On the nonexistence of semi-regular relative difference sets

Ka Hin Leung[a] [*], Bernhard Schmidt[b] [†], and Tao Zhang[c,‡]

[a] Department of Mathematics, National University of Singapore, Kent Ridge, Singapore 119260, Republic of Singapore.

[b] Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637371, Republic of Singapore.

[c] Zhejiang Lab, Hangzhou 311100, China.

Abstract

In this paper, we study semi-regular relative difference sets. We give some nonexistence results on abelian (mn, n, mn, m) relative difference sets. In particular, we focus on the case when m is prime and show that, for any fixed integer $n \geq 2$, there are at most finitely many primes p for which an abelian (pn, n, pn, p) relative difference set may exist. We illustrate our results by investigating the existence of (mn, n, mn, m) relative difference sets with $m \in \{2, 3, 4\}$ in detail.

Keywords: Semi-regular relative difference set; Weil number; group ring.

AMS subject classifications: 05B10.

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

[†]This research is supported by the Ministry of Education, Singapore, under its Academic Research Fund Tier 1 (RG27/18)

[‡]Research is supported by the National Natural Science Foundation of China under Grant No. 11801109.

1 Introduction

Let G be a group of order un and N be a subgroup of G of order n. A k-subset D of G is called an (u, n, k, λ) relative difference set (RDS) in G with respect to N if the expressions $d_1 d_2^{-1}$ with $d_1, d_2 \in D$, $d_1 \neq d_2$, represent each element of $G \backslash N$ exactly λ times and represent no element of N. If the group G is abelian, then D is called abelian RDS. If $k = u$, then D is called semi-regular RDS.

In this paper, we focus on semi-regular RDS. Semi-regular RDSs not only have their own interest, but also have applications in mutually unbiased bases [7]. There have been a number of papers devoted to the research on (p^a, p^b, p^a, p^{a-b}) RDSs (see [15, 17] and the references therein). A construction of $(p^{2t}(p+1), p+1, p^{2t}(p+1), p^{2t})$ RDSs can be found in [3, 9], where t is a positive integer and $p = 2$ or p is a Mersenne prime. Feng [5] gave a construction of $(p(p+1), p, p(p+1), p+1)$ RDSs, where p is a Mersenne prime. Constructions of non-abelian RDSs with parameters $(4q, q, 4q, 4)$ and $(16q, q, 16q, 16)$ can be found in [6, 20], where q is a sufficient large prime power with $q \equiv 1 \pmod 4$. For the nonexistence results, Ma [14] showed that there does not exist abelian (pq, q, pq, p) RDSs with p, q being two distinct odd primes such that $p > q$. In [10], Leung, Ma and Tan showed that there is no abelian $(3pq, 3, 3pq, pq)$ RDS with p, q being two distinct primes larger than 3. Feng and Xiang [6] proved that if $a = 1$ or 2 and p is an odd prime, then there does not exist an abelian $(2^a p, p, 2^a p, 2^a)$ RDS except $a = 2$ and $p = 3$. In [8], Hiramine proved that if an abelian $(2n, n, 2n, 2)$ RDS exists, then n is a power of 2 except for a few cases. Some nonexistence results on (mn, n, mn, m) RDS with $\gcd(m, n) = 1$ can be found in [5, 20].

The primary aim of this paper is to continue this investigation and provide new nonexistence results for semi-regular RDSs. Some of our results still rely on the "traditional" self-conjugacy approach, but the most significant parts of our paper concern cases without the self-conjugacy condition. This in fact extends the pioneering work of Ma [14] who developed powerful tools that do not require the self-conjugacy assumption. In this vein, we combine a new "trick" to deal with Weil numbers corresponding to characters of different orders with a result on unique differences modulo p to prove that, for any fixed integer $n \geq 2$, there are at most finitely many primes p for which an abelian (pn, n, pn, p) relative difference set may exist.

2 Preliminaries

To study a relative difference sets in a group G, it is convenient to use group ring notations. Let $\mathbb{Z}[G]$ denote the group ring of G over $\mathbb{Z}$. For any $A \in \mathbb{Z}[G]$, A can be written as $A = \sum_{g\in G} a_g g$, where $a_g \in \mathbb{Z}$. We identify a subset S of G with the group ring element $\sum_{g\in S} g$. Given any $A = \sum_{g\in G} a_g g \in \mathbb{Z}[G]$, we define $A^{(t)} = \sum_{g\in G} a_g g^t$. We also define $\mathrm{supp}(A) = \{g \in G : a_g \neq 0\}$.

It is well known that a subset D in G is an (mn, n, mn, m) RDS with forbidden group N if and only if

$$DD^{(-1)} = mn1_G + m(G - N), \tag{1}$$

where 1_G is the identity of group G. Moreover, if D is an (mn, n, mn, m) RDS in G with forbidden group N, then D contains exactly one element of each coset of N in G.

Lemma 2.1. [16, Theorem 4.1.1] *Let R be an abelian $(m, n, m, m/n)$ RDS in G relative to N. Then $\exp(G)|m$ or $G = \mathbb{Z}_4$, $n = 2$.*

Lemma 2.2. [4] *Let R be an (m, n, k, λ) RDS in G relative to N. If U is a normal subgroup of G contained in N, and if ρ denotes the canonical epimorphism $G \to G/U$, then $\rho(R)$ is an $(m, n/u, k, \lambda u)$ RDS in G/U relative to N/U.*

The standard tool to investigate if possible solutions exist for (1) is to apply character theory. We denote the group of all characters of G by G^*. For any $A = \sum_{g\in G} d_g g$ and $\chi \in G^*$, define $\chi(A) = \sum_{g\in G} d_g \chi(g)$. The following *inversion formula* shows that A is completely determined by its character value $\chi(A)$, where χ ranges over G^*.

Lemma 2.3 (Fourier inversion formula)**.** *Let G be an abelian group. If $A = \sum_{g\in G} a_g g \in \mathbb{Z}[G]$, then*

$$a_g = \frac{1}{|G|} \sum_{\chi\in G^*} \chi(A)\chi(g^{-1}),$$

for all $g \in G$.

For any subgroup U of G, we set

$$U^\perp = \{\chi \in G^* : \chi(g) = 1,\ \forall g \in U\}.$$

Using Fourier inversion formula, it is easy to conclude the following:

Lemma 2.4. *Let D be a subset of G. D is an (mn, n, mn, m) RDS with forbidden group N in G if and only if for any character $\chi \in G^*$,*

$$|\chi(D)|^2 = \begin{cases} m^2n^2, & \text{if } \chi \text{ is principal;} \\ 0, & \text{if } \chi \text{ is nonprincipal and } \chi \in N^\perp; \\ mn, & \text{if } \chi \text{ is nonprincipal and } \chi \notin N^\perp. \end{cases}$$

Suppose $G = U \times K$. Then for any $A = \sum_{g \in G} a_g g$, we may write $A = \sum_{g \in K} D_g g$ where $D_g \in \mathbb{Z}[U]$. Often, we are interested in finding the value of $\chi(D_g)$ for any character $\chi \in G^*$.

Lemma 2.5. *Let G be an abelian group and let $E = \sum_{g \in G} a_g g \in \mathbb{Z}[G]$. For every subgroup U of G and every $\chi \in G^*$, we have*

$$\sum_{\tau \in U^\perp} \chi\tau(E) = |U^\perp| \chi \left(\sum_{g \in U} a_g g \right).$$

Proof. Using the orthogonality relations, we compute

$$\begin{aligned} \sum_{\tau \in U^\perp} \chi\tau(E) &= \sum_{\tau \in U^\perp} \chi\tau(\sum_{g \in G} a_g g) \\ &= \sum_{\tau \in U^\perp} \sum_{g \in G} a_g \chi\tau(g) \\ &= \sum_{g \in G} a_g \chi(g) \sum_{\tau \in U^\perp} \tau(g) \\ &= |U^\perp| \sum_{g \in U} a_g \chi(g) \\ &= |U^\perp| \chi(\sum_{g \in U} a_g g). \end{aligned}$$

This proves the lemma. □

From now on, we assume ζ_m is a primitive m-th root of unity.

Corollary 2.6. *Let $G = U \times K$ be an abelian group of exponent e and suppose that $D \in \mathbb{Z}[G]$ satisfies $\psi(D) \equiv 0 \pmod{B}$ for all $\psi \in G^*$ for some $B \in \mathbb{Z}[\zeta_e]$ coprime to $|K|$. Write $D = \sum_{g \in K} D_g g$ with $D_g \in \mathbb{Z}[U]$. Then $\chi(D_g) \equiv 0 \pmod{B}$ for all $g \in K$ and $\chi \in G^*$.*

Proof. Let $g \in K$, write $E = Dg^{-1} = \sum_{h \in G} a_h h$ with $a_h \in \mathbb{Z}$, and let χ be any character of G. Comparing the coefficients of elements of K on both sides of $Eg = D$, we see that $\sum_{h \in U} a_h h = D_g$. Note that $|U^\perp| = |K|$. Hence

$$|K|\chi(D_g) = |U^\perp|\chi\left(\sum_{h \in U} a_h h\right) = \sum_{\tau \in U^\perp} \chi\tau(E) \tag{2}$$

by Lemma 2.5. Note that $\chi\tau(E) = \chi\tau(D)\chi\tau(g^{-1}) \equiv 0 \pmod{B}$ by assumption. Hence $|K|\chi(D_g) \equiv 0 \pmod{B}$ by (2). As $|K|$ and B are coprime, this implies $\chi(D_g) \equiv 0 \pmod{B}$. □

3 Number Theoretic Background

By Lemma 2.4, we are led to study the equation $|X|^2 = n$ in $\mathbb{Z}[\zeta_u]$ for integers n and u, the solution X is called a *Weil number*. There are basically two directions to prove non-existence results. One direction is to find conditions on n and u such that no solution exists. If there are indeed solutions, we find all of them and try to show that the structure of the solutions does not meet the requirements for such difference sets.

Generally, it is quite difficult to find all the solutions for $|X|^2 = n$ in $\mathbb{Z}[\zeta_u]$. We say that $A, B \in \mathbb{Z}[\zeta_u]$ are *equivalent* if $B = \pm\zeta_u^i \tau(A)$ for some integer i and some $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_u)/Q)$. For $n = 2$, we have the following:

Lemma 3.1. [2, Lemma 6] *Let u be a positive integer and $X \in \mathbb{Z}[\zeta_u]$ with $|X|^2 = 2$. Then X is equivalent to $1 + \zeta_4$, $1 + \zeta_7 + \zeta_7^3$, or $1 + \zeta_{15}^6 - \zeta_{15}^8$.*

In [11] and [12], we obtained some interesting results when u is a prime power. We record some of them that we will apply in later sections.

Lemma 3.2. [11, Theorem 4.7] *Let p be an odd prime and let a, w be positive integers with $\gcd(w, p) = 1$. Suppose that $X \in \mathbb{Z}[\zeta_{p^a}]$ satisfies $|X|^2 = w^2$. Write $w = w_0 w_1$ such that $ord_p(q) \equiv 0 \pmod{2}$ for all prime divisors q of w_0 and $ord_p(q) \equiv 1 \pmod{2}$ for all prime divisors q of w_1. If $w_1 = 1$ or $w_1 > 1$ and $\gcd(ord_p(q_1), \ldots, ord_p(q_k)) > 2w_1 - 1$, where $q_1, \ldots, q_k$ are the distinct prime divisors of w_1, then $X = \eta w$ for some root of unity η.*

The following two lemmas follow from [12, Theorems 22 and 23].

Lemma 3.3. *Let p be an odd prime and n be a nonsquare integer not divisible by p. Let $q_1, \ldots, q_s$ be the distinct prime divisors of n. Write $f = \gcd\{ord_p(q_1), \ldots, ord_p(q_s)\}$. Assume that there is $X \in \mathbb{Z}[\zeta_{p^a}]$ with $|X|^2 = n$. Then f is odd and $p \leq n^2 + n + 1$.*

Lemma 3.4. *Let a be a positive integer. Let p, q be primes satisfying $ord_p(q) \geq 2q$. Then there is no solution for $|X|^2 = q$, $X \in \mathbb{Z}[\zeta_{p^a}]$.*

Definition 3.5. *Let p be an odd prime. We define*

$$\Theta_p := \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) \zeta_p^x$$

where $(\frac{x}{p})$ is the Legendre symbol. For convenience, we set $\Theta_2 = 1 + \zeta_4$.

Note that Θ_p a Gauss sum. We record a known result concerning Θ_p.

Lemma 3.6. [12, Corollary 8] *Suppose $X \in \mathbb{Z}[\zeta_{p^a}]$ satisfies $|X|^2 = p^{2r+i}n$ where $n \in \mathbb{N}$, $r \in \mathbb{N} \cup \{0\}$ and $i \in \{0, 1\}$. Then $X = p^r \Theta_p^i A$ for some $A \in \mathbb{Z}[\zeta_{p^a}]$ with $|A|^2 = n$.*

Next, we deal with the case where u not necessarily is a prime power. For our application, we record a simplified version of [18, Theorem 2.2.2].

Lemma 3.7. *Let p, q be distinct primes and $u = pq^r$ where r is a positive integer. Suppose $X \in \mathbb{Z}[\zeta_u]$ is a solution of $X\overline{X} = q^a$ with $a \geq 1$. If $p \nmid q - 1$, then there is an integer j such that*

$$X\zeta_u^j \in \mathbb{Z}[\zeta_p] \text{ or } X = \zeta_u^j \Theta_q Y,$$

where $Y \in \mathbb{Z}[\zeta_p]$ with $|Y|^2 = q^{a-1}$.

For more general situations, we need the so-called self-conjugacy assumption to determine the solution of $|X|^2 = n$.

Definition 3.8. *Let $u = p^a u'$ with $\gcd(p, u') = 1$ where p is a prime and u' is a positive integer. Then p is called self-conjugate modulo u if there exists an integer j such that $p^j \equiv -1 \pmod{u'}$. A composite integer n is called self-conjugate modulo u if every prime divisor of n is self-conjugate modulo u.*

The self-conjugacy assumption imposes a strong necessary condition on the solution of equation $|X|^2 = n$ in $\mathbb{Z}[\zeta_u]$.

Proposition 3.9. *Suppose that $A \in \mathbb{Z}[\zeta_u]$ satisfies $|A|^2 = n$ and let w be a divisor of n that is self-conjugate modulo u. Write $w = w_1^2 w_2$ where $w_2 = \prod_{i=1}^{k} p_i$ is the square-free part of w and the p_i's are distinct primes ($k = 0$, i.e., $w_2 = 1$ is allowed) that divides w_2. Then*

$$A \equiv 0 \pmod{w_1 \prod_{i=1}^{k} \Theta_{p_i}}.$$

Proof. Write $B = w_1 \prod_{i=1}^{k} \Theta_{p_i}$, where $\Theta_{p_i}\overline{\Theta_{p_i}} = p_i$. Note that $|B|^2 = w_1^2 \prod_{i=1}^{k} p_i = w$. Let $\mathfrak{p}$ be any prime ideal of $\mathbb{Z}[\zeta_u]$ above w and, for $X \in \mathbb{Z}[\zeta_u]$, let $\nu_{\mathfrak{p}}(X)$ be the largest nonnegative integer such that $X \in \mathfrak{p}^{\nu_{\mathfrak{p}}(X)}$. Note that $\mathfrak{p}$ is invariant under complex conjugation, since w is self-conjugate modulo u. Hence $|A|^2 = n \equiv 0 \pmod{w}$ and $|B|^2 = w$ imply $\nu_{\mathfrak{p}}(A) \geq \nu_{\mathfrak{p}}(B)$. We conclude $A \equiv 0 \pmod{B}$. □

Corollary 3.10. *Let p be a prime and let n, u be a positive integers with $\gcd(u, p) = 1$. Suppose $A \in \mathbb{Z}[\zeta_u]$ and $|A|^2 = n$. If $p^t || n$ and p is self-conjugate modulo u, then t is even.*

Proof. Since p is self-conjugate modulo u, then $(p) = \mathfrak{p}_1 \cdots \mathfrak{p}_s$, where the $\mathfrak{p}_i$'s are distinct prime ideals of $\mathbb{Z}[\zeta_u]$ above p, and $\mathfrak{p}_i = \overline{\mathfrak{p}_i}$. By Proposition 3.9, the result follows. □

To end this section, we prove a technical lemma.

Lemma 3.11. *Let p be a prime and m a positive integer with $p \nmid m$. Let $X = \sum_{i=0}^{p-1} x_i \zeta_p^i$ and $Y = \sum_{i=0}^{p-1} x_i$ where $x_i \in \mathbb{Z}[\zeta_m]$. Suppose $p \nmid Y$, $|X|^2 = |Y|^2 = pw$ and $p \nmid w$. Then $p | X\bar{Y}$.*

Proof. Since $|Y|^2 = pw$ and $Y \in \mathbb{Z}[\zeta_m]$, Corolllary 3.10 implies that p is not self-conjugate modulo m. Hence the prime ideal factorization of $p\mathbb{Z}[\zeta_m]$ has the form

$$p\mathbb{Z}[\zeta_m] = \prod_{i=1}^{c/2} \mathfrak{P}_i \overline{\mathfrak{P}_i}, \tag{3}$$

where $c = \varphi(m)/\mathrm{ord}_m(p)$ and the $\mathfrak{P}_i$'s are pairwise distinct prime ideals of $\mathbb{Z}[\zeta_m]$. By (3), the prime ideal factorization of Y has the form

$$Y\mathbb{Z}[\zeta_m] = W\prod_{i=1}^{c/2}\mathfrak{P}_i^{\alpha_i}\overline{\mathfrak{P}_i}^{\beta_i}$$

where W is some product of prime ideals that contain w and α_i, β_i, are nonnegative integers. Since $|Y|^2 = pw$ with $p \nmid w$, we have $\alpha_i+\beta_i = 1$ for all i. Hence, interchanging $\mathfrak{P}_i$ with $\overline{\mathfrak{P}_i}$ if necessary, we have

$$Y\mathbb{Z}[\zeta_m] = W\prod_{i=1}^{c/2}\mathfrak{P}_i \tag{4}$$

where W is an ideal in $\mathbb{Z}[\zeta_m]$ relatively prime to $p\mathbb{Z}[\zeta_m]$. On the other hand,

$$p\mathbb{Z}[\zeta_{pm}] = \left(\prod_{i=1}^{c/2}\mathfrak{Q}_i\overline{\mathfrak{Q}_i}\right)^{p-1}, \tag{5}$$

where the $\mathfrak{Q}_i$'s are pairwise distinct prime ideals of $\mathbb{Z}[\zeta_{pm}]$, $\mathfrak{Q}_i^{p-1} = \mathfrak{P}_i\mathbb{Z}[\zeta_{pm}]$ for all i, and $\prod_{i=1}^{c/2}\mathfrak{Q}_i\overline{\mathfrak{Q}_i} = (1-\zeta_p)\mathbb{Z}[\zeta_{pm}]$.

By (5), the prime ideal factorization of X has the form

$$X\mathbb{Z}[\zeta_{pm}] = W'\prod_{i=1}^{c/2}\mathfrak{Q}_i^{\alpha_i}\overline{\mathfrak{Q}_i}^{(p-1)-\alpha_i} \text{ with } 0 \le \alpha_i \le (p-1),$$

and W' is a product of prime ideals that contain w. To show $p|X\bar{Y}$, it suffices to show $\alpha_i = p-1$ for all i.

Note that $X - Y = \sum_{i=1}^{p-1} x_i(1-\zeta_p^i)$. Hence, $X - Y \equiv 0 \bmod (1-\zeta_p)$. Since $1-\zeta_p \in \mathfrak{Q}_i^{\alpha_i} \cap \overline{\mathfrak{Q}_i}$ and $Y \in \mathfrak{P}_i \subset \mathfrak{Q}_i^{\alpha_i}$, it follows that $X \in \mathfrak{Q}_i^{\alpha_i}$. In particular, $\alpha_i \ge 1$. To show $\alpha_i = p-1$, it suffices to show that $X \notin \overline{\mathfrak{Q}_i}$. Otherwise, it follows that $Y \in \overline{\mathfrak{Q}_i}$ also. But then as $\overline{\mathfrak{P}_i} = \overline{\mathfrak{Q}_i} \cap \mathbb{Z}[\zeta_m]$, we have $Y \in \overline{\mathfrak{P}_i}$ also. This is impossible and thus $\alpha_i = p-1$. □

4 Results on the $\mathcal{M}$-Function

As demonstrated in [11], $\mathcal{M}$-function is a useful tool to study Weil numbers. We first recall the definition of $\mathcal{M}$-function.

Definition 4.1 ($\mathcal{M}$-function)**.** *For $X \in \mathbb{Z}[\zeta_u]$, let*

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

where φ denotes the Euler totient function.

Note that $\mathcal{M}(X) \geq 1$ for all nonzero $X \in \mathbb{Z}[\zeta_u]$ by the inequality of geometric and arithmetic means, since $\prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_u)/\mathbb{Q})} (X\overline{X})^\sigma \geq 1$. The following lemma is a consequence of [2, (3.4),(3.16)]. For the convenience of readers, we give a proof here.

Lemma 4.2. *Let $X \in \mathbb{Z}[\zeta_n]$, let q be a prime divisor of n, and write $n = q^b n'$ with $\gcd(q, n') = 1$. If $b = 1$, then $X = \sum_{i=0}^{q-1} X_i \zeta_q^i$ with $X_i \in \mathbb{Z}[\zeta_{n'}]$ and*

$$\mathcal{M}(X) = \frac{1}{q-1} \sum_{0 \leq i < j \leq q-1} \mathcal{M}(X_i - X_j). \tag{6}$$

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

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

Proof. Observe that

$$|X|^2 = \sum_{i=0}^{q^{b-1}-1} |X_i|^2 + \sum_{i=0}^{q^{b-1}-1} \sum_{0 \leq j \neq i \leq q^{b-1}-1} X_i \overline{X_j} \zeta_{q^b}^{i-j}.$$

Therefore,

$$\sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})} \sigma(|X|^2) = \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})} \sum_{i=0}^{q^{b-1}-1} \sigma(|X_i|^2) + Tr\Big(\sum_{0 \leq j \neq i \leq q^{b-1}-1} X_i \overline{X_j} \zeta_{q^b}^{i-j} \Big)$$

where $Tr : \mathbb{Q}(\zeta_n) \to \mathbb{Q}$ is the trace function.

For $b = 1$, we then have

$$\varphi(n)\mathcal{M}(X) = \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{n'})/\mathbb{Q})} [(q-1)\sigma(\sum_{i=0}^{q-1} |X_i|^2) + \sigma(\sum_{0 \leq j \neq i \leq q-1} X_i \overline{X_j})(-1)].$$

Note that $\sum_{j=1}^{q-1} \zeta_q^j = -1$. Hence,

$$\varphi(n)\mathcal{M}(X) = \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{n'})/\mathbb{Q})} \sum_{0 \leq i < j \leq q-1} \sigma(|X_i - X_j|^2) = \sum_{0 \leq i < j \leq q-1} \varphi(n')\mathcal{M}(X_i - X_j).$$

Since $\varphi(n) = (q-1)\varphi(n')$, (a) follows.

For $b \geq 2$, $q^2 | Ord(\zeta_{q^b}^{i-j})$ and thus for each summand z in $X_i\overline{X_j}\zeta_{q^b}^{i-j}$, $q^2 | Ord(z)$. Therefore, $Tr(z) = 0$ and

$$Tr(\sum_{0 \leq j \neq i \leq q-1} X_i\overline{X_j}\zeta_q^{i-j}) = 0.$$

On the other hand,

$$\sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})} \sum_{i=0}^{q^{b-1}-1} \sigma(|X_i|^2) = \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{qn'})/\mathbb{Q})} \sum_{i=0}^{q^{b-1}-1} q^{b-1}\sigma(|X_i|^2)$$

as each $X_i \in \mathbb{Q}(\zeta_{qn'})$. We thus get (b). □

The length of a cyclotomic integers was defined in [12]. Here, we generalize the definition. Recall that the $\mathrm{supp}(A)$ denotes the support of a group ring element A, as defined in Section 2.

Definition 4.3. *Let n, m be positive integers with $\gcd(m,n) = 1$. Let G be a cyclic group of order n, and let g be a fixed generator of G. For $Y = \sum_{i=0}^{n-1} a_i g^i \in \mathbb{Z}[\zeta_m][G]$, write $Y(\zeta_n) = \sum_{i=0}^{n-1} a_i \zeta_n^i$. We say that Y is m-**minimal** if*

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

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

It is straightforward to check that by using a similar argument as in the proof of [12, Lemma 20], with a_i^2 replaced by $\mathcal{M}(a_i)$, we obtain the following:

Lemma 4.4. *Let p be prime and $p \nmid m$. Suppose $X = \sum_{i=0}^{p-1} a_i \zeta_p^i$ with all a_i's are in $\mathbb{Z}[\zeta_m]$. Then*

$$\mathcal{M}(X) \geq \frac{1}{p-1}\left((p - \ell_m(X))\sum_{i=0}^{p-1}\mathcal{M}(a_i) + \ell_m(X)\max\{0, \ell_m(X) - \frac{p}{2}\}\right). \quad (8)$$

In particular,

$$\mathcal{M}(X) \geq \max\left\{\frac{p\ell_m(X)}{2(p-1)}, \frac{\ell_m(X)(p-\ell_m(X))}{p-1}\right\}. \quad (9)$$

Note that in the argument shown in [12, Lemma 20], we need to apply Lemma 4.2 and use the fact that $\mathcal{M}(a_i) \geq 1$ whenever $a_i \neq 0$. The following is a "field-descent" result based on the investigation of unique differences modulo p. In a group G, a subset A in G is said to have a unique difference if there exist $g, h \in A$ such that $gh^{-1} \neq xy^{-1}$ for any $x, y \in G$ with $(g, h) \neq (x, y)$. For the convenience of readers, we record the following result by Lev [13].

Result 4.5. *Let A be a subset of a finite abelian group G and let p be the smallest prime divisor of $|G|$. If $p > 2^{|A|-1}$, then A has a unique difference.*

Proposition 4.6. *Let $u = p^a u'$, where p is a prime, $a \geq 1$ and $\gcd(p, u') = 1$. Let n be any positive integer such that $p > \max\{4n^2, 2^{n-1}\}$. If $X \in \mathbb{Z}[\zeta_u]$ is a solution of $X\overline{X} = n$, then there is an integer j such that $X\zeta_{p^a}^j \in \mathbb{Z}[\zeta_{u'}]$.*

Proof. We first deal with the case $a \geq 2$. Write $X = \sum_{i=1}^{s} X_i \zeta_{p^a}^{a_i}$ where $0 \neq X_i \in \mathbb{Z}[\zeta_{pu'}]$ and $0 \leq a_1 < a_2 < \ldots < a_s \leq p^{a-1} - 1$.

By Lemma 4.2 (7),

$$n = \mathcal{M}(X) = \sum_{i=1}^{s} \mathcal{M}(X_i).$$

Since $\mathcal{M}(X_i) \geq 1$ if $X_i \neq 0$, we conclude that $s \leq n$. We claim that $\{a_1, \ldots, a_s\}$ does not have a unique difference modulo p^{a-1} if $s \geq 2$.

Consider the equation

$$XX^{(-1)} = \sum_{r=0}^{p^{a-1}-1} \sum_{a_i - a_j \equiv r \bmod p^{a-1}} X_i \overline{X_j} \zeta_{p^a}^{a_i - a_j - r} \zeta_{p^a}^r = n.$$

Note that $X_i \overline{X_j} \zeta_{p^a}^{a_i - a_j - r} \in \mathbb{Q}[\zeta_{pu'}]$ if $a_i - a_j \equiv r \bmod p^{a-1}$. As $\{1, \zeta_{p^a}, \ldots, \zeta_{p^a}^{p^{a-1}-1}\}$ is linearly independent over $\mathbb{Q}[\zeta_{pu'}]$, we see that

$$\sum_{a_i - a_j \equiv r \bmod p^{a-1}} X_i \overline{X_j} \zeta_{p^a}^{a_i - a_j - r} = 0.$$

As all X_i's are nonzero, the sum above either consists of no terms or at least two summands. Therefore, by viewing $\{a_1 \ldots, a_s\} \subset \mathbb{Z}_{p^{a-1}}$, we see that $\{a_1 \ldots, a_s\}$ does not have unique difference. By Result 4.5, this is impossible if $s \geq 2$ as $p > 2^{n-1}$. Therefore, $s = 1$ and we may assume $X \in \mathbb{Z}[\zeta_{pu'}]$.

As before, we write $X = \sum_{i=1}^{s} X_i \zeta_p^{a_i}$ where $0 \neq X_i \in \mathbb{Z}[\zeta_{u'}]$ and $0 \leq a_1 < a_2 < \ldots < a_s \leq p-1$. We claim that $s = \ell_{u'}(X) \leq n$.

In view of Lemma 4.4, we conclude that

$$2n = 2\mathcal{M}(X) > \mathcal{M}(X)\frac{2p-2}{p} \geq s.$$

Hence $s \leq 2n-1$. Observe that $2n-1 \leq (p-1)/2$ as $p > n^2+n+1$. Thus the product $s(p-s)$ is increasing when s varies from 1 to $2n-1$. However, if $s \geq n+1$, then by Lemma 4.4,

$$\mathcal{M}(X) \geq \frac{s(p-s)}{p-1} \geq \frac{(n+1)(p-(n+1))}{p-1} \geq n + \frac{n+p-(n+1)^2}{p-1} > n.$$

It follows that $s \leq n$. Write

$$n = XX^{(-1)} = \sum_{r=0}^{p-1} \sum_{a_i - a_j \equiv r \bmod p} X_i \overline{X_j} \zeta_p^r.$$

Since $p > n^2+n+1 > s^2$, there exists $0 < t \leq p-1$ such that $t \neq a_i - a_j$ for any $1 \leq i, j \leq s$. In particular,

$$\sum_{a_i - a_j \equiv t \bmod p} X_i \overline{X_j} \zeta_p^t = 0.$$

As $\{1, \zeta_p, \ldots, \zeta_p^{p-1}\} \backslash \{\zeta_p^t\}$ is linearly independent over $\mathbb{Q}[\zeta_{u'}]$, it then follows for $1 \leq r \leq p-1$,

$$\sum_{a_i - a_j \equiv r \bmod p} X_i \overline{X_j} \zeta_p^r = 0.$$

Using a similar argument as before, we see that $\{a_1, \ldots, a_s\} \subset \mathbb{Z}_p$ does not have a unique difference if $s > 1$, which again is impossible. Hence $s = 1$ and $X = \zeta_p X'$ for some $X' \in \mathbb{Z}[\zeta_{u'}]$. □

Lemma 4.7. *Let u be a positive integer and $X, Y \in \mathbb{Z}[\zeta_u]$.*

(a) We have

$$\mathcal{M}(X+Y)^{1/2} \leq \mathcal{M}(X)^{1/2} + \mathcal{M}(Y)^{1/2}. \tag{10}$$

Moreover, equality holds in (10) *if and only if $Y = \alpha X$ for some $\alpha \in \mathbb{Q}$.*

(b) If $X \neq 0$ and $X \equiv 0 \pmod{m}$ for some integer m, then

$$\mathcal{M}(X) \geq m^2. \tag{11}$$

Proof. For a proof of (10), please see [19, p. 70]. Suppose that $X \equiv 0 \pmod{m}$. Then $X = mY$ for some $Y \in \mathbb{Z}[\zeta_n]$, and $M(X) = m^2 M(Y) \geq m^2$, since $M(Y) \geq 1$. □

Lemma 4.8. *Suppose that $X, Y \in \mathbb{Z}[\zeta_u]$ satisfy $|X|^2 = |Y|^2 = n$ and $X \equiv Y \pmod{a}$ where a, n, v are positive integers. If $X \neq Y$, then $a \leq 2\sqrt{n}$.*

Proof. Suppose that $X \neq Y$. Note that $\mathcal{M}(X) = \mathcal{M}(Y) = n$. As $X \equiv Y \pmod{a}$ by assumption, we have $\mathcal{M}(X - Y) \geq a^2$ by (11). On the other hand,

$$\mathcal{M}(X - Y) \leq \mathcal{M}(X) + \mathcal{M}(Y) + 2\mathcal{M}(X)^{1/2}\mathcal{M}(Y)^{1/2} = 4n$$

by (10). We conclude $a^2 \leq 4n$ and thus $a \leq 2\sqrt{n}$. □

Lemma 4.9. *Let $u, n \geq 2$ be integers and suppose that $X, Y \in \mathbb{Z}[\zeta_u]$ satisfy $|X|^2 = |Y|^2 = n$. If $X \equiv Y \pmod{n}$, then $X = Y$, except for the following cases.*

(i) $n = 2$, X is equivalent to $1 + \zeta_4$, and $Y = \bar{X}$;
(ii) $n = 2$, X is equivalent to $1 + \zeta_4$, $1 + \zeta_7 + \zeta_7^3$, or $1 + \zeta_{15}^6 - \zeta_{15}^8$, and $Y = -X$;
(iii) $n = 3$, $Y \in \{\eta(-1 + \zeta_3), \eta(-1 + \zeta_3^2)\}$ for some root of unity η, and $X = Y + 3\eta$;
(iv) $n = 4$, $X = \pm 2\eta$ for some root of unity η, and $Y = -X$.

Proof. Suppose that $X \equiv Y \pmod{n}$ and $X \neq Y$. By Lemma 4.8, we have $n \leq 2\sqrt{n}$ and thus $n \leq 4$.

Suppose that $n = 4$. By (10),

$$\mathcal{M}(X - Y) \leq \mathcal{M}(X) + \mathcal{M}(Y) + 2\mathcal{M}(X)^{1/2}\mathcal{M}(Y)^{1/2} = 16.$$

Since $X \equiv Y \pmod{4}$, then $\mathcal{M}(X - Y) \geq 16$. Hence we have equality in (10) and thus $Y = \alpha X$ for some $\alpha \in \mathbb{Q}$. Since $|X| = |Y|$, we conclude $X = \pm Y$. As $X \neq Y$, this implies $X = -Y$. Hence $2X \equiv X - Y \equiv 0 \pmod{4}$ and thus $X \equiv 0 \pmod{2}$. This implies $X = 2\eta$ for some root of unity η.

Suppose that $n = 3$. As $X \equiv Y \pmod{3}$, we have $X - Y = 3Z$ for some $Z \in \mathbb{Z}[\zeta_u]$. Suppose that Z is not a root of unity. Then $\mathcal{M}(Z) \geq 3/2$ by [2, Lemma 2]. Thus $\mathcal{M}(X - Y) = 9\mathcal{M}(Z) \geq 27/2$, contradicting (10). Hence Z is a root of unity, i.e., $X - Y = 3\eta$ for some root of unity η. We conclude

$$3 = |X|^2 = |Y + 3\eta|^2 = |Y|^2 + 9 + 3(Y\bar{\eta} + \bar{Y}\eta) = 12 + 3(Y\bar{\eta} + \bar{Y}\eta)$$

and hence $T + \bar{T} = -3$ where $T = Y\bar{\eta}$. This implies $\Re(T) = -3/2$, where $\Re(T)$ denotes the real part of T. Thus $T = -3/2 + ai$ with $a \in \mathbb{Q}$. Note that $3 = |Y|^2 = |T|^2 = 9/4 + a^2$. Hence $a = \pm\sqrt{3}/2$ and $T = -3/2 \pm (\sqrt{3}/2)i = -1 + \zeta_3$ or $T = -1 + \zeta_3^2$. We conclude $Y = \eta T \in \{\eta(-1 + \zeta_3), \eta(-1 + \zeta_3^2)\}$.

Finally, for $n = 2$, we check that either (i) or (ii) holds by applying Lemma 3.1. □

Lemma 4.10. *Suppose $X = \sum_{i=0}^{p-1} x_i \zeta_p^i$ and $x_i \in \mathbb{Z}[\zeta_m]$ for all i. If $p \nmid m$, $|X|^2 = p$ and $|\sum_{i=0}^{p-1} x_i|^2 = p$, then there exists j such that $|x_j|^2 = p$ and $x_i = 0$ if $i \neq j$.*

Proof. Let $Y = \sum_{i=0}^{p-1} x_i$. We first deal with the case $p = 2$. In this case $X = x_0 - x_1$ and $Y = x_0 + x_1$. But by Lemma 4.9, we see that $X = \pm Y$. That means either $x_0 = 0$ or $x_1 = 0$.

We may now assume $p \geq 3$. By Lemma 3.11, we see that $p | X\bar{Y}$. Therefore,

$$X\bar{Y} = \sum_{i=0}^{p-1} x_i \bar{Y} \zeta_p^i = pZ$$

for some $Z \in \mathbb{Z}[\zeta_{pm}]$. Since $|X|^2 = |Y|^2 = p$, it follows that $|X\bar{Y}| = p$. Hence $|Z| = 1$. Therefore, $Z = \zeta\zeta_p^t$ for some integer t and a root of unity $\zeta \in \mathbb{Z}[\zeta_m]$. We may assume $t = 0$. Then

$$\sum_{i=0}^{p-2} (x_i - x_{p-1}) \bar{Y} \zeta_p^i = p\zeta.$$

Multiplying both sides by Y, we obtain $\sum_{i=0}^{p-2} (x_i - x_{p-1}) \zeta_p^i = Y\zeta$ as $Y\bar{Y} = p$.Therefore, $(x_0 - x_{p-1}) = Y\zeta$ and $x_i - x_{p-1} = 0$ whenever $0 < i \leq p - 2$. Thus, $Y = \sum_{i=0}^{p-1} x_i = Y\zeta + p x_{p-1}$. By Lemma 4.9, $x_{p-1} = 0$ and $\zeta = 1$ if $p > 3$. It then follows $x_i = 0$ for $i \neq 0$. Our conclusion then follows.

Finally, we assume $p = 3$. By Lemma 4.9, if $x_{p-1} \neq 0$, we may then assume X or Y is in $\mathbb{Z}[\zeta_3]$ and $X = Y + 3$ after multiplying X and Y by η^{-1}. Thus, we may assume both $X, Y \in \mathbb{Z}[\zeta_3]$. This is impossible as $Y \in \mathbb{Z}[\zeta_m]$ with $3 \nmid m$. Therefore, $x_{p-1} = 0$ and hence $x_i = 0$ if $i \neq 0$. □

5 General Nonexistence Results

In this section, we assume D is an (mn, n, mn, m) RDS in an abelian group G. We will derive some necessary conditions on m, n.

Theorem 5.1. *Let D be an (mn, n, mn, m) RDS in group G relative to a subgroup N. Suppose q is a prime divisor of n and $q^t \| mn$.*

(a) For any prime $p \neq q$ that divides mn and self-conjugate modulo q if q is odd or q^t if $q = 2$, then $p^b \| mn$ implies b is even.

(b) Let $q_1, q_2, \ldots, q_s$ be all the distinct prime divisors of mn which are self-conjugate modulo q if q is odd and q^t if $q = 2$. Suppose $q \neq q_i$ for all i and $q_i^{b_i} \| mn$ for $i = 1, \ldots, s$. Denote $A := mn/(q^t q_1^{b_1} \ldots q_s^{b_s})$. Then either A is a square or $q \leq A^2 + A + 1$.

Proof. There exists $\chi \notin N^\perp$ such that $\mathrm{ord}(\chi) = q^r$. By Lemma 2.4, $|\chi(D)|^2 = mn$. Since $p^b \| mn$ and $\chi(D) \in \mathbb{Z}[\zeta_{q^r}]$, it follows from Corollary 3.10 that b is even.

For (b), it follows from Proposition 3.9 that there exists $B \in \mathbb{Z}[\zeta_{q^r}]$ such that $B | \chi(D)$ and $|B|^2 = q^a q_1^{b_1} \ldots q_s^{b_s}$. Therefore, there exists $X \in \mathbb{Z}[\zeta_{q^r}]$ such that $|X|^2 = A$. It follows from Lemma 3.3 that $q \leq A^2 + A + 1$. □

To deal with the case when A is a square, we need a different approach.

Lemma 5.2. *Let D be an (mn, n, mn, m) RDS in group G relative to a subgroup N. Suppose $q^{2c} \| mn$ and there exists a subgroup G' such that $G = G' \times G_1$ and $q \nmid |G'|$. If $q^c | \chi(D)$ for all $\chi \in G_1^\perp$, then*

$$q^c n \leq n + |G_1| - |G_1 \cap N|.$$

Proof. Let $\eta : G \to G'$ be the natural projection. Write $D = \sum_{h \in G'} X_h h$ where $X_h \in \mathbb{Z}[G_1]$. Note that $\eta(D) = \sum_{h \in G'} |X_h| h$ and

$$\eta(DD^{(-1)}) = mn + m|G_1| \cdot G' - m \cdot \eta(N). \tag{12}$$

By Corollary 2.6, $|X_h| \equiv 0 \pmod{q^c}$ for all h. By comparing the coefficients of identity in both sides of the Equation (12), we get

$$\sum_{h \in G'} |X_h|^2 \leq mn + m|G_1| - m|G_1 \cap N|.$$

Since $\sum_{h\in G'}|X_h| = mn$ and q^c divides $|X_h|$, it follows that

$$\sum_{h\in G'}|X_h|^2 \geq q^{2c}\frac{\sum_{h\in G'}|X_h|}{q^c}.$$

(Here we use the inequality that if all a_i's are nonzero integers, $\sum_{i=1}^{r}|a_i|^2 \geq |a|^2 r$ where $a = min\{a_i : i = 1,\ldots,r\}$.) Therefore, $q^{2c}(\frac{mn}{q^c}) \leq mn + m|G_1| - m|G_1 \cap N|$ and our lemma follows. □

Theorem 5.3. *Let D be an (mn, n, mn, m) RDS in group G relative to a subgroup N. Suppose q is a prime; $q^c \| mn$ and n is not a power of q. If there exist $m'|m$, $n'|n$ such that the following conditions hold:*

(i) $\gcd(\frac{mn^2}{m'n'^2}, m'n'^2) = 1$;

(ii) $q \nmid m'n'$ *and* $n' \neq 1$;

(iii) q *is self-conjugate modulo* $m'n'^2$;

then c is even and $q^{\frac{c}{2}}n' \leq n' + \frac{mn}{m'n'} - 1$.

Proof. By (i), there exist subgroups G' of order $m'n'^2$ and subgroup G_1 of order $\frac{mn^2}{m'n'^2}$ such that $G = G' \times G_1$. For any nonprincipal $\chi \in G_1^{\perp}$, $\chi(D) \in \mathbb{Z}[\zeta_{m'n'}]$ and $|\chi(D)|^2 = mn$ or 0. As $q \nmid n'$ and $n' > 1$, it follows from Theorem 5.1 that c is even. By Proposition 3.9 , we deduce that $q^{c/2}|\chi(D)$. Our Theorem now follows from Lemma 5.2. □

For the purpose of our applications, it is sufficient to consider the case m', n' in Theorem 5.3 are p-powers.

Theorem 5.4. *Let D be an (mn, n, mn, m) RDS in group G relative to a subgroup N. Suppose $m = p^a r$, $n = p^b s$ where p is an odd prime, a, b are integers with $b \geq 1$; and $\gcd(p, r) = \gcd(p, s) = 1$. Suppose rs is a square, write $rs = (v_0 v_1)^2$, where $ord_p(q) \equiv 0 \pmod 2$ if $q|v_0$; and $ord_p(q) \equiv 1 \pmod 2$ if $q|v_1$. If one of the following conditions*

(i) $v_1 = 1$;

(ii) $v_1 > 1$ *and* $\gcd(ord_p(q_1), \ldots, ord_p(q_k)) > 2v_1 - 1$, *where* $q_1, \ldots, q_k$ *are the distinct prime divisors of* v_1*;*

holds, then $p^b \leq \sqrt{rs} + 1$.

Proof. We will follow the notation used in Theorem 5.3. In this case, $|G'| = p^{a+b}$ and $|G_1| = rs$. It follows from Lemma 3.2 that $(v_0 v_1) \mid \chi(D)$. Since $\gcd(v_0 v_1, p) = 1$, we may argue by a similar argument as in Theorem 5.3 and obtain

$$(v_0 v_1)^2 \frac{p^{a+b} rs}{v_0 v_1} \leq mn + m(rs^2) - p^a rs = p^{a+b} rs + p^a r^2 s^2 - p^a rs.$$

Recall that $rs = (v_0 v_1)^2$. After simplification, we obtain $p^b \leq \sqrt{rs} + 1$. □

The following results were implicitly contained in [1] and recorded in [8]. The first one deal with the exponent of the group.

Lemma 5.5. *Let* D *be an abelian* (mn, n, mn, m) *RDS in* G *relative to* N. *For any prime* p *that divides* n, *we let* S_p *be the* p*-Sylow subgroup of* N. *Then either* $p < m+1$ *or* $|S_p| > \sqrt{n}$.

Lemma 5.6. *Let* R *be an abelian* (mn, n, mn, m) *RDS in* G *relative to* N. *Suppose* $p \geq 3$ *is a prime dividing* n *and* $r_p(G)$ *denote the* p*-rank of* G, *i.e. the minimum number of generators of the Sylow* p*-subgroup of* G. *Then*

$$(p - m - 1)n \leq p^{r_p(G)} - p^{r_p(N)} - p^{r_p(G/N)}.$$

It is easy to deduce the following from Lemma 5.6.

Corollary 5.7. *Let* D *be an abelian* (mn, n, mn, m) *RDS in* G *relative to* N. *There exists at most one prime* p *that divides* n *with* $p > m + 1$.

Corollary 5.7 is crucial in the proof [8, Theorem 61.] as it reduces to the case when n has at most one prime factor larger than 3. To end this section, we record a technical result.

Lemma 5.8. *Suppose* D *is an* (mn, n, mn, m) *RDS in* G *relative to* N *and* $\gcd(m, n) = 1$. *Write* $G = G' \times H$ *where* G' *is a subgroup of order* m *and* H *a subgroup of order* n^2. *If* $D = \sum_{g \in G'} D_g g$, *then* $D_g D_h \neq H$ *for some* $g \neq h$ *in* G'.

Proof. Suppose $D_gD_h = H$ for all $g \neq h$ in G'. Then $D_gD_h^{(-1)} = H$ for all $g \neq h$ in G'. Set $W_g = \mathrm{supp}(D_gD_g^{(-1)})$ for any $g \in G'$. Suppose $ab^{-1} = cd^{-1}$ for some elements $a, b \in \mathrm{supp}(D_g)$ and $c, d \in \mathrm{supp}(D_h)$. As $ad = bc$ and $D_gD_h = H$, we have $a = b$ and $c = d$. Therefore, $ab^{-1} = e$. This shows $W_g \cap W_h = \{e\}$. In particular, $\bigcup_{g\neq e} \mathrm{supp}(D_gD_g^{(-1)}) \cap \mathrm{supp}(D_eD_e^{(-1)}) = \{e\}$. Write

$$\sum_{g\in G'\setminus\{e\}} D_gD_g^{(-1)} = (m-1)n + T_1 \text{ and } D_eD_e^{(-1)} = n + T_2$$

where $T_1, T_2 \in \mathbb{Z}[H]$. Note that $\mathrm{supp}(T_1) \cap \mathrm{supp}(T_2) \subset \{e\}$. On the other hand, as $DD^{(-1)} = mn + m(G - N)$, it follows that

$$\sum_{g\in G'} D_gD_g^{(-1)} = mn + m(H - N) = mn + T_1 + T_2.$$

Hence, $T_1 + T_2 = m(H - N)$. As $\mathrm{supp}(T_1) \cap \mathrm{supp}(T_2) \subset \{e\}$, it follows that $T_1 = mT_1'$ and $T_2 = mT_2'$ where $T_1', T_2' \in \mathbb{Z}[H]$.

Let χ be a nontrivial character on H. Then $\chi(D_e) = 0$ implies $n + m\chi(T_2') = 0$. Hence, $m|n$. This is impossible. On the other hand, if $\chi(D_e) \neq 0$, then $\chi(D_g) = 0$ for all $g \neq e$. Therefore, $(m-1)n + m\chi(T_1') = 0$. Again, $m|n$, which is impossible. □

6 Abelian (pn, n, pn, p) RDSs

In this section, we are only concerned with (pn, n, pn, p) RDSs for prime p.

Theorem 6.1. *Let p, q be distinct primes. Then there does not exist an abelian (pq^r, q^r, pq^r, p) RDS if either one of the following holds:*

(a) $ord_q(p) \geq 2p$.

(b) $p^2 + p + 1 < q$.

(c) q is self-conjugate modulo p.

Proof. Let $G = \langle g\rangle \times H$ be an abelian group, where $g^p = 1$ and $|H| = q^{2r}$. Write $D = \sum_{i=0}^{p-1} D_ig^i$, where $D_i \subseteq H$.

Recall that D contains exactly one element of each coset of N. Since $g \notin N$ and $N \subset H$, this implies that each D_i contains exactly one element of each coset of N

in H. Suppose ψ is a nontrival character of H that is trivial on N. Let τ be the character of H/N that is induced by ψ, that is, $\tau(Ng) = \psi(g)$ for all $g \in H$. Note that τ is nontrivial since ψ is nontrivial. Hence

$$\chi(D_i) = \sum_{g \in D_i} \psi(g) = \sum_{g \in D_i} \tau(Ng) = \tau(H/N) = 0 \text{ for all } i. \tag{13}$$

To prove part (a), we let $\chi \notin N^\perp$ with $\mathrm{ord}(\chi) = q^a$ for some integer a. Then $|\chi(D)|^2 = pq^r$. By Lemma 3.6, there exists $X \in \mathbb{Z}[\zeta_{q^a}]$ such that $|X|^2 = p$. By Lemma 3.4, we get a contradiction.

(b) follows from Lemma 3.3.

Finally, we assume q is self-conjugate modulo p. Let $\chi \notin N^\perp$ be any nontrivial character of group G with $\mathrm{ord}(\chi) = q^a$ for some integer a and σ be a character of order p. Clearly,

$$|\sum_{i=0}^{p-1} \chi(D_i)\zeta_p^{ij}|^2 = pq^r$$

for $j = 0, \ldots, p-1$. Since q is self-conjugate modulo p, we deduce from Corollary 2.6 that $\Theta^r | \chi(D_i)$ for $i = 0, \ldots, p-1$. Let $\chi(D_i) = \Theta^r x_i$. Then we have

$$|\sum_{j=0}^{p-1} x_j \zeta_p^j|^2 = p \text{ and } |\sum_{j=0}^{p-1} x_j|^2 = p.$$

By Lemma 4.10, we see that there exists $i(\chi)$ such that $|x_{i(\chi)}|^2 = p$ for some $i(\chi)$ and $x_j = 0$ if $j \neq i(\chi)$. Therefore, $|\chi(D_{i(\chi)})|^2 = pq^r$ and $\chi(D_j) = 0$ if $j \neq i(\chi)$. Hence for any $\chi \notin N^\perp$, we have $\chi(D_i D_j) = 0$ whenever $i \neq j$. Combining this with (13), we conclude that, for every nontrivial character χ of H, we have $\chi(D_i D_j) = 0$ for $i \neq j$. Note that as $|D_i||D_j| = |H|$, $D_i D_j = H$. This contradicts Lemma 5.8. □

We remark that Theorem 6.1 can be generalized by using a similar argument, but omit the tedious details.

Theorem 6.2. *Let p a prime, let $n > 1$ be an integer coprime to p, and let u be a divisor of n such that $\gcd(u, n/u) = 1$ and n/u is self-conjugate modulo pn. If an abelian (pn, n, pn, p) RDS exists, then $p \leq \max\{4u^4, 2^{u^2-1}\}$.*

Proof. Suppose such RDS exists and assume that $p > \max\{4u^4, 2^{u^2-1}\}$. Let $G = \langle g \rangle \times H$ be an abelian group, where g is an element of order p and $|H| = n^2$. By Lemma 2.1, we have $\exp(G)|np$ (the case $G = \mathbb{Z}_4$ cannot occur, since $\gcd(p, n) = 1$). As n/u is self-conjugate modulo pn by assumption, we conclude that n/u is self-conjugate modulo $\exp(G)$.

Let q, q' be primes that divide n/u. Suppose $q^t||(n/u)$. Then by Theorem 5.1 (a), t is even if $q \neq q'$. As $q \neq p$ and $\gcd(n/u, u) = 1$. It follows that either n/u is a square or $n/u = q^r$ for some odd integer r.

For any nonprincipal character χ, $|\chi(D)|^2 = pn$ or 0. As the order of χ divides $\exp(G)$ and n/u is self conjugate modulo $\exp(G)$, we then conclude from Proposition 3.9 that there exist integer x and a prime $q|n$ such that $|x\Theta_q^i|^2 = n/u$; and

$$\chi(D) \equiv 0 \pmod{x\Theta_q^i}.$$

Here $i = 0$ or 1 and $i = 0$ if n/u is a square. For convenience, we write $y = x\Theta_q^i$.

Write $D = \sum_{i=0}^{p-1} D_i g^i$ as in Theorem 6.1. In view of Corollary 2.6, we conclude that if χ is nonprincipal, then $y|\chi(D_i)$. Thus, we may set $x_i = \chi(D_i)/y$ for all i and $x_i \in \mathbb{Z}[\zeta_n]$ as $\chi(D_i) \in \mathbb{Z}[\zeta_n]$.

If $\chi \notin N^\perp$, then $|\chi(D)|^2 = pn$ and thus

$$|\sum_{i=0}^{p-1} x_i \zeta_p^i|^2 = |\sum_{i=0}^{p-1} x_i|^2 = pu.$$

By Lemma 3.11,

$$(\sum_{i=0}^{p-1} x_i \zeta_p^i)(\sum_{i=0}^{p-1} x_i) = pY$$

where $Y \in \mathbb{Z}[\zeta_{pn}]$ and $|Y|^2 = u^2$. Write $Y = \sum_{i=0}^{p-1} y_i \zeta_p^i$ where $y_i \in \mathbb{Z}[\zeta_n]$. By Proposition 4.6 and our assumption that $p > \max\{4u^4, 2^{u^2-1}\}$, we see that there exists t such that $Y = y_t \zeta_p^t$ and $y_j = 0$ if $j \neq t$. Hence,

$$\sum_{j=0}^{p-1} x_j \zeta_p^j = (\sum_{j=0}^{p-1} x_j)^{-1} p y_t \zeta_p^t \in \mathbb{Q}[\zeta_n]\zeta_p^t.$$

Since $\sum_{j=0}^{p-1} x_j \zeta_p^j$ is an algebraic integer in $\mathbb{Z}[\zeta_{pn}]$,

$$x_t + \sum_{j \neq t} x_j \zeta_p^{j-t} = (\sum_{j=0}^{p-1} x_j \zeta_p^j)\zeta_p^{-t} = (\sum_{j=0}^{p-1} x_j)^{-1} p y_t \in \mathbb{Z}[\zeta_n].$$

It follows that $x_j = x_i$ whenever $j \neq t, i \neq t$. Now set $s \neq t$ and observe that

$$x_t - x_s = \sum_{j=0}^{p-1} x_j \zeta_p^{j-t}.$$

Hence, $|x_t - x_s|^2 = pu$. Moreover,

$$\sum_{i=0}^{p-1} x_i = (x_t - x_s) + px_s.$$

If $x_s \neq 0$, then by Lemma 4.8, we obtain $p < 2\sqrt{pu^2}$. This is impossible. Hence, $x_s = 0$ and $x_j = 0$ if $j \neq t$. Therefore, $\chi(D_t) \neq 0$ and $\chi(D_j) = 0$ if $j \neq t$. That means $\chi(D_i D_j) = 0$. Since this is true for all nonprincipal $\chi \in \langle g \rangle^{\perp}$, $D_i D_j = aH$ for an integer a. Now $|D_i| = |D_j| = n$ and $|H| = n^2$, so $a = 1$. By Lemma 5.8, we get a contradiction. □

Corollary 6.3. *For any fixed integer $n \geq 2$, an abelian (pn, n, pn, p) RDS exists for at most finitely many primes p.*

Proof. Assume that an abelian (pn, n, pn, p) RDS exists. We set $u = n$ in Theorem 6.2. Then $n/u = 1$. We may then say n/u is self conjugate modulo pn and by Theorem 6.2, we get the desired conclusion. On the other hand, one may set $y = 1$ in the proof of Theorem 6.2, and then apply the argument to conclude $p \leq \max\{4n^4, 2^{n^2-1}\}$. □

Corollary 6.4. *Let $p > 3$ be a prime and let n be a positive integer such that n is self-conjugate modulo pn. Then no abelian (pn, n, pn, p) RDS exists.*

Proof. Assume that an abelian (pn, n, pn, p) RDS exists. Setting $u = 1$ in Theorem 6.2, we conclude $p \leq \max(4, 2^0) = 4$. □

Note that Corollary 6.4 generalizes Theorem 6.1 (c) if $p > 3$. Next, we consider cases without the self-conjugacy condition. It has been shown in [14] that (pq, q, pq, p) RDS does not exist if $p > q$.

Theorem 6.5. *Let p and q be two distinct odd primes such that* $\gcd(p, q-1) = 1$. *Then there does not exist an abelian (pq, q, pq, p) RDS. In particular, there is no abelian (pq, q, pq, p) RDS if $p > q$.*

Proof. Let $G = \langle g \rangle \times H$ be an abelian group, where $\mathrm{ord}(g) = p$ and $|H| = q^2$. Write $D = \sum_{i=0}^{p-1} D_i g^i$, where $D_i \subseteq H$. Note that by Lemma 2.1, $\exp(G) = pq$. Let $\chi \in G^* \backslash N^\perp$ be a character of order q and τ be a character of order p. Note that $\chi(D) = x\Theta_q$ where $x \in \mathbb{Z}[\zeta_q]$ with $|x|^2 = p$.

By Lemma 3.11, we see that $x|\tau\chi(D)$ and therefore, $\tau\chi(D) = xY$ with $Y \in \mathbb{Z}[\zeta_{pq}]$. As $|Y|^2 = q$, it follows from Lemma 3.7 that either $Y = \Theta_q\zeta$ or $Y \in \mathbb{Z}[\zeta_p]\zeta$ where ζ is a root of unity. Note that as $x \in \mathbb{Z}[\zeta_q]$ and $x|\tau\chi(D)$, $x|\chi(D_i - D_j)$ for any i, j.

We first consider the case $Y \in \mathbb{Z}[\zeta_p]\zeta_q^j$ for some j. We may assume $Y = (\sum_{i=1}^{p-1} a_i\zeta_p^i)\zeta_q^j$ where a_i's are integers. As $x|\chi(D_i - D_0)$, $\chi(D_i - D_0) = xa_i\zeta_q^j$. Note that $\mathrm{ord}(\chi) = q$ as $\exp(G)|pq$. $H = (Ker(\chi) \cap H) \times Q$ where Q is a subgroup of order q. Let $\eta : G \to H$ be the natural projection. We may consider χ a character of Q and $|\chi(\eta(D_i - D_0))|^2 = pa_i^2$. Thus,

$$\eta((D_i - D_0)(D_i - D_0)^{(-1)}) = pa_i^2 + \alpha Q. \tag{14}$$

But by applying the principal character on the above equation, we conclude that $pa_i^2 + \alpha q = 0$. Note that $\alpha \neq 0$ if $a_i \neq 0$. Therefore, $q|a_i$. But then we have $q|Y$, which is impossible as $|Y|^2 = q$. Hence $Y = \Theta_q\zeta$ where ζ is a root of unity.

We may assume $Y = \Theta_q\zeta\zeta_p^j$ where ζ is a root of unity in $\mathbb{Z}[\zeta_q]$. Pick $t \neq j$, then $\sum \chi(D_i - D_t)\zeta_p^i = xZ$. It is then clear that $\chi(D_i - D_t) = 0$ and $\chi(D_j - D_t) = x\Theta_q\zeta$. But then

$$x\Theta_q = \sum_{i=0}^{p-1} \chi(D_i) = \sum \chi(D_i - D_t) + p\chi(D_t) = x\Theta_q\zeta + p\chi(D_t).$$

If $\zeta \neq 1$, then p divides $|1 - \zeta|$. This is impossible as $\zeta = \pm\zeta_q^i$. Thus $\chi(D_t) = 0$; $\chi(D_j) = \chi(D)$ and $\chi(D_i) = 0$ if $i \neq j$.

It follows that $\chi(D_iD_j) = 0$ for all nonprincipal $\chi \in \langle g \rangle^\perp$. Note that $\chi(D_i) = 0$ if $\chi \in N^\perp$ by the same argument as for (13). Therefore $D_iD_j = aH$ for an integer a. As $|D_i| \cdot |D_j| = n^2 = |H|$, we see that $a = 1$ and $D_iD_j = H$. This contradicts Lemma 5.8. □

7 $m = 2, 3$ or 4

In this section, we focus cases on $m \leq 4$. We will now illustrate how our previous results be applied in these situations. First, $(2n, n, 2n, 2)$-RDSs have been studied

extensively in [8]. One of main result is the following:

Result 7.1. [8, Theorem 6.10] *If an abelian $(2n, n, 2n, 2)$ RDS exists, then n is a power of 2 except in the following cases.*

(a) $n = 2^a 3^b$, $a, b \geq 1$.

(b) $n = 2^a 3^b p^c$, $p^c > 2^a 3^b > 1$ *for a prime* $p > 3$.

Here, we illustrate how we derive the above result from ours. By Theorem 6.1, we see that $(2q^r, q^r, 2q^r, 2)$ RDS does not exist if q is a prime larger than 3. It then follows from Corollary 6.4 that $2|n$ and there is at most one prime $p \geq 5$ that divides n.

Unfortunately, Corollary 6.4 cannot be applied to exclude cases not yet excluded from Result 7.1. However, we may apply Theorem 5.4 to study $(q^{2c}p^{a+b}, q^{\alpha}p^b, q^{2c}p^{a+b}, q^{2c-\alpha}p^a)$ RDS.

Lemma 7.2. *Suppose p, q are distinct primes and p is odd. Let a, b, c, α be positive integers and D be $(q^{2c}p^{a+b}, q^{\alpha}p^b, q^{2c}p^{a+b}, q^{2c-\alpha}p^a)$ RDS. If q is self-conjugate modulo p or $ord_p(q) > q^c - 1$, then $p^b \leq q^c + 1$.*

Theorem 7.3. *Suppose an abelian $(2n, n, 2n, 2)$ RDS exists and p is an odd prime.*

(a) If $n = 2p^b$, then $p = 7$ and b is even.

(b) If $n = 4p^b$, then $p^b \in \{7^r, 23^r, 31^r, 73^s : \ r \geq 2$ is even, $s \geq 1\}$.

(c) If $n = 8p^b$, then $p^b = 3$ or 7^r with $r \geq 2$.

Proof. If 2 is self-conjugate modulo p or $\mathrm{ord}_p(q) \geq 3$, then by Lemma 7.2, $p \leq 3$ and $b = 1$. But as 3 is self-conjugate modulo 4, it follows from Theorem 6.1 that b is even if $n = 2 \cdot 3^b$.

If 2 is not self-conjugate modulo p and $\mathrm{ord}_p(2) > 2v_1 - 1 = 3$, then again by Lemma 7.2, we get $p^b \leq 3$. This is impossible. Thus, $\mathrm{ord}_p(2) \leq 3$. Consequently, $p = 3, 5$ or 7. As we assume 2 is not self-conjugate modulo p, $p = 7$. Again, as 7 is conjugate modulo 4 from Theorem 6.1 that b is even.

For (b), by Theorem 5.1 (b), there exists $B \in \mathbb{Z}[\zeta_{p^b}]$ such that $|B|^2 = 8$. As shown in [12, Corollary 33], $p = 3, 5, 7, 23, 31, 73$. Since 2 is self-conjugate modulo 3 and

5, then p cannot be 3 or 5. Note that 7, 23 and 31 are self-conjugate modulo 8, it follows from Theorem 6.1 that b is even if $n = 4 \cdot 7^b$, $n = 4 \cdot 23^b$ or $n = 4 \cdot 31^b$.

The proof of (c) is similar as (a). If 2 is self-conjugate modulo p, then $p^b \leq 2^2+1 \leq 5$. Thus, $p^b = 3$ or 5. By Lemma 5.5, p^b cannot be 5.

If 2 is not self-conjugate modulo p and $\mathrm{ord}_p(2) > 2v_1 - 1 = 7$, then $p^b \leq 5$. This is impossible. Thus, $\mathrm{ord}_p(2) \leq 7$. Consequently, $p = 3, 5, 7, 31$ or 127. As we assume 2 is not self-conjugate modulo p, $p = 7, 31$ or 127. For any $\chi \notin N^\perp$ with order p^a for some $a \geq 1$, we have $|\chi(D)| = 16p^b$. Then $\chi(D) = \Theta_p^b Y$, where $Y \in \mathbb{Z}[\zeta_{p^a}]$. Hence $|Y|^2 = 16$. By using a similar argument as in [12, Corollary 33], we see that either $4|Y$ or $p = 7$. If $\neq 7$, we get a contradiction by Lemma 5.5. (Note that using the notation in Lemma 5.5, $q^{2c} = 16$, $n = 4p^b$, $|G_1| = 16$ and $|G'| = p^{2b}$.) □

For $m = 3$, we obtain a result analogous to Result 7.1 as follows:

Theorem 7.4. *Suppose an abelian* $(3n, n, 3n, 3)$ *RDS exists. Then one of the following conditions is satisfied:*

(a) $n = p^r$ *with* $p = 3$ *or* 13.

(b) $n = 2^a 3^b$, $a, b \geq 1$.

(c) $n = 2^a 3^b p^c$, $p^c > 2^a 3^b > 1$ *for a prime* $p > 3$.

Proof. By Theorem 6.1, we see that $p \leq 13$. On the other hand, 3 is not self-conjugate modulo p and p is not self-conjugate modulo 3, therefore, $p = 2$ or 13. By Corollary 6.4, there is at most one prime factor of n larger than 3. Thus (b) or (c) holds. □

Again, by applying Lemma 7.2, we obtain the following in case $n = 3p^r$.

Theorem 7.5. *Let* $p > 3$ *be a prime. If an abelian* $(9p^r, 3p^r, 9p^r, 3)$ *RDS exists, then* $p = 11$ *or* 13.

Proof. Suppose $\mathrm{ord}_p(3) > 5$ or p is self-conjugate modulo 3. Then by Lemma 7.2, $p^r \leq 3 + 1 = 4$. This is impossible as $p \geq 5$. Therefore, $\mathrm{ord}_p(3) \leq 5$ and p is not self-conjugate modulo 3. Thus, $p = 11$ and 13. □

For $m = 4$, using a similar argument as Theorem 7.3, we deduce the following:

Theorem 7.6. *Let p be a prime and r be a positive integer, then there does not exist an abelian $(4p^r, p^r, 4p^r, 4)$ RDS except $p = 2, 7$ and $p = 3,\ r = 1$.*

Note that an abelian $(12, 3, 12, 4)$ RDS indeed exists [3, 9] as now $2 \nmid n$ and Theorem 6.1 is no longer applicable in that case. In case $p = 7$, it has been shown that $r \neq 1$ in [6]. It is possible to apply our results to get another proof but the main idea behind is not so different though. Next, we summarize the result for $(4n, n, 4n, 4)$ RDS, which now follows from Corollary 5.7 and Theorem 7.6.

Corollary 7.7. *If an abelian $(4n, n, 4n, 4)$ RDS exists, then one of the following conditions is satisfied:*

(1) $n = 2^a, 3$ or 7^b, where $a \geq 1$, $b \geq 2$;

(2) $n = 2^a 3^b 5^c$, at least two of a, b, c greater than 0.

(3) $n = 2^a 3^b 5^c p^d$, $p^d > 2^a 3^b 5^c > 1$ for a prime $p > 5$.

Analogous to Theorem 7.3, we obtain the following:

Theorem 7.8. *Let p be an odd prime.*

(a) There does not exist an abelian $(8p^b, 2p^b, 8p^b, 4)$ RDS unless $p^b \in \{7^r, 23^r, 31^r, 73^s : r \geq 2$ is even, $s \geq 1\}$.

(b) There does not exist an abelian $(16p^b, 4p^b, 8p^b, 4)$ RDS unless $p^b \in \{3, 5, 7^r : \ r \geq 2\}$.

Proof. The proof of (a) is similar to that in Theorem 7.3 (b). For (b), the proof is similar as Theorem 7.3 Lastly, note that $p^b \neq 7$ from Lemma 5.6. □

8 Conclusion

In this paper, we have proved several nonexistence results of abelian (mn, n, mn, m) RDS. In particular, we show that there is no abelian $(2n, n, 2n, 2)$ RDS for all $3 \leq n \leq 100$ except n is a 2-power and 3 other cases which is summarized in Table 1. Similarly, there is no abelian $(3n, n, 3n, 3)$ RDS for all $2 \leq n \leq 100$ except n is a

3-power and 4 other cases which is summarized in Table 2, and there is no abelian $(4n, n, 4n, 4)$ RDS for all $3 \leq n \leq 100$ except n is a 2-power and 6 other cases which is summarized in Table 3.

Acknowledgment

The authors express their gratitude to the anonymous reviewers for their detailed and constructive comments which are very helpful to the improvement of the presentation of this paper.

References

[1] A. Blokhuis, D. Jungnickel, and B. Schmidt. Proof of the prime power conjecture for projective planes of order n with abelian collineation groups of order n^2. *Proc. Amer. Math. Soc.*, 130(5):1473–1476, 2002.

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

[3] J. A. Davis, J. Jedwab, and M. Mowbray. New families of semi-regular relative difference sets. *Des. Codes Cryptogr.*, 13(2):131–146, 1998.

[4] J. E. H. Elliott and A. T. Butson. Relative difference sets. *Illinois J. Math.*, 10:517–531, 1966.

[5] T. Feng. Relative (pn, p, pn, n)-difference sets with $\mathrm{GCD}(p, n) = 1$. *J. Algebraic Combin.*, 29(1):91–106, 2009.

[6] T. Feng and Q. Xiang. Semi-regular relative difference sets with large forbidden subgroups. *J. Combin. Theory Ser. A*, 115(8):1456–1473, 2008.

[7] C. Godsil and A. Roy. Equiangular lines, mutually unbiased bases, and spin models. *European J. Combin.*, 30(1):246–262, 2009.

[8] Y. Hiramine. On abelian $(2n, n, 2n, 2)$-difference sets. *J. Combin. Theory Ser. A*, 117(7):996–1003, 2010.

[9] K. H. Leung, S. Ling, and S. L. Ma. Constructions of semi-regular relative difference sets. *Finite Fields Appl.*, 7(3):397–414, 2001.

[10] K. H. Leung, S. L. Ma, and V. Tan. Planar functions from Z_n to Z_n. *J. Algebra*, 224(2):427–436, 2000.

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

[12] K. H. Leung and B. Schmidt. Nonexistence results on generalized bent functions $\mathbb{Z}_q^m \to \mathbb{Z}_q$ with odd m and $q \equiv 2 \pmod 4$. *J. Combin. Theory Ser. A*, 163:1–33, 2019.

[13] V. F. Lev. The rectifiability threshold in abelian groups. *Combinatorica*, 28:491–497, 2008.

[14] S. L. Ma. Planar functions, relative difference sets, and character theory. *J. Algebra*, 185(2):342–356, 1996.

[15] S. L. Ma and B. Schmidt. Relative (p^a, p^b, p^a, p^{a-b})-difference sets: a unified exponent bound and a local ring construction. *Finite Fields Appl.*, 6(1):1–22, 2000.

[16] A. Pott. *Finite geometry and character theory*, volume 1601 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1995.

[17] B. Schmidt. On (p^a, p^b, p^a, p^{a-b})-relative difference sets. *J. Algebraic Combin.*, 6(3):279–297, 1997.

[18] B. Schmidt. *Characters and cyclotomic fields in finite geometry*, volume 1797 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2002.

[19] F. Stan and A. Zaharescu. The Siegel norm of algebraic numbers. *Bull. Math. Soc. Sci. Math. Roumanie (N.S.)*, 55(103)(1):69–77, 2012.

[20] T. Zhang and G. Ge. On (mn, n, mn, m) relative difference sets with $\gcd(m, n) = 1$. *J. Algebraic Combin.*, 48:565–579, 2018.

n	nonexistence	n	nonexistence	n	nonexistence
3	[8], Theorem 6.1	5	[8], Theorem 6.1	6	Theorem 5.1
7	[8], Theorem 6.1	9	[8], Theorem 6.1	10	Theorem 7.3
11	[8], Theorem 6.1	12	Theorem 5.1	13	[8], Theorem6.1
14	Theorem 5.1	15	Theorem 5.1	17	[8], Theorem 6.1
18	Theorem 7.3	19	[8], Theorem 6.1	20	Theorem 5.1
21	Theorem 5.1	22	Theorem 5.1	23	[8], Theorem 6.1
24	?	25	[8], Theorem 6.1	26	Theorem 7.3
27	[8], Theorem 6.1	28	Theorem 5.1	29	[8], Theorem 6.1
30	Theorem 5.1	31	[8], Theorem 6.1	33	Theorem 5.1
34	Theorem 7.3	35	Theorem 5.1	36	Theorem 5.1
37	[8], Theorem 6.1	38	Theorem 5.1	39	Theorem 5.1
40	[8, Theorem 3.11]	41	[8], Theorem 6.1	42	Theorem 5.1
43	[8], Theorem 6.1	44	Theorem 5.1	45	Theorem 5.1
46	Theorem 5.1	47	[8], Theorem 6.1	48	Theorem 5.1
49	[8], Theorem 6.1	50	Theorem 7.3	51	Theorem 5.1
52	Theorem 5.1	53	[8], Theorem 6.1	54	Theorem 5.1
55	Theorem 5.1	56	[8, Theorem 3.11]	57	Theorem 5.1
58	Theorem 7.3	59	[8], Theorem 6.1	60	Theorem 5.1
61	[8], Theorem 6.1	62	Theorem 5.1	63	Theorem 5.1
65	Theorem 5.1	66	Theorem 5.1	67	[8], Theorem 6.1
68	Theorem 5.1	69	Theorem 5.1	70	Theorem 5.1
71	[8], Theorem 6.1	72	Theorem 5.3	73	[8], Theorem 6.1
74	Theorem 7.3	75	Theorem 5.1	76	Theorem 5.1
77	Theorem 5.1	78	Theorem 5.1	79	[8], Theorem 6.1
80	Theorem 5.1	81	[8], Theorem 6.1	82	Theorem 7.3
83	[8], Theorem 6.1	84	Theorem 5.1	85	Theorem 5.1
86	Theorem 5.1	87	Theorem 5.1	88	Theorem 7.2
89	[8], Theorem 6.1	90	Theorem 5.1	91	Theorem 5.1
92	Theorem 7.3	93	Theorem 5.1	94	Theorem 5.1
95	Theorem 5.1	96	?	97	[8], Theorem 6.1
98	?	99	Theorem 5.1	100	Theorem 5.1

Table 1: Nonexistence of abelian $(2n, n, 2n, 2)$ RDS for $2 \leq n \leq 100$ and $n \neq 2^a$

n	nonexistence	n	nonexistence	n	nonexistence
2	Theorem 7.4	4	Theorem 7.4	5	Theorem 7.4
6	Theorem 5.1	7	Theorem 7.4	8	Theorem 7.4
10	Theorem 5.1	11	Theorem 7.4	12	?
13	?	14	Theorem 5.1	15	Theorem 5.1
16	Theorem 7.4	17	Theorem 7.4	18	Theorem 5.1
19	Theorem 7.4	20	Theorem 5.1	21	Theorem 5.3
22	Theorem 5.1	23	Theorem 7.4	24	Theorem 5.1
25	Theorem 7.4	26	Theorem 5.1	28	Theorem 5.1
29	Theorem 7.4	30	Theorem 5.1	31	Theorem 7.4
32	Theorem 7.4	33	Theorem 5.1	34	Theorem 5.1
35	Theorem 5.1	36	Theorem 5.1	37	Theorem 7.4
38	Theorem 5.1	39	?	40	Theorem 5.1
41	Theorem 7.4	42	Theorem 5.1	43	Theorem 7.4
44	Theorem 5.1	45	Theorem 5.1	46	Theorem 5.1
47	Theorem 7.4	48	?	49	Theorem 7.4
50	Theorem 5.1	51	Theorem 5.1	52	Theorem 5.1
53	Theorem 7.4	54	Theorem 5.1	55	Theorem 5.1
56	Theorem 5.1	57	Theorem 7.5	58	Theorem 5.1
59	Theorem 7.4	60	Theorem 5.1	61	Theorem 7.4
62	Theorem 5.1	63	Theorem 5.1	64	Theorem 7.4
65	Theorem 5.1	66	Theorem 5.1	67	Theorem 7.4
68	Theorem 5.1	69	Theorem 7.4	70	Theorem 5.1
71	Theorem 7.4	72	Theorem 5.1	73	Theorem 7.4
74	Theorem 5.1	75	Theorem 5.3	76	Theorem 5.1
77	Theorem 5.1	78	Theorem 5.1	79	Theorem 7.4
80	Theorem 5.1	82	Theorem 5.1	83	Theorem 7.4
84	Theorem 5.1	85	Theorem 5.1	86	Theorem 5.1
87	Theorem 5.1	88	Theorem 5.1	89	Theorem 7.4
90	Theorem 5.1	91	Theorem 5.1	92	Theorem 5.1
93	Theorem 7.5	94	Theorem 5.1	95	Theorem 5.1
96	Theorem 5.1	97	Theorem 7.4	98	Theorem 5.1
99	Theorem 5.1	100	Theorem 5.1		

Table 2: Nonexistence of abelian $(3n, n, 3n, 3)$ RDS for $2 \leq n \leq 100$ and $n \neq 3^a$

n	nonexistence	n	nonexistence	n	nonexistence
5	Theorem 7.6	6	Theorem 5.1	7	[6]
9	Theorem 7.6	10	Theorem 5.1	11	Theorem 7.6
12	?	13	Theorem 7.6	14	Theorem 5.1
15	Theorem 5.1	17	Theorem 7.6	18	Theorem 5.1
19	Theorem 7.6	20	?	21	Theorem 5.1
22	Theorem 5.1	23	Theorem 7.6	24	Theorem 5.1
25	Theorem 7.6	26	Theorem 5.1	27	Theorem 7.6
28	Lemma 5.6	29	Theorem 7.6	30	Theorem 5.1
31	Theorem 7.6	33	Theorem 5.1	34	Theorem 5.1
35	Theorem 5.1	36	Theorem 5.3	37	Theorem 7.6
38	Theorem 5.1	39	Theorem 5.3	40	Theorem 5.1
41	Theorem 7.6	42	Theorem 5.1	43	Theorem 7.6
44	Theorem 5.3	45	Theorem 5.1	46	Theorem 5.1
47	Theorem 7.6	48	?	49	?
50	Theorem 5.1	51	Theorem 5.1	52	Theorem 5.3
53	Theorem 7.6	54	Theorem 5.1	55	Theorem 5.3
56	Corollary 7.7	57	Theorem 5.1	58	Theorem 5.1
59	Theorem 7.6	60	Theorem 5.1	61	Theorem 7.6
62	Theorem 5.1	63	Corollary 7.7	65	Theorem 5.1
66	Theorem 5.1	67	Theorem 7.6	68	Theorem 5.1
69	Theorem 5.1	70	Theorem 5.1	71	Theorem 7.6
72	Theorem 5.1	73	Theorem 7.6	74	Theorem 5.1
75	Theorem 5.1	76	Theorem 5.3	77	Theorem 5.1
78	Theorem 5.1	79	Theorem 7.6	80	?
81	Theorem 7.6	82	Theorem 5.1	83	Theorem 7.6
84	Theorem 5.1	85	Theorem 5.1	86	Theorem 5.1
87	Theorem 5.1	88	Theorem 5.1	89	Theorem 7.6
90	Theorem 5.1	91	Theorem 5.1	92	Theorem 7.8
93	Theorem 5.1	94	Theorem 5.1	95	Theorem 5.3
96	Theorem 5.1	97	Theorem 7.6	98	?
99	Theorem 5.1	100	Theorem 5.3		

Table 3: Nonexistence of abelian $(4n, n, 4n, 4)$ RDS for $2 \leq n \leq 100$, $n \neq 3$ and $n \neq 2^a$