\lambda}\left(2^{2m} + 2^{m+1}\lambda + \lambda^2 - 9 \cdot 2^m\right) < \frac{2^{2m}}{9},$$

contradicting our assumptions.

Case 4. $\alpha = 2$. In this case, $\beta = 0$. Using (53), we get $2^m + \lambda p = (c_0 + \beta)^2 = c_0^2 \leq 2^m + \lambda$. This is impossible.

We have thus shown that (54) holds. Hence $Z = c_0 + \gamma \sum_{i=1}^{u} \Gamma_i$ with $\gamma = \pm 1$. This shows that w indeed has a minimal alias for the form (41). Moreover, $p > 2^{2m}/9 > 2^{m+2}$ by assumption. Hence condition (35) is satisfied by Lemma 42. □

The following provides lists primes that survive all previous necessary conditions, but are ruled out by Theorem 39 and Lemma 44.

Corollary 45. *Assume the existence of a GBF from* $\mathbb{Z}_{2p^a}^m$ *to* $\mathbb{Z}_{2p^a}$*. If* $m = 7$*, then* $p \notin \{2089, 2143, 2351, 3191, 4513, 6361, 8191, 9719, 11119, 13367\}$*.*

Finally, we summarize or results on GBFs from $\mathbb{Z}_{2p^a}^m$ to $\mathbb{Z}_{2p^a}$.

Theorem 46. *Let* p *be an odd prime, let* a, m *be positive integers, and suppose that* m *is odd. If a GBF from* $\mathbb{Z}_{2p^a}^m$ *to* $\mathbb{Z}_{2p^a}$ *exists, then the following hold.*

- $m \geq 3$*.*
- $p \leq 2^{2m} + 2^m + 1$*.*
- $\text{ord}_p(2)$ *is even and* $\text{ord}_p(2) \leq 2^{m-1}$*.*
- *If* $m \geq 7$*, then* $p \leq 2^{2m}/9$ *or* $\text{ord}_p(2) \leq (2^m + 3)/5$*.*
- *If* $m = 3$*, then* $p = 7$*.*
- *If* $m = 5$*, then* $p \in \{7, 23, 31, 73, 89\}$*.*
- *If* $m = 7$*, then*
  $p \in \{7, 23, 31, 47, 71, 73, 79, 89, 103, 223, 233, 337, 431, 601, 631, 881, 1103, 1801\}$*.*

Proof. This follows from Lemmas 38, 40, 44, Theorem 39, and Corollaries 25, 37, 43, 41, and 45. □

Acknowledgement We thank the anonymous referees for their extremely careful reading of the manuscript, which helped to considerably improve the exposition of the paper.

References

[1] L. D. Baumert: *Cyclic Difference Sets.* Springer 1971.

[2] T. Beth, D. Jungnickel, H. Lenz: *Design Theory* (2nd edition). Cambridge University Press 1999.

[3] C. Blondeau, K. Nyberg: Perfect nonlinear functions and cryptography. *Finite Fields Appl.* **32** (2015), 120-147.

[4] Z. I. Borevich, I. R. Shafarevich: *Number Theory.* Academic Press 1966.

[5] J. W. S. Cassels: On a conjecture of R. M. Robinson about sums of roots of unity. *J. Reine Angew. Math.* **238** (1969) 112–131.

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

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

[8] C. F. Gauß: *Disquisitiones Arithmeticae* (English Translation). Yale University Press 1965.

[9] Y. Jiang, Y. Deng: New results on nonexistence of generalized bent functions. *Des. Codes Cryptogr.* **75** (2015), 375–385.

[10] K. Ireland, M. I. Rosen: *A Classical Introduction to Modern Number Theory, 2nd edition.* Springer 1990.

[11] P. V. Kumar, R. A. Scholtz, L. R. Welch: Generalized bent functions and their properties. *J. Combin. Theory Ser. A* **40** (1985), 90–107.

[12] P. H. J. Lampio, P. Östergard, F. Szöllösi: Orderly generation of Butson Hadamard matrices. `arXiv:1707.02287v1` (2017).

[13] K. H. Leung, B. Schmidt: The Field Descent Method. *Des. Codes Cryptogr.* **36** (2005), 171–188.

[14] K. H. Leung, B. Schmidt: The anti-field-descent method. *J. Combin. Theory Ser. A* **139** (2016), 87–131.

[15] H. Liu, K. Feng, R. Feng: Nonexistence of generalized bent functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_m$. *Des. Codes Cryptogr.* **82** (2017), 647–662.

[16] D. A. Marcus: *Number fields.* Springer 1995.

[17] D. K. Nguyen, B. Schmidt: Fast Computation of Gauss Sums and Resolution of the Root of Unity Ambiguity. *Acta Arith.* **140** (2009), 205–232.

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

[19] O. S. Rothaus: On Bent Functions. Institute of Defense Analysis, USA, W. P. 169 (1966).

[20] O. S. Rothaus: On 'bent' functions. *J. Combin. Theory Ser. A* **20** (1976), 300–305.

[21] B. Schmidt: Cyclotomic Integers and Finite Geometry. *J. Amer. Math. Soc.* **12** (1999), 929–952.

[22] B. Schmidt: *Characters and Cyclotomic Fields in Finite Geometry.* Lecture Notes in Mathematics **1797**, Springer 2002.

[23] K.-U. Schmidt: Quaternary constant-amplitude codes for multicode CDMA. *IEEE Trans. Inf. Theory* **55** (2009), 1824–1832.

[24] K.-U. Schmidt: $\mathbb{Z}_4$-valued quadratic forms and quaternary sequence families. *IEEE Trans. Inf. Theory* **55** (2009) 5803–5810.

[25] N. N. Tokareva: Generalizations of bent functions: a survey. *J. Appl. Ind. Math.* **5** (2011), 110–129