J Algebr Comb (2018) 48:565–579
https://doi.org/10.1007/s10801-017-0805-z

On (mn, n, mn, m) relative difference sets with $\gcd(m, n) = 1$

Tao Zhang[1] · **Gennian Ge**[1]

Received: 20 March 2017 / Accepted: 15 November 2017 / Published online: 27 November 2017

Abstract There has been much research on (p^a, p^b, p^a, p^{a-b}) relative difference sets with p a prime, while there are only a few results on (mn, n, mn, m) relative difference sets with $\gcd(m, n) = 1$. The non-existence results on (mn, n, mn, m) relative difference sets with $\gcd(m, n) = 1$ have only been obtained for the following five cases: (1) $m = p,\ n = q,\ p > q$; (2) $m = pq,\ n = 3,\ p, q > 3$; (3) $m = 4,\ n = p$; (4) $m = 2$ and (5) $n = p$, where p, q are distinct odd primes. For the existence results, there are only four constructions of semi-regular relative difference sets in groups of size not a prime power with the forbidden subgroup having size larger than 2. In this paper, we present some more non-existence results on (mn, n, mn, m) relative difference sets with $\gcd(m, n) = 1$. In particular, our result is a generalization of the main result of Hiramine's work (J Comb Theory Ser A 117(7):996–1003, 2010). Meanwhile, we give a construction of non-abelian $(16q, q, 16q, 16)$ relative difference sets, where q is a prime power with $q \equiv 1 \pmod 4$ and $q > 4.2 \times 10^8$. This is the third known infinite classes of non-abelian semi-regular relative difference sets.

Keywords Relative difference set · Semi-regular relative difference set · Self-conjugate

Mathematics Subject Classification 05B10

Research supported by the National Natural Science Foundation of China under Grant Nos. 11431003 and 61571310, Beijing Scholars Program, Beijing Hundreds of Leading Talents Training Project of Science and Technology and Beijing Municipal Natural Science Foundation.

✉ Gennian Ge
gnge@zju.edu.cn

[1] School of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China

1 Introduction

Let G be a finite group of order uv, and let N be a subgroup of G of order v. A k subset D of G is called a (u, v, k, λ) *relative difference set* (RDS) in G relative to N if the multiset of differences $r_1 r_2^{-1}$ for $r_1, r_2 \in D$, $r_1 \neq r_2$, contains every element of $G \backslash N$ exactly λ times and contains no element of N. If the group G is abelian (resp. non-abelian), then D is called an abelian (resp. non-abelian) RDS. If $k = v\lambda$, then D is called semi-regular RDS.

There has been extensive research on (p^a, p^b, p^a, p^{a-b}) RDSs with p a prime, see [14–16] and the references therein. In this paper, we focus on (mn, n, mn, m) RDSs with $\gcd(m, n) = 1$. Research works on semi-regular RDSs involve both existence and non-existence results. For the non-existence results, Ma showed that there is no abelian (pq, q, pq, p) RDS with p, q being two distinct odd primes such that $p > q$ in [13]. In [12], 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. In [6], Feng and Xiang proved that there does not exist a $(2p, p, 2p, 2)$ RDS with p an odd prime and there does not exist an abelian $(4p, p, 4p, 4)$ RDS with $p > 4$ an odd prime. Later, Hiramine [8] generalized one of Feng–Xiang's results and proved that if an abelian $(2n, n, 2n, 2)$ RDS exists, then n is a power of 2 except for a few special cases. In [5], Feng gave some non-existence and structural results on (pm, p, pm, m) RDS with p an odd prime and $\gcd(p, m) = 1$ through a group ring approach. For the existence results, most known semi-regular RDSs have parameters (p^a, p^b, p^a, p^{a-b}) with p a prime. To the best of our knowledge, there are only four constructions of semi-regular RDSs in groups of size not a prime power with the forbidden subgroup having size larger than 2. In [4,11], the authors constructed a family of relative difference sets with parameters $(p^{2t}(p+1), p+1, p^{2t}(p+1), p^{2t})$, where t is a positive integer and $p = 2$ or p is a Mersenne prime. In [6], Feng and Xiang constructed a family of non-abelian relative difference sets with parameters $(4q, q, 4q, 4)$, where q is an odd prime power with $q \equiv 1 \pmod 4$ and $q > 9$. In [5], Feng gave a construction of $(p(p+1), p, p(p+1), p+1)$ RDSs, where p is a Mersenne prime.

Semi-regular relative difference sets not only have their own interest, but also have applications in mutually unbiased bases. In [7], the authors proved that if there exists a semi-regular (mn, n, mn, m) RDS in an abelian group, then there exists a set of $n+1$ mutually unbiased bases of $\mathbb{C}^{mn}$. It is also known that [10,18] there are at least $\min_{p|d}\{v_p(d) + 1\}$ mutually unbiased bases of $\mathbb{C}^d$, where p is a prime and $v_p(d)$ denotes p^a such that $p^a | d$ and $p^{a+1} \nmid d$. Motivated by the above connection, it is natural to ask the following question: Does there exist an abelian semi-regular relative difference set with parameters $(m, n, m, m/n)$ satisfying $n > \min_{p|m}\{v_p(m)\}$?

In this paper, we give some non-existence results on (mn, n, mn, m) relative difference sets with $\gcd(m, n) = 1$. We also construct a family of non-abelian $(16q, q, 16q, 16)$ relative difference sets, where q is a prime power with $q \equiv 1 \pmod 4$ and $q > 4.2 \times 10^8$. This paper is organized as follows. In Sect. 2, we give some basic facts about relative difference sets, group rings and number theory. In Sect. 3, we prove some non-existence results on abelian relative difference sets. In Sect. 4, we construct a family of non-abelian relative difference sets.

2 Preliminaries

2.1 Relative difference sets and group rings

The following lemma is very useful in the study of semi-regular relative difference sets.

Lemma 2.1 [15] *Let R be an abelian $(m, n, m, m/n)$ RDS in G relative to N. Then $exp(G)|m$ or $G = \mathbb{Z}_4$, $n = 2$.*

Let G be a finite group. The group ring $\mathbb{Z}[G]$ is a free abelian group with a basis $\{g \mid g \in G\}$, and the multiplication as a ring is inherited from the operation in G. For any set A whose elements belong to G (A may be a multiset), we identify A with the group ring element $\sum_{g\in G} d_g g$, where d_g is the multiplicity of g appeared in A. Set $A^{(-1)} = \{x^{-1} \mid x \in A\}$. Then an (m, n, k, λ) relative difference set D in G with forbidden group N can be expressed in a succinct way:

$$DD^{(-1)} = k1_G + \lambda(G - N),$$

where 1_G is the identity of group G.

For a finite abelian group G, denote its character group by $\widehat{G}$. For any $A = \sum_{g\in G} d_g g$ and $\chi \in \widehat{G}$, 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 $\widehat{G}$.

Lemma 2.2 *Let G be an abelian group. If $A = \sum_{g\in G} d_g g \in \mathbb{Z}[G]$, then*

$$d_h = \frac{1}{|G|} \sum_{\chi\in\widehat{G}} \chi(A)\chi\left(h^{-1}\right),$$

for all $h \in G$.

2.2 Number theoretic background

For a positive integer m, we denote by ζ_m a primitive m-th root of unity in $\mathbb{C}$.

Definition 2.3 Let $m = p^a m'$ with $\gcd(p, m') = 1$. Then p is called self-conjugate modulo m if there exists an integer j such that $p^j \equiv -1 \pmod{m'}$. A composite integer n is called self-conjugate modulo m if every prime divisor of n is self-conjugate modulo m.

A proof of the following result can be found in [17, Thoerem 1.4.3], for instance.

Lemma 2.4 *Let p be a prime, $m = p^a m'$ be an integer with $p \nmid m'$. Let P be a prime ideal above p in $\mathbb{Z}[\zeta_m]$. If $\sigma \in Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ satisfies $\sigma(\zeta_{m'}) = \zeta_{m'}^{p^j}$ for some positive integer j, then $\sigma(P) = P$.*

Then we have the following corollary.

Corollary 2.5 *Let p be a prime, $m = p^a m'$ be an integer with $p \nmid m'$. Then the decomposition group of p in $\mathbb{Q}(\zeta_m)/Q$ contains $\overline{\sigma_m} : \zeta_m \to \zeta_m^{-1}$ if p is self-conjugate modulo m.*

The following lemma can be found in [17, Lemma 2.1.2].

Lemma 2.6 *Let $a \in \mathbb{Z}[\zeta_m]$ be a solution of $x\overline{x} = n$, where n is a positive integer. If $\sigma \in Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ fixes all primes above n in $\mathbb{Q}(\zeta_m)$, then $\sigma(a) = \varepsilon a$ for some root of unity ε.*

Let τ be a solution of $x\overline{x} = 2$ in $\mathbb{Z}[\zeta_n]$, where n is an odd integer. Let ρ be any prime ideal above τ, then $\rho|\tau$ and $\overline{\rho}|\overline{\tau}$. If $\rho = \overline{\rho}$, then 2 is ramified in $\mathbb{Z}[\zeta_n]$, which is a contradiction. Hence $\rho \neq \overline{\rho}$, and we have a factorization $(2) = \rho_1 \dots \rho_r \overline{\rho_1} \dots \overline{\rho_r}$. Set $\overline{\rho_i} = \rho_{i+r}$. Then $(\tau) = \rho_{i_1} \dots \rho_{i_r}$ and $(\overline{\tau}) = \rho_{i_1+r} \dots \rho_{i_r+r}$, the set $\{i_1, \dots, i_r\}$ is called *the type of the element* τ. We have the following lemma.

Lemma 2.7 [9] *Let τ_1 and τ_2 be two solutions of $x\overline{x} = 2$ in $\mathbb{Z}[\zeta_n]$, where n is an odd integer. Then they are at the same type if and only if they differ by a root of unity.*

3 Non-existence results for semi-regular relative difference sets

In this section, we prove some non-existence results on (mn, n, mn, m) relative difference sets with $\gcd(m, n) = 1$.

Theorem 3.1 *Let m, n be integers with $gcd(m, n) = 1$. Suppose m, n satisfy one of the following conditions:*

1. *$m = 2^l m'$, l and m' are odd integers, and 2 is self-conjugate modulo n.*
2. *$m = 2p$, $p = 1$ or p is an odd prime, and pn is self-conjugate modulo pn.*
3. *m is an odd prime and mn is self-conjugate modulo mn.*

Then there does not exist an (mn, n, mn, m) RDS in abelian group $G = \mathbb{Z}_m \times H$, where H is an abelian group with order n^2. In particular, if m is a squarefree integer, then there does not exist an abelian (mn, n, mn, m)-RDS.

Proof Let $G = \langle g \rangle \times H$, where $|H| = n^2$ and $g^m = 1$. Assume D is an (mn, n, mn, m) RDS in abelian group G relative to a subgroup N of G with order n. Since $\gcd(m, n) = 1$, we may assume $N \subseteq H$. Then

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

Write $D = D_0 + D_1 g + \cdots + D_{m-1} g^{m-1} \in \mathbb{Z}[G]$, where $D_i \subseteq H, 0 \leq i \leq m-1$. Note that $|D||N| = |G|$ and if there exist $d_1, d_2 \in D$ and $n_1, n_2 \in N$ such that $d_1 n_1 = d_2 n_2$, then $n_1/n_2 = d_2/d_1 \in N$ since N is a subgroup. Hence $d_1 = d_2$ and $n_1 = n_2$. Thus $DN = G$. It follows that $(D_0 + D_1 g + \cdots + D_{m-1} g^{m-1})N = H + Hg + \cdots + Hg^{m-1}$. Then we have

$$D_0N = D_1N = \cdots = D_{m-1}N = H, \tag{2}$$
$$|D_0| = |D_1| = \cdots = |D_{m-1}| = n. \tag{3}$$

By Eq. (1), we obtain

$$\begin{aligned} DD^{(-1)} &= \left(D_0 + D_1 g + \cdots + D_{m-1} g^{m-1}\right) \\ &\quad \left(D_0^{(-1)} + D_1^{(-1)} g^{m-1} + \cdots + D_{m-1}^{(-1)} g\right) \\ &= mn + m(H - N) + mHg + \cdots + mHg^{m-1}. \end{aligned}$$

It follows that

$$\sum_{i=0}^{m-1} D_i D_i^{(-1)} = mn + m(H - N), \tag{4}$$
$$\sum_{i=0}^{m-1} D_i D_{i+k}^{(-1)} = mH, \text{ for } 1 \le k \le m-1, \tag{5}$$

where the subscripts are reduced modulo m.

Let χ be a non-trivial character of group H. If $\chi|_N = 1$, then by Eq. (2), $\chi(D_0) = \chi(D_1) = \cdots = \chi(D_{m-1}) = 0$.

In the following, we assume $\chi|_N \ne 1$. Set $\chi(D_i) = \eta_i$ $(0 \le i \le m-1)$. By Lemma 2.1, $\exp(G)|mn$, then $\exp(H)|n$, and so $\eta_i \in \mathbb{Z}[\zeta_n]$. From Eqs. (4) and (5), the following hold

$$\sum_{i=0}^{m-1} \eta_i \overline{\eta_i} = mn, \tag{6}$$
$$\sum_{i=0}^{m-1} \eta_i \overline{\eta_{i+k}} = 0, \text{ for } 1 \le k \le m-1, \tag{7}$$

where the subscripts are reduced modulo m. Computing Eq. (6) $+ \zeta_m^{-j} \cdot$ (the first equation of Eq. (7)) $+ \cdots + \zeta_m^{-j(m-1)} \cdot$ (the $(m-1)$-st equation of Eq. (7)) for $0 \le j \le m-1$, we have

$$\left(\sum_{i=0}^{m-1} \zeta_m^{ij} \eta_i\right) \left(\overline{\sum_{i=0}^{m-1} \zeta_m^{ij} \eta_i}\right) = mn, \ 0 \le j \le m-1.$$

Denote $A_j = \sum_{i=0}^{m-1} \zeta_m^{ij} \eta_i$, then $A_j \overline{A_j} = mn$ and $A_j \in \mathbb{Z}[\zeta_{mn}]$ for $0 \le j \le m-1$. Below, we split our discussion into three cases according to the conditions of our theorem.

Case 1 $m = 2^l m'$, l and m' are odd integers, and 2 is self-conjugate modulo n.

Note that $A_0 \in \mathbb{Z}[\zeta_n]$. Let P be any prime ideal above 2 in $\mathbb{Z}[\zeta_n]$. Since 2 is self-conjugate modulo n, by Corollary 2.5, we have $\sigma_{-1}(P) = P$. Let $v_P(a)$ denote the largest number i such that $P^i|a$. Let $v_P(A_0) = t$, then $v_P(\overline{A_0}) = t$. Hence $v_P(mn) = v_P(A_0) + v_P(\overline{A_0}) = 2t$. Note that 2 is unramified in $\mathbb{Q}(\zeta_n)$, we have $v_P(mn) = v_P(2^l) = l$ is odd, which is a contradiction.

Case 2 $m = 2p$, $p = 1$ or p is an odd prime, and pn is self-conjugate modulo pn.

Note that pn is self-conjugate modulo pn. By Corollary 2.5, $\sigma_{-1} : \zeta_{pn} \to \zeta_{pn}^{-1}$ fixes all prime ideals above pn. Let $pn = \prod_{i=1}^r p_i^{e_i}$, where p_i, $1 \le i \le r$ are primes. Let $\omega_{pn} = \prod_{i=1}^r (\sqrt{(-1)^{\frac{p_i-1}{2}} p_i})^{e_i}$, then $\omega_{pn} \in \mathbb{Z}[\zeta_{pn}] = \mathbb{Z}[\zeta_{2pn}]$ and $\overline{\omega_{pn}}\omega_{pn} = pn$. For any $i \in \{1, 2, \cdots, r\}$, the principal ideal $(1 - \zeta_{p_i^{e_i}})$ is a prime ideal in $\mathbb{Z}[\zeta_{p_i^{e_i}}]$ and $(p_i) = (1 - \zeta_{p_i^{e_i}})^{\varphi(p_i^{e_i})}$, $(\sqrt{(-1)^{\frac{p_i-1}{2}} p_i}) = (1 - \zeta_{p_i^{e_i}})^{\frac{\varphi(p_i^{e_i})}{2}}$. Since the prime ideal $(1 - \zeta_{p_i^{e_i}})$ lying over p_i in $\mathbb{Z}[\zeta_{p_i^{e_i}}]$ is decomposed into prime ideals in $\mathbb{Z}[\zeta_{pn}]$ without ramification, we can write the prime ideal factorization of p_i in $\mathbb{Z}[\zeta_{pn}]$ as: $(p_i) = (\prod_\lambda \varrho_{i,\lambda})^{\varphi(p_i^{e_i})}$, where all prime ideals $\varrho_{i,\lambda}$ are distinct and $\overline{\varrho_{i,\lambda}} = \varrho_{i,\lambda}$. Then we have $(pn) = \prod_{i=1}^r (\prod_\lambda \varrho_{i,\lambda})^{\varphi(p_i^{e_i})e_i}$ and $(\omega_{pn}) = \prod_{i=1}^r (\prod_\lambda \varrho_{i,\lambda})^{\frac{\varphi(p_i^{e_i})e_i}{2}}$.

Note that $A_j\overline{A_j} = mn = 2pn$ and $A_j \in \mathbb{Z}[\zeta_{pn}]$ for $0 \le j \le m-1$. Then comparing the prime ideal factorizations of both sides, and taking into account that a prime ideal above pn in $\mathbb{Z}[\zeta_{pn}]$ exactly divides A_j with an exponent, and consequently it equally divides $\overline{A_j}$ with the same exponent, we deduce that $A_j \in (\omega_{pn})$. Hence there is an algebraic integer $B_j \in \mathbb{Z}[\zeta_{pn}]$ such that $A_j = B_j\omega_{pn}$ and $B_j\overline{B_j} = 2$.

Note that $A_j = \sum_{i=0}^{m-1} \zeta_m^{ij}\eta_i$ for $0 \le j \le m-1$. Then

$$A_j + A_{j+p} = 2\sum_{i=0}^{p-1} \zeta_m^{2ij}\eta_{2i} = \omega_{pn}(B_j + B_{j+p}).$$

If B_j and B_{j+p} are not of the same type, then there is a prime ideal above 2 dividing B_j but not B_{j+p}, which is a contradiction. Hence B_j and B_{j+p} are of the same type for $0 \le j \le p-1$. By Lemma 2.7, they differ by a root of unity. Assume $B_{j+p} = \mu_j B_j$, where $\mu_j \in \mathbb{Z}[\zeta_{pn}]$ is a root of unity. Note that

$$A_j - A_{j+p} = 2\sum_{i=0}^{p-1} \zeta_m^{(2i+1)j}\eta_{2i+1} = \omega_{pn}B_j(1 - \mu_j).$$

Then

$$\overline{B_j}\sum_{i=0}^{p-1} \zeta_m^{(2i+1)j}\eta_{2i+1} = \omega_{pn}(1 - \mu_j),$$

so $\overline{B_j}|(1-\mu_j)$. Assume μ_j is a primitive l-th root of unity. If l has at least two distinct prime factors, then $1 - \mu_j$ is a unit, which is a contradiction. If l is a power of a prime

$q|(pn)$, then $(1-\mu_j)|q$, which is also a contradiction. Therefore $l = 1$ or 2. That is $A_{j+p} = A_j$ or $A_{j+p} = -A_j$ for $0 \le j \le p-1$.

If $p = 1$, then it is easy to get that $\eta_0 = 0$ or $\eta_1 = 0$.

If $p > 1$, set

$$S_1 = \{j : 0 \le j \le p-1, A_{j+p} = A_j\},$$
$$S_2 = \{j : 0 \le j \le p-1, A_{j+p} = -A_j\}.$$

Note that $S_1 \bigcup S_2 = \{0, 1, \cdots, p-1\}$. If $S_1 = \{0\}$, then $A_0 = A_p$ and $A_1 = -A_{p+1}$. It follows that

$$\sum_{i=0}^{p-1} \eta_{2i+1} = 0 \text{ and } \sum_{i=0}^{p-1} \zeta_m^{2i} \eta_{2i} = 0.$$

Since $m = 2p$ and p is an odd prime, we have $\eta_0 = \eta_2 = \cdots = \eta_{2p-2}$. Then $A_0 = p\eta_0$. Therefore $A_0\overline{A_0} = p^2\eta_0\overline{\eta_0} = 2pn$, which contradicts the fact that $\gcd(p, 2n) = 1$. Similarly for the case $S_2 = \{0\}$. Hence if $0 \in S_i$, then $|S_i| \ge 2$.

If $0, t \in S_1$ for some $1 \le t \le p-1$, then

$$\sum_{i=0}^{p-1} \eta_{2i+1} = 0,$$
$$\sum_{i=0}^{p-1} \zeta_{2p}^{t(2i+1)} \eta_{2i+1} = 0.$$

This forces $\eta_1 = \eta_3 = \cdots = \eta_{m-1} = 0$. Similarly, if $0, t \in S_2$ for some $1 \le t \le p-1$, then we have $\eta_0 = \eta_2 = \cdots = \eta_{m-2} = 0$.

Therefore we have proved that for any $i \in \{0, 2, \cdots, 2p-2\}$, $j \in \{1, 3, \cdots, 2p-1\}$ and any non-trivial character χ of H, $\chi(D_i D_j) = 0$. By Lemma 2.2, we can compute to get that $D_i D_j = H$. Set $W_k = \text{supp}(D_k D_k^{(-1)})$, $k = 0, 1, \cdots, m-1$, where $\text{supp}(\sum_{h\in H} a_h h) = \{h : a_h \ne 0\}$ for $\sum_{h\in H} a_h h \in \mathbb{Z}[H]$. Assume there exists non-identity element $h \in W_i \cap W_j$. Then $h = ab^{-1} = cd^{-1}$ for some elements $a, b \in D_i$ and $c, d \in D_j$. As $ad = bc$ and $D_i D_j = H$, we have $a = b$ and $c = d$, which is contrary to the choice of h. Thus $W_i \cap W_j = \{1\}$. By Eq. (4), there exists a partition $H - N = T_1 \cup T_2$ satisfying $\sum_{i=0}^{p} D_{2i} D_{2i}^{(-1)} = pn + mT_1$ and $\sum_{i=0}^{p} D_{2i+1} D_{2i+1}^{(-1)} = pn + mT_2$. Since there exists some character χ of H such that $\chi(D_i) = 0$ for $i = 0, 2, \cdots, m-2$ or $\chi(D_i) = 0$ for $i = 1, 3, \cdots, m-1$, we have $pn = -m\chi(T_i)$ for some $i \in \{1, 2\}$. Then $n = -2\chi(T_i)$, which is a contradiction.

Case 3 m is an odd prime and mn is self-conjugate modulo mn.

The discussion is similar as that of Case 2; we skip the proof. (In this case, we need Lemmas 2.4 and 2.6.) □

Remark 3.2 Let $m = 2$, $n = p^r$ be an odd prime power. Applying Theorem 3.1 (condition 2), there does not exist an abelian $(2p^r, p^r, 2p^r, 2)$-RDS. This result was obtained in [8].

4 A family of non-abelian $(16q, q, 16q, 16)$ relative difference sets

In this section, we construct a family of $(16q, q, 16q, 16)$ RDSs in certain non-abelian groups of order $16q^2$, where q is an odd prime power, $q \equiv 1 \pmod 4$ and $q > 4.2 \times 10^8$.

Our construction is based on Weil's theorem. Given a prime power $q \equiv 1 \pmod r$ and a primitive element $g \in \mathbb{F}_q$, we use C_0^r to denote the multiplicative subgroup $\{g^{ir} : 0 \le i < (q-1)/r\}$, and C_j^r to denote the coset of C_0^r in $\mathbb{F}_q$, i.e., $C_j^r = g^j \cdot C_0^r$, $0 \le j < r$. Here is an application of Weil's theorem on multiplicative character sums, which can be found in [2,3].

Lemma 4.1 *Let $q \equiv 1 \pmod r$ be a prime power satisfying the inequality*

$$q - \left[\sum_{i=0}^{l-2} \binom{l}{i}(l-i-1)(r-1)^{l-i}\right]\sqrt{q} - lr^{l-1} > 0.$$

Then, for any given l-tuple $(j_1, j_2, \ldots, j_l) \in [0, r-1]^l$ and any given l-tuple $(c_1, c_2, \ldots, c_l)$ of pairwise distinct elements of $\mathbb{F}_q$, there exists an element $x \in \mathbb{F}_q$ such that $x + c_i \in C_{j_i}^r$ for each $i \in [1, l]$.

For a prime power $q = p^n, n \ge 1$, p an odd prime, let $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$, $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ be the absolute trace function. The quadratic character η on $\mathbb{F}_q$ is defined by

$$\eta(x) = \begin{cases} 1, & \text{if } x \text{ is a nonzero square of } \mathbb{F}_q; \\ 0, & \text{if } x = 0; \\ -1, & \text{if } x \text{ is a non-square of } \mathbb{F}_q. \end{cases}$$

For $u \in \mathbb{F}_q^*$, we define

$$S(u) := \sum_{x \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}(ux^2)}.$$

Then it is easy to see that $S(u) = \eta(u)S(1)$ and $S(1)\overline{S(1)} = q$.

In the rest of this section we assume that $q \equiv 1 \pmod 4$, $e \in \mathbb{F}_q$ satisfying $e^2 = -1$. Given two elements $s_2, s_8 \in \mathbb{F}_q^*$, we define

$$s_1 = \frac{1+e}{2} + \frac{1-e}{2}s_2, \quad s_3 = \frac{1-e}{2} + \frac{1+e}{2}s_2, \quad s_4 = \frac{1+e}{2} + \frac{1-e}{2}s_8,$$

$$s_5 = \frac{1-e}{2}s_2 + \frac{1+e}{2}s_8, \quad s_6 = \frac{1-e}{2} + s_2 + \frac{e-1}{2}s_8, \quad s_7 = 1 + \frac{1+e}{2}s_2 + \frac{-1-e}{2}s_8,$$

$$s_9 = \frac{1-e}{2} + \frac{1-e}{2}s_2 + es_8, \quad s_{10} = 1 + s_2 - s_8, \quad s_{11} = \frac{1+e}{2} + \frac{1+e}{2}s_2 - es_8,$$

$$s_{12} = \frac{1-e}{2} + \frac{1+e}{2}s_8, \quad s_{13} = 1 + \frac{1-e}{2}s_2 + \frac{e-1}{2}s_8, \quad s_{14} = \frac{1+e}{2} + s_2 + \frac{-1-e}{2}s_8,$$

$$s_{15} = \frac{1+e}{2}s_2 + \frac{1-e}{2}s_8.$$

Lemma 4.2 *If $q > 4.2 \times 10^8$, then there exist $s_2, s_8 \in \mathbb{F}_q^*$ such that*

$$\eta(s_1) = \eta(s_2) = \eta(s_4) = \eta(s_5) = \eta(s_6) = \eta(s_8) = \eta(s_9) = \eta(s_{10}) = \eta(s_{15}) = 1,$$
$$\eta(s_3) = \eta(s_7) = \eta(s_{11}) = \eta(s_{12}) = \eta(s_{13}) = \eta(s_{14}) = -1.$$

Proof If $\frac{1-e}{2}, \frac{1+e}{2}, e \in C_0^2$, then the condition $\eta(s_1) = 1, \eta(s_3) = -1$, is equivalent to $\frac{2}{1-e}s_1 = \frac{1+e}{1-e} + s_2 \in C_0^2$ and $\frac{2}{1+e}s_3 = \frac{1-e}{1+e} + s_2 \in C_1^2$. Since $0, \frac{1+e}{1-e}, \frac{1-e}{1+e}$ are distinct elements in $\mathbb{F}_q$, applying Lemma 4.1 with $r = 2, l = 3, (j_1, j_2, j_3) = (0, 0, 1)$ and $(c_1, c_2, c_3) = (0, \frac{1+e}{1-e}, \frac{1-e}{1+e})$, we can find $s_2 \in \mathbb{F}_q^*$ such that $s_1, s_2 \in C_0^2$ and $s_3 \in C_1^2$ for any odd prime power $q > 4.2 \times 10^8$. Once the element s_2 has been determined, we can take $l = 12$ and $r = 2$ in Lemma 4.1; then, it is easy to obtain that

$$q - \left[\sum_{i=0}^{10} \binom{12}{i}(11-i)\right]\sqrt{q} - 12 \times 2^{11} > 0,$$

hence we can obtain the required element s_8 for any odd prime power $q > 4.2 \times 10^8$. For the other cases of $\frac{1-e}{2}, \frac{1+e}{2}, e$, the proof is similar. □

Set $s_0 := 1$, then from the definition of s_i $(0 \le i \le 15)$, we have the following lemma.

Lemma 4.3 (1) $\frac{s_0-s_2}{s_1-s_3} = \frac{s_1-s_3}{s_2-s_0} = \frac{s_4-s_6}{s_5-s_7} = \frac{s_5-s_7}{s_6-s_4} = \frac{s_8-s_{10}}{s_9-s_{11}} = \frac{s_9-s_{11}}{s_{10}-s_8} = \frac{s_{12}-s_{14}}{s_{13}-s_{15}} = \frac{s_{13}-s_{15}}{s_{14}-s_{12}} = \frac{1}{e}$;

(2) $s_0 + s_2 = s_1 + s_3,\ s_4 + s_6 = s_5 + s_7,\ s_8 + s_{10} = s_9 + s_{11},\ s_{12} + s_{14} = s_{13} + s_{15}$;

(3) $\frac{s_0-s_8}{s_4-s_{12}} = \frac{s_1-s_9}{s_5-s_{13}} = \frac{s_2-s_{10}}{s_6-s_{14}} = \frac{s_3-s_{11}}{s_7-s_{15}} = \frac{s_4-s_{12}}{s_8-s_0} = \frac{s_5-s_{13}}{s_9-s_1} = \frac{s_6-s_{14}}{s_{10}-s_2} = \frac{s_7-s_{15}}{s_{11}-s_3} = \frac{1}{e}$;

(4) $s_0 + s_5 = s_8 + s_{13},\ s_1 + s_6 = s_9 + s_{14},\ s_2 + s_7 = s_{10} + s_{15},\ s_3 + s_4 = s_{11} + s_{12},\ s_4 + s_9 = s_{12} + s_1,\ s_5 + s_{10} = s_{13} + s_2,\ s_6 + s_{11} = s_{14} + s_3,\ s_7 + s_8 = s_{15} + s_0$;

(5) $\frac{s_0-s_8}{s_{14}-s_6} = \frac{s_1-s_9}{s_{15}-s_7} = \frac{s_2-s_{10}}{s_{12}-s_4} = \frac{s_3-s_{11}}{s_{13}-s_5} = \frac{s_4-s_{12}}{s_2-s_{10}} = \frac{s_5-s_{13}}{s_3-s_{11}} = \frac{s_6-s_{14}}{s_0-s_8} = \frac{s_7-s_{15}}{s_1-s_9} = \frac{1}{e}$;

(6) $s_0+s_2 = s_5+s_7,\ s_1+s_3 = s_4+s_6,\ s_4+s_6 = s_9+s_{11},\ s_5+s_7 = s_8+s_{10},\ s_8+s_{10} = s_{13} + s_{15},\ s_9 + s_{11} = s_{12} + s_{14}, s_{12} + s_{14} = s_1 + s_3, s_{13} + s_{15} = s_0 + s_2$;

(7) $s_0 + s_8 = s_4 + s_{12},\ s_1 + s_9 = s_5 + s_{13},\ s_2 + s_{10} = s_6 + s_{14},\ s_3 + s_{11} = s_7 + s_{15}$;

(8) $\frac{s_0-s_4}{s_{13}-s_9} = \frac{s_1-s_5}{s_{14}-s_{10}} = \frac{s_2-s_6}{s_{15}-s_{11}} = \frac{s_3-s_7}{s_{12}-s_8} = \frac{s_8-s_{12}}{s_5-s_1} = \frac{s_9-s_{13}}{s_6-s_2} = \frac{s_{10}-s_{14}}{s_7-s_3} = \frac{s_{11}-s_{15}}{s_4-s_0} = \frac{1}{e}$;

(9) $s_{10} - s_0 = s_{14} - s_4,\ s_{11} - s_1 = s_{15} - s_5,\ s_8 - s_2 = s_{12} - s_6,\ s_9 - s_3 = s_{13} - s_7$.

With $e, s_i \in \mathbb{F}_q^*$, $(1 \le i \le 15)$ as above. Let $H = \mathbb{F}_q \times \mathbb{F}_q$, $N = \{0\} \times \mathbb{F}_q \le H$, and

$$G = \langle x, y, H : x^4 = y^4 = 1, xy = yx, (u, v)^x = (u, ev), (u, v)^y = (u, ev) \text{ for any } (u, v) \in H\rangle,$$

where $(u, v)^x$ stands for $x^{-1}(u, v)x$. Define

$$D := \sum_{i=0}^{3}\sum_{j=0}^{3} D_{4j+i}x^i y^j \in \mathbb{Z}[G],$$

where $D_i = \{(z, \frac{1}{s_i} z^2) : z \in \mathbb{F}_q\}$.

Theorem 4.4 *Let q be a prime power such that $q \equiv 1 \pmod 4$ and $q > 4.2 \times 10^8$. Then D is a $(16q, q, 16q, 16)$ RDS in G relative to N.*

Proof To prove the theorem, we will show that

$$DD^{(-1)} = 16q + 16(G - N). \tag{8}$$

Define $D_i^{(-x^j y^k)} = \sum_{d \in D_i} x^{-j} y^{-k} d^{-1} x^j y^k$. Note that by applying $h \to h^{-1}$ for any $h \in H$, we have

$$\begin{aligned}
&D_i D_j^{(-x)} \to x^3 D_j D_i^{(-x^3)} x^3, && D_i D_j^{(-y)} \to y^3 D_j D_i^{(-y^3)} y^3,\\
&D_i D_j^{(-xy)} \to x^3 y^3 D_j D_i^{(-x^3 y^3)} x^3 y^3, && D_i D_j^{(-x^2 y)} \to x^2 y^3 D_j D_i^{(-x^2 y^3)} x^2 y^3,\\
&D_i D_j^{(-x^3 y)} \to x y^3 D_j D_i^{(-x y^3)} x y^3, && D_i D_j^{(-x y^2)} \to x^3 y^2 D_j D_i^{(-x^3 y^2)} x^3 y^2.
\end{aligned}$$

Then Eq. (8) is equivalent to the following system of group ring equations in $\mathbb{Z}[H]$:

$$\sum_{i=0}^{15} D_i D_i^{(-1)} = 16q + 16(H - N), \tag{9}$$

$$\begin{aligned}
&D_0 D_1^{(-x)} + D_1 D_2^{(-x)} + D_2 D_3^{(-x)} + D_3 D_0^{(-x)} + D_4 D_5^{(-x)} + D_5 D_6^{(-x)}\\
&\quad + D_6 D_7^{(-x)} + D_7 D_4^{(-x)} + D_8 D_9^{(-x)} + D_9 D_{10}^{(-x)} + D_{10} D_{11}^{(-x)}\\
&\quad + D_{11} D_8^{(-x)} + D_{12} D_{13}^{(-x)} + D_{13} D_{14}^{(-x)} + D_{14} D_{15}^{(-x)} + D_{15} D_{12}^{(-x)} = 16H,
\end{aligned} \tag{10}$$

$$\begin{aligned}
&D_0 D_2^{(-x^2)} + D_1 D_3^{(-x^2)} + D_2 D_0^{(-x^2)} + D_3 D_1^{(-x^2)} + D_4 D_6^{(-x^2)} + D_5 D_7^{(-x^2)}\\
&\quad + D_6 D_4^{(-x^2)} + D_7 D_5^{(-x^2)} + D_8 D_{10}^{(-x^2)} + D_9 D_{11}^{(-x^2)} + D_{10} D_8^{(-x^2)}\\
&\quad + D_{11} D_9^{(-x^2)} + D_{12} D_{14}^{(-x^2)} + D_{13} D_{15}^{(-x^2)} + D_{14} D_{12}^{(-x^2)} + D_{15} D_{13}^{(-x^2)} = 16H,
\end{aligned} \tag{11}$$

$$\begin{aligned}
&D_0 D_4^{(-y)} + D_1 D_5^{(-y)} + D_2 D_6^{(-y)} + D_3 D_7^{(-y)} + D_4 D_8^{(-y)} + D_5 D_9^{(-y)}\\
&\quad + D_6 D_{10}^{(-y)} + D_7 D_{11}^{(-y)} + D_8 D_{12}^{(-y)} + D_9 D_{13}^{(-y)} + D_{10} D_{14}^{(-y)}\\
&\quad + D_{11} D_{15}^{(-y)} + D_{12} D_0^{(-y)} + D_{13} D_1^{(-y)} + D_{14} D_2^{(-y)} + D_{15} D_3^{(-y)} = 16H,
\end{aligned} \tag{12}$$

$$\begin{aligned}
&D_0 D_5^{(-xy)} + D_1 D_6^{(-xy)} + D_2 D_7^{(-xy)} + D_3 D_4^{(-xy)} + D_4 D_9^{(-xy)} + D_5 D_{10}^{(-xy)}\\
&\quad + D_6 D_{11}^{(-xy)} + D_7 D_8^{(-xy)} + D_8 D_{13}^{(-xy)} + D_9 D_{14}^{(-xy)} + D_{10} D_{15}^{(-xy)}\\
&\quad + D_{11} D_{12}^{(-xy)} + D_{12} D_1^{(-xy)} + D_{13} D_2^{(-xy)} + D_{14} D_3^{(-xy)} + D_{15} D_0^{(-xy)} = 16H,
\end{aligned} \tag{13}$$

$$\begin{aligned}
&D_0 D_6^{(-x^2 y)} + D_1 D_7^{(-x^2 y)} + D_2 D_4^{(-x^2 y)} + D_3 D_5^{(-x^2 y)} + D_4 D_{10}^{(-x^2 y)}\\
&\quad + D_5 D_{11}^{(-x^2 y)} + D_6 D_8^{(-x^2 y)} + D_7 D_9^{(-x^2 y)} + D_8 D_{14}^{(-x^2 y)} + D_9 D_{15}^{(-x^2 y)}
\end{aligned}$$

$$
\begin{aligned}
&+ D_{10}D_{12}^{(-x^2y)} + D_{11}D_{13}^{(-x^2y)} + D_{12}D_{2}^{(-x^2y)} + D_{13}D_{3}^{(-x^2y)} + D_{14}D_{0}^{(-x^2y)} \\
&+ D_{15}D_{1}^{(-x^2y)} = 16H, \qquad (14) \\
&D_0D_7^{(-x^3y)} + D_1D_4^{(-x^3y)} + D_2D_5^{(-x^3y)} + D_3D_6^{(-x^3y)} + D_4D_{11}^{(-x^3y)} \\
&+ D_5D_8^{(-x^3y)} + D_6D_9^{(-x^3y)} + D_7D_{10}^{(-x^3y)} + D_8D_{15}^{(-x^3y)} + D_9D_{12}^{(-x^3y)} \\
&+ D_{10}D_{13}^{(-x^3y)} + D_{11}D_{14}^{(-x^3y)} + D_{12}D_{3}^{(-x^3y)} + D_{13}D_{0}^{(-x^3y)} + D_{14}D_{1}^{(-x^3y)} \\
&+ D_{15}D_{2}^{(-x^3y)} = 16H, \qquad (15) \\
&D_0D_8^{(-y^2)} + D_1D_9^{(-y^2)} + D_2D_{10}^{(-y^2)} + D_3D_{11}^{(-y^2)} + D_4D_{12}^{(-y^2)} \\
&+ D_5D_{13}^{(-y^2)} + D_6D_{14}^{(-y^2)} + D_7D_{15}^{(-y^2)} + D_8D_{0}^{(-y^2)} + D_9D_{1}^{(-y^2)} + D_{10}D_{2}^{(-y^2)} \\
&+ D_{11}D_{3}^{(-y^2)} + D_{12}D_{4}^{(-y^2)} + D_{13}D_{5}^{(-y^2)} + D_{14}D_{6}^{(-y^2)} + D_{15}D_{7}^{(-y^2)} = 16H, \qquad (16) \\
&D_0D_9^{(-xy^2)} + D_1D_{10}^{(-xy^2)} + D_2D_{11}^{(-xy^2)} + D_3D_{8}^{(-xy^2)} + D_4D_{13}^{(-xy^2)} \\
&+ D_5D_{14}^{(-xy^2)} + D_6D_{15}^{(-xy^2)} + D_7D_{12}^{(-xy^2)} + D_8D_{1}^{(-xy^2)} + D_9D_{2}^{(-xy^2)} \\
&+ D_{10}D_{3}^{(-xy^2)} + D_{11}D_{0}^{(-xy^2)} + D_{12}D_{5}^{(-xy^2)} + D_{13}D_{6}^{(-xy^2)} + D_{14}D_{7}^{(-xy^2)} \\
&+ D_{15}D_{4}^{(-xy^2)} = 16H, \qquad (17) \\
&D_0D_{10}^{(-x^2y^2)} + D_1D_{11}^{(-x^2y^2)} + D_2D_{8}^{(-x^2y^2)} + D_3D_{9}^{(-x^2y^2)} + D_4D_{14}^{(-x^2y^2)} \\
&+ D_5D_{15}^{(-x^2y^2)} + D_6D_{12}^{(-x^2y^2)} + D_7D_{13}^{(-x^2y^2)} + D_8D_{2}^{(-x^2y^2)} + D_9D_{3}^{(-x^2y^2)} \\
&+ D_{10}D_{0}^{(-x^2y^2)} + D_{11}D_{1}^{(-x^2y^2)} + D_{12}D_{6}^{(-x^2y^2)} + D_{13}D_{7}^{(-x^2y^2)} + D_{14}D_{4}^{(-x^2y^2)} \\
&+ D_{15}D_{5}^{(-x^2y^2)} = 16H. \qquad (18)
\end{aligned}
$$

In order to prove these equations, we will prove that the left-hand side and the right-hand side of these equations have the same character values for all characters of H. This can be checked easily for the principal character of H. In the following, we consider non-trivial character of H. Note that any non-trivial character χ of H can be written as

$$\chi_{g,h}(g', h') = \zeta_p^{\mathrm{Tr}(gg'+hh')}, \text{ for any } (g', h') \in H,$$

for some $(g, h) \in H$, $(g, h) \neq (0, 0)$.

If $h = 0$, then $\chi_{g,0}(D_i) = 0$ and $\chi_{g,0}$ is principal on N. It is easy to see that all equations above hold in this case.

If $h \neq 0$, then $\chi_{g,h}$ is non-principal on N and we can compute to get that

$$\chi_{g,h}(D_i) = \sum_{z\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}\left(gz+\frac{h}{s_i}z^2\right)}$$

$$
\begin{aligned}
&= \sum_{z\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}\left(\frac{h}{s_i}\left(z+\frac{s_i g}{2h}\right)^2-\frac{g^2 s_i}{4h}\right)} \\
&= \sum_{z\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}\left(\frac{h}{s_i}z^2\right)}\zeta_p^{-\mathrm{Tr}\left(\frac{g^2 s_i}{4h}\right)} \\
&= \eta(h)\eta(s_i)S(1)\zeta_p^{-\mathrm{Tr}\left(\frac{g^2 s_i}{4h}\right)}.
\end{aligned}
$$

It is easy to check that Eq. (9) holds in this case. The proofs of Eqs. (10)–(18) are similar; we will only prove Eqs. (10) and (13). Note that $\chi_{g,h}(16H) = 0$, we only need to prove that $\chi_{g,h}(\text{LHS of Eq. (10)}) = 0$ and $\chi_{g,h}(\text{LHS of Eq. (13)}) = 0$.

By Lemma 4.2, we have $\eta(s_0s_1s_2s_3) = \eta(s_4s_5s_6s_7) = \eta(s_8s_9s_{10}s_{11}) = \eta(s_{12}s_{13}s_{14}s_{15}) = -1$. By Lemma 4.3 (1), we can get that $\frac{g^2s_1}{4eh} - \frac{g^2s_0}{4h} = \frac{g^2s_3}{4eh} - \frac{g^2s_2}{4h}$. We can also compute to get that

$$
\begin{aligned}
\chi_{g,h}\left(D_i^{(-x)}\right) &= \chi_{g,h}\left(\sum_{d\in D_i} x^{-1}d^{-1}x\right) \\
&= \chi_{g,h}\left(\sum_{z\in\mathbb{F}_q}\left(-z,-\frac{e}{s_i}z^2\right)\right) \\
&= \sum_{z\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}\left(-gz-\frac{eh}{s_i}z^2\right)} \\
&= \overline{\chi_{g,eh}(D_i)} \\
&= \eta(eh)\eta(s_i)\overline{S(1)}\zeta_p^{\mathrm{Tr}\left(\frac{g^2 s_i}{4eh}\right)}.
\end{aligned}
$$

Hence we have

$$
\begin{aligned}
&\chi_{g,h}\left(D_0D_1^{(-x)}\right) + \chi_{g,h}\left(D_2D_3^{(-x)}\right) \\
&= \eta(h)\eta(s_0)S(1)\zeta_p^{-\mathrm{Tr}\left(\frac{g^2s_0}{4h}\right)}\eta(eh)\eta(s_1)\overline{S(1)}\zeta_p^{\mathrm{Tr}\left(\frac{g^2s_1}{4eh}\right)} \\
&\quad+\eta(h)\eta(s_2)S(1)\zeta_p^{-\mathrm{Tr}\left(\frac{g^2s_2}{4h}\right)}\eta(eh)\eta(s_3)\overline{S(1)}\zeta_p^{\mathrm{Tr}\left(\frac{g^2s_3}{4eh}\right)} \\
&= \eta(es_0s_1)q\zeta_p^{\mathrm{Tr}\left(\frac{g^2s_1}{4eh}-\frac{g^2s_0}{4h}\right)} + \eta(es_2s_3)q\zeta_p^{\mathrm{Tr}\left(\frac{g^2s_3}{4eh}-\frac{g^2s_2}{4h}\right)} \\
&= (\eta(es_0s_1)+\eta(es_2s_3))q\zeta_p^{\mathrm{Tr}\left(\frac{g^2s_1}{4eh}-\frac{g^2s_0}{4h}\right)} \\
&= 0.
\end{aligned}
$$

Similarly, we can prove that

$$\begin{aligned}
\chi_{g,h}\left(D_1 D_2^{(-x)}\right) + \chi_{g,h}\left(D_3 D_0^{(-x)}\right) &= 0,\\
\chi_{g,h}\left(D_4 D_5^{(-x)}\right) + \chi_{g,h}\left(D_6 D_7^{(-x)}\right) &= 0,\\
\chi_{g,h}\left(D_5 D_6^{(-x)}\right) + \chi_{g,h}\left(D_7 D_4^{(-x)}\right) &= 0,\\
\chi_{g,h}\left(D_8 D_9^{(-x)}\right) + \chi_{g,h}\left(D_{10} D_{11}^{(-x)}\right) &= 0,\\
\chi_{g,h}\left(D_9 D_{10}^{(-x)}\right) + \chi_{g,h}\left(D_{11} D_8^{(-x)}\right) &= 0,\\
\chi_{g,h}\left(D_{12} D_{13}^{(-x)}\right) + \chi_{g,h}\left(D_{14} D_{15}^{(-x)}\right) &= 0,\\
\chi_{g,h}\left(D_{13} D_{14}^{(-x)}\right) + \chi_{g,h}\left(D_{15} D_{12}^{(-x)}\right) &= 0.
\end{aligned}$$

Therefore, we have proved that $\chi_{g,h}(\text{LHS of Eq. (10)}) = 0$.

By Lemma 4.2, we have $\eta(s_0s_5s_8s_{13}) = \eta(s_1s_6s_9s_{14}) = \eta(s_2s_7s_{10}s_{15}) = \eta(s_3s_4s_{11}s_{12}) = \eta(s_4s_9s_{12}s_1) = \eta(s_5s_{10}s_{13}s_2) = \eta(s_6s_{11}s_{14}s_3) = \eta(s_7s_8s_{15}s_0) = -1$. By Lemma 4.3 (4), we can get that $\frac{g^2s_0}{4h} + \frac{g^2s_5}{4h} = \frac{g^2s_8}{4h} + \frac{g^2s_{13}}{4h}$. We can also compute to get that

$$\begin{aligned}
\chi_{g,h}\left(D_i^{(-xy)}\right) &= \chi_{g,h}\left(\sum_{d\in D_i} y^{-1}x^{-1}d^{-1}xy\right)\\
&= \chi_{g,h}\left(\sum_{z\in\mathbb{F}_q}\left(-z, \frac{1}{s_i}z^2\right)\right)\\
&= \sum_{z\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}\left(-gz+\frac{h}{s_i}z^2\right)}\\
&= \sum_{z\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}\left(\frac{h}{s_i}\left(z-\frac{gs_i}{2h}\right)^2-\frac{g^2s_i}{4h}\right)}\\
&= \eta(h)\eta(s_i)S(1)\zeta_p^{-\mathrm{Tr}\left(\frac{g^2s_i}{4h}\right)}.
\end{aligned}$$

Hence we have

$$\begin{aligned}
&\chi_{g,h}\left(D_0 D_5^{(-xy)}\right) + \chi_{g,h}\left(D_8 D_{13}^{(-xy)}\right)\\
&= \eta(h)\eta(s_0)S(1)\zeta_p^{-\mathrm{Tr}\left(\frac{g^2s_0}{4h}\right)}\eta(h)\eta(s_5)S(1)\zeta_p^{-\mathrm{Tr}\left(\frac{g^2s_5}{4h}\right)}\\
&+ \eta(h)\eta(s_8)S(1)\zeta_p^{-\mathrm{Tr}\left(\frac{g^2s_8}{4h}\right)}\eta(h)\eta(s_{13})S(1)\zeta_p^{-\mathrm{Tr}\left(\frac{g^2s_{13}}{4h}\right)}
\end{aligned}$$

$$
\begin{aligned}
&= \eta(s_0 s_5) S(1)^2 \zeta_p^{\mathrm{Tr}\left(-\frac{g^2 s_0}{4h} - \frac{g^2 s_5}{4h}\right)} + \eta(s_8 s_{13}) S(1)^2 \zeta_p^{\mathrm{Tr}\left(-\frac{g^2 s_8}{4h} - \frac{g^2 s_{13}}{4h}\right)} \\
&= (\eta(s_0 s_5) + \eta(s_8 s_{13})) S(1)^2 \zeta_p^{\mathrm{Tr}\left(-\frac{g^2 s_0}{4h} - \frac{g^2 s_5}{4h}\right)} \\
&= 0.
\end{aligned}
$$

Similarly, we can prove that

$$
\begin{aligned}
\chi_{g,h}\left(D_1 D_6^{(-xy)}\right) + \chi_{g,h}\left(D_9 D_{14}^{(-xy)}\right) &= 0, \\
\chi_{g,h}\left(D_2 D_7^{(-xy)}\right) + \chi_{g,h}\left(D_{10} D_{15}^{(-xy)}\right) &= 0, \\
\chi_{g,h}\left(D_3 D_4^{(-xy)}\right) + \chi_{g,h}\left(D_{11} D_{12}^{(-xy)}\right) &= 0, \\
\chi_{g,h}\left(D_4 D_9^{(-xy)}\right) + \chi_{g,h}\left(D_{12} D_1^{(-xy)}\right) &= 0, \\
\chi_{g,h}\left(D_5 D_{10}^{(-xy)}\right) + \chi_{g,h}\left(D_{13} D_2^{(-xy)}\right) &= 0, \\
\chi_{g,h}\left(D_6 D_{11}^{(-xy)}\right) + \chi_{g,h}\left(D_{14} D_3^{(-xy)}\right) &= 0, \\
\chi_{g,h}\left(D_7 D_8^{(-xy)}\right) + \chi_{g,h}\left(D_{15} D_0^{(-xy)}\right) &= 0.
\end{aligned}
$$

Therefore, we have proved that $\chi_{g,h}(\text{LHS of Eq. (13)}) = 0$.

We can do similarly for other equations of Eqs. (10)–(18) by Lemma 4.2 and other formulas of Lemma 4.3. □

Remark 4.5 Using MAGMA [1], we found that for all prime power $q \equiv 1 \pmod 4$ and $353 \leq q < 1.2 \times 10^6$, there exist $s_2, s_8 \in \mathbb{F}_q^*$ satisfying the conditions of Lemma 4.2, and then there exist the corresponding relative difference sets. Our experiment suggests that for all prime power $q \equiv 1 \pmod 4$ and $q \geq 353$, there may exist $s_2, s_8 \in \mathbb{F}_q^*$ satisfying the conditions of Lemma 4.2.

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

References

1. Bosma, W., Cannon, J., Playoust, C.: The magma algebra system I: the user language. J. Symb. Comput. **24**(3–4), 235–265 (1997)
2. Buratti, M.: Cyclic designs with block size 4 and related optimal optical orthogonal codes. Des. Codes Cryptogr. **26**(1–3), 111–125 (2002)
3. Chang, Y., Ji, L.: Optimal $(4up, 5, 1)$ optical orthogonal codes. J. Comb. Des. **12**(5), 346–361 (2004)
4. Davis, J.A., Jedwab, J., Mowbray, M.: New families of semi-regular relative difference sets. Des. Codes Cryptogr. **13**(2), 131–146 (1998)
5. Feng, T.: Relative (pn, p, pn, n)-difference sets with $\mathrm{GCD}(p, n) = 1$. J. Algebr. Comb. **29**(1), 91–106 (2009)
6. Feng, T., Xiang, Q.: Semi-regular relative difference sets with large forbidden subgroups. J. Comb. Theory Ser. A **115**(8), 1456–1473 (2008)

7. Godsil, C., Roy, A.: Equiangular lines, mutually unbiased bases, and spin models. Eur. J. Comb. **30**(1), 246–262 (2009)
8. Hiramine, Y.: On abelian $(2n, n, 2n, 2)$-difference sets. J. Comb. Theory Ser. A **117**(7), 996–1003 (2010)
9. Ikeda, M.: A remark on the non-existence of generalized bent functions. In: Yildirim, C.Y., Stepanov, S.A. (eds.) Number Theory and Its Applications (Ankara, 1996), Volume 204 of Lecture Notes in Pure and Applied Mathematics, pp. 109–119. Dekker, New York (1999)
10. Ivanović, I.D.: Geometrical description of quantal state determination. J. Phys. A **14**(12), 3241–3245 (1981)
11. Leung, K.H., Ling, S., Ma, S.L.: Constructions of semi-regular relative difference sets. Finite Fields Appl. **7**(3), 397–414 (2001)
12. Leung, K.H., Ma, S.L., Tan, V.: Planar functions from Z_n to Z_n. J. Algebra **224**(2), 427–436 (2000)
13. Ma, S.L.: Planar functions, relative difference sets, and character theory. J. Algebra **185**(2), 342–356 (1996)
14. Ma, S.L., Schmidt, B.: 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)
15. Pott, A.: Finite Geometry and Character Theory, Volume 1601 of Lecture Notes in Mathematics. Springer, Berlin (1995)
16. Schmidt, B.: On (p^a, p^b, p^a, p^{a-b})-relative difference sets. J. Algebr. Comb. **6**(3), 279–297 (1997)
17. Schmidt, B.: Characters and Cyclotomic Fields in Finite Geometry, Volume 1797 of Lecture Notes in Mathematics. Springer, Berlin (2002)
18. Wootters, W.K., Fields, B.D.: Optimal state-determination by mutually unbiased measurements. Ann. Phys. **191**(2), 363–381 (1989)