

Note

Proof of a conjecture on semiregular relative difference sets in $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$

Yutaka Hiramine

Department of Mathematics, Faculty of Education, Kumamoto University, Kurokami, Kumamoto, Japan

Received 19 May 2005

Available online 26 July 2006

Communicated by William M. Kantor

Abstract

In this article we show that there is no (p^3, p, p^3, p^2) -difference set in $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ for all primes $p > 3$. This is an affirmative answer to a conjecture raised by S.L. Ma and B. Schmidt.

© 2006 Elsevier Inc. All rights reserved.

Keywords: Relative difference set; Semiregular; Abelian p -group; Ring

1. Introduction

Let G be a group of order mu and U a subgroup of G of order u . A k -subset D of G is called a (m, u, k, λ) -difference set in G with respect to U if $DD^{(-1)} = k + \lambda(G - U)$, where we identify a subset X of G with a group ring element $\sum_{x \in X} x \in \mathbb{Z}[G]$ and set $X^{(-1)} = \sum_{x \in X} x^{-1}$. The set D is also called a *relative difference set* relative to U . A relative difference set D is called *semiregular* if $k = u\lambda$ (i.e. $(m, u, k, \lambda) = (u\lambda, u, u\lambda, \lambda)$).

In their paper [3], Davis and Jedwab improved Ma–Schmidt’s result on (p^a, p, p^a, p^{a-1}) -difference sets [5] and showed the following.

Result 1.1. ([3], see also p. 3 of [6].) *For each $d \geq 1$, there exists a $(p^{2d+1}, p, p^{2d+1}, p^{2d})$ -difference set in any abelian p -group of order p^{2d+2} and exponent at most p^{d+1} relative to any subgroup U of order p , except possibly when $G \simeq \mathbb{Z}_{p^{d+1}} \times \mathbb{Z}_{p^{d+1}}$ or $d > 1$ and when $G \simeq \mathbb{Z}_{p^{d+1}} \times \mathbb{Z}_{p^d} \times U$.*

E-mail address: hiramine@gpo.kumamoto-u.ac.jp.

Concerning one of the open cases in Result 1.1 Ma and Schmidt gave the following result.

Result 1.2. (Ma–Schmidt [6, Theorem 5.10].) Assume p is an odd prime and let D be a (p^3, p, p^3, p^2) -difference set in $G = \langle a, b \rangle (\simeq \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2})$ relative to $N = \langle b^p \rangle (\simeq \mathbb{Z}_p)$. Then,

$$D = \sum_{i,j=0}^{p-1} a^i b^j \sum_{x=0}^{p-1} (a^p)^x (b^p)^{u_{ij}x^2 + v_{ij}x + w_{ij}},$$

where $u_{ij}, v_{ij}, w_{ij} \in \{0, 1, \dots, p-1\}, u_{ij} \neq 0$.

They also gave a necessary and sufficient condition using functions from $\mathbb{Z}_p \times \mathbb{Z}_p$ to $\mathbb{Z}_p$ (see Theorem 5.14 of [6]). For $p = 3$ Remling (1996) showed the nonexistence of such functions (see remark in Section 5 of [6]). Kenji Kawamoto also showed the nonexistence for $p = 3$ in a different method in his master's thesis [4]. In remark mentioned above Ma and Schmidt conjectured that there is no such a relative difference set when p is an odd prime. We note that when $p = 2$, there exists a $(2^3, 2, 2^3, 2^2)$ -difference set D in $\langle a \rangle \times \langle b \rangle (\simeq \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2})$ relative to $\langle b^2 \rangle (\simeq \mathbb{Z}_2)$: $D = \{1, a, a^2, a^3b^2, b, ab, a^2b, a^3b^3\}$.

In this article we give an affirmative answer to this conjecture and prove the following.

Theorem 1.3. There is no (p^3, p, p^3, p^2) -difference set in $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ for all primes $p > 3$.

2. Properties of u_{ij}, v_{ij} and w_{ij}

Let p be an odd prime and D a (p^3, p, p^3, p^2) -difference set in a group $G = \langle a, b \rangle (\simeq \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2})$ relative to $N = \langle b^p \rangle (\simeq \mathbb{Z}_p)$. By definition,

$$DD^{(-1)} = p^3 + p^2(G - N). \quad (1)$$

Throughout this article $I_m (= \{0, 1, \dots, m-1\})$ always denotes the set of nonnegative integers less than m . We often identify I_m with $\mathbb{Z}_m = \{0, 1, \dots, m-1\} \pmod{m}$. Let χ be a character of G . Then, there exist $\ell \in I_{p^2}$ and $m \in I_{p^2}$ such that $\chi(a^r b^s) = \theta^{\ell r} \theta^{ms}$ for $r, s \in I_{p^2}$, where $\theta = e^{2\pi i/p^2}$. By (1), we have

$$\chi(D)\overline{\chi(D)} = p^3 \quad \text{if } m \not\equiv 0 \pmod{p}. \quad (2)$$

Set $D = \{a^{r_j} b^{s_j} \mid j \in I_{p^3}\}$ and let χ_ℓ be a character of G such that $\chi_\ell(a) = \theta^\ell$ and $\chi_\ell(b) = \theta$. Put $n_j = |\{i \mid \chi(a^{r_i} b^{s_i}) = \theta^j\}|$ for each $j \in I_{p^2}$. We note that n_j depends on the choice of $\ell (\in I_{p^2})$. From now on, we set $\chi = \chi_\ell$. By definition,

$$\chi(D) = \sum_{i \in I_{p^2}} n_i \theta^i. \quad (3)$$

By Result 1.2, $\chi(D)$ is represented in the following form:

$$\chi(D) = \sum_{i,j \in I_p} \theta^{i\ell+j} \sum_{x \in I_p} (\theta^p)^{u_{ij}x^2 + (v_{ij}+\ell)x + w_{ij}}, \quad (4)$$

where $u_{ij}, v_{ij}, w_{ij} \in I_p, u_{ij} \neq 0$.

By (4), we have the following.

Lemma 2.1. For each $k \in I_p$, $n_k + n_{k+p} + n_{k+2p} + \cdots + n_{k+(p-1)p} = p^2$.

Lemma 2.2. There exist integers $r_\ell \in I_{p^2}$ and $e_\ell \in \{\pm 1\}$ satisfying $\chi(D) = e_\ell p \sqrt{p^*} \theta^{r_\ell}$, where $p^* = (-1)^{(p-1)/2} p$.

Proof. Set $\xi = \chi(D)$ and $\beta = \xi / (p \sqrt{p^*})$. Then $\xi, \beta \in \mathbb{Q}(\theta)$ and $|\beta| = 1$ by (2). On the other hand, p has the factorization $(p) = \mathfrak{P}^{p(p-1)}$ in $\mathbb{Q}(\theta)$, where $\mathfrak{P}$ is a prime ideal in $\mathbb{Q}(\theta)$. Hence, by (2), $(\xi \bar{\xi}) = (p^3) = \mathfrak{P}^{3p(p-1)}$ and so $(\xi^2) = (p^3)$. Thus $\xi^2 = p^3 \alpha$ for an algebraic integer $\alpha \in \mathbb{Z}[\theta]$. It follows that $\beta^2 = (-1)^{(p-1)/2} \alpha$ and so β is also an algebraic integer contained in $\mathbb{Z}[\theta]$. Let σ be a field automorphism of $\mathbb{Q}(\theta)$. Then χ^σ is also a character of G . Hence, $|\beta^\sigma| = |(\chi(D))^\sigma| / |(p \sqrt{p^*})^\sigma| = |\chi^\sigma(D)| / p \sqrt{p} = 1$ by (2). Therefore the absolute value of any conjugate of β over $\mathbb{Q}$ is 1. Applying Kronecker's lemma (Lemma 3 of Section 1, Chapter 3 in [1]), $\beta = e_\ell \theta^{r_\ell}$ for some $e_\ell \in \{\pm 1\}$ and $r_\ell \in I_{p^2}$. $\square$

We can easily verify the following lemma, which we use to determine n_i 's.

Lemma 2.3. Let p^n be a power of a prime p and let θ be a primitive p^n th root of unity. If $\sum_{0 \leq i \leq p^n-1} a_i \theta^i = 0$ for some integers $a_0, a_1, \dots, a_{p^n-1}$ and if $s \equiv t \pmod{p^{n-1}}$, then $a_s = a_t$.

Lemma 2.4. Set $r = r_\ell$ and $e = e_\ell$. Then the following hold.

- (i) If $i \not\equiv r \pmod{p}$, then $n_i = p$.
- (ii) $n_{jp+r} = (1 + e(j/p))p \in \{0, p, 2p\}$ for $j \in I_p$, where $(*/*)$ is the Legendre symbol and indices are taken modulo p^2 .

Proof. By (3) and Lemma 2.2, $\sum_{j \in I_{p^2}} n_j \theta^j = ep \sqrt{p^*} \theta^r$, where $e = e_\ell$ and $r = r_\ell$. On the other hand, $\sqrt{p^*} = \sum_{j \in I_p} (j/p) \theta^{pj}$ (Gauss sum). Hence, $\sum_{j \in I_{p^2}} n_j \theta^j = ep \sum_{j \in I_p} (j/p) \theta^{pj+r}$. By Lemma 2.3, the following hold.

$$n_t = n_{t+jp}, \quad \forall j \in I_p, \quad \forall t \in I_p \text{ if } t \not\equiv r \pmod{p}, \quad (5)$$

$$n_r = n_{r+jp} - ep \left(\frac{j}{p} \right), \quad \forall j \in I_p. \quad (6)$$

By Lemma 2.1, $pn_t = \sum_{j \in I_p} n_{t+jp} = p^2$ and

$$pn_r = \sum_{j \in I_p} \left(n_{r+jp} - ep \left(\frac{j}{p} \right) \right) = \sum_{0 \leq j \leq p-1} n_{r+jp} - ep \sum_{0 \leq j \leq p-1} \left(\frac{j}{p} \right) = p^2.$$

Therefore $n_t = p$ if $t \not\equiv r \pmod{p}$ and $n_r = p$. Thus the lemma follows from (5) and (6). $\square$

Notation 2.5. For $n \in \mathbb{N} \cup \{0\}$, let $\langle\langle n \rangle\rangle$ be the remainder of n modulo p and put $((n)) = (n - \langle\langle n \rangle\rangle)/p$ (i.e. $n = ((n))p + \langle\langle n \rangle\rangle$).

For a multiset $T = \{(\theta^p)^{m_1}, (\theta^p)^{m_2}, \dots, (\theta^p)^{m_d}\}$ we define

$$f(T) = \{m_1, m_2, \dots, m_d\} \pmod{p}$$

as a multiset. We note that each element of $f(T)$ is always taken modulo p . Moreover, for a multiset S on $\mathbb{Z}_p$ and an element $z \in \mathbb{Z}_p$, we put $S + z = \{x + z \mid x \in S\}$ as a multiset.

In the rest of this section set $\ell = \alpha p + \beta$, $r = \lambda p + \mu$ ($\alpha, \beta, \lambda, \mu \in I_p$). We note that λ and μ are uniquely determined by α and β by Lemma 2.2. Set $\mu = \psi(\alpha, \beta)$.

Notation 2.6. For all $\beta, \tau \in I_p$, we define $\Omega_\beta(\tau)$ by

$$\Omega_\beta(\tau) = \{(i, j) \mid i, j \in I_p, i\beta + j \equiv \tau \pmod{p}\}.$$

Remark 2.7. As $\beta \neq 0$, $|\Omega_\beta(\tau)| = p$. Moreover, for all $i \in I_p$,

$$|\Omega_\beta(\tau) \cap (\{i\} \times I_p)| = 1.$$

By (4),

$$\begin{aligned} \chi(D) &= \sum_{i, j \in I_p} \theta^{i\alpha p + ((i\beta + j))p + ((i\beta + j))} \sum_{x \in I_p} (\theta^p)^{u_{ij}x^2 + (v_{ij} + \beta)x + w_{ij}} \\ &= \sum_{\tau \in I_p} \sum_{(i, j) \in \Omega_\beta(\tau)} \left(\theta^{i\alpha p + ((i\beta + j))p} \sum_{x \in I_p} (\theta^p)^{u_{ij}x^2 + (v_{ij} + \beta)x + w_{ij}} \right) \theta^\tau. \end{aligned}$$

Set $T_{ij\beta} = \{f((\theta^p)^{u_{ij}x^2 + (v_{ij} + \beta)x + w_{ij}}) \mid x \in I_p\}$ as a multiset. Then we have

$$T_{ij\beta} = u_{ij}\Gamma + k_{ij\beta}, \quad (7)$$

where $\Gamma = \{x^2 \mid x \in \mathbb{Z}_p\}$ as a multiset and

$$k_{ij\beta} = \frac{4u_{ij}w_{ij} - (v_{ij} + \beta)^2}{4u_{ij}}. \quad (8)$$

Therefore,

$$\begin{aligned} \chi(D) &= \sum_{\tau \in I_p} \left(\sum_{(i, j) \in \Omega_\beta(\tau)} \sum_{y \in T_{ij\beta}} (\theta^p)^y (\theta^p)^{i\alpha + ((i\beta + j))} \right) \theta^\tau \\ &= \sum_{\tau \in I_p} \left(\sum_{(i, j) \in \Omega_\beta(\tau)} \sum_{y \in \Delta} (\theta^p)^y \right) \theta^\tau, \end{aligned}$$

where $\Delta = u_{ij}\Gamma + k_{ij\beta} + i\alpha + ((i\beta + j))$.

By Lemma 2.4, we have the following.

Lemma 2.8. Set $\mu = \psi(\alpha, \beta)$. Then,

- (i) The multiset $\bigcup_{(i, j) \in \Omega_\beta(\mu)} u_{ij}\Gamma + k_{ij\beta} + i\alpha + ((i\beta + j))$ contains exactly $(p + 1)/2$ distinct elements of $\mathbb{Z}_p$.
- (ii) Let $\tau \in I_p$, and assume $\tau \neq \mu$. Then, as a multiset

$$\begin{aligned} &\bigcup_{(i, j) \in \Omega_\beta(\tau)} u_{ij}\Gamma + k_{ij\beta} + i\alpha + ((i\beta + j)) \\ &= \underbrace{\{0, \dots, 0\}}_{p\text{-times}} \cup \underbrace{\{1, \dots, 1\}}_{p\text{-times}} \cup \dots \cup \underbrace{\{p-1, \dots, p-1\}}_{p\text{-times}}. \end{aligned}$$

Let p be an odd prime and $a, b \in \mathbb{Z}_p \setminus \{0\}$. By Theorem 10.5.1 of [2], we have the following.

$$\#\{(x, y) \mid x, y \in \mathbb{Z}_p, x^2 - ay^2 = b\} = p - \left(\frac{a}{p}\right). \quad (9)$$

Lemma 2.9. Let $r, s, c, d \in \mathbb{Z}_p$ ($r, s \neq 0$) and set $a = sr^{-1}, b = (d - c)r^{-1}, \varepsilon = (-1/p)$. If $c \neq d$, then the number of solutions (x^2, y^2) to $rx^2 + c = sy^2 + d$ with $x, y \in \mathbb{Z}_p$ is

$$\frac{p - \varepsilon}{4} + \frac{1 + \varepsilon}{2} + \frac{\varepsilon\left(\left(\frac{a}{p}\right) + \varepsilon\right)\left(\left(\frac{b}{p}\right) - \varepsilon\right)}{4}.$$

Proof. Using a and b , the equation becomes $x^2 - ay^2 = b$. Obviously the number of solutions $(x^2, 0)$ to $x^2 - ay^2 = b$ is $((b/p) + 1)/2$ and the number of solutions $(0, y^2)$ to $x^2 - ay^2 = b$ is $(\varepsilon(a/p)(b/p) + 1)/2$. Hence, by (9), the number of solutions (x^2, y^2) to $x^2 - ay^2 = b$ is

$$\begin{aligned} & \frac{p - \left(\frac{a}{p}\right) - 2\left(\frac{(b/p)+1}{2} + \frac{\varepsilon(a/p)(b/p)+1}{2}\right)}{4} + \frac{\left(\frac{b}{p}\right) + 1}{2} + \frac{\varepsilon\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) + 1}{2} \\ &= \frac{p - \left(\frac{a}{p}\right) + \left(\frac{b}{p}\right) + \varepsilon\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) + 2}{4} \\ &= \frac{p - \varepsilon}{4} + \frac{1 + \varepsilon}{2} + \frac{\varepsilon\left(\left(\frac{a}{p}\right) + \varepsilon\right)\left(\left(\frac{b}{p}\right) - \varepsilon\right)}{4}. \quad \square \end{aligned}$$

Hypothesis 2.10. In the rest of this article we assume that $p > 3$.

Lemma 2.11. Let notations be as in Lemma 2.8(i) and set $u_i = u_{ij}$ and $d_i = k_{ij\beta} + i\alpha + ((i\beta + j))$, where $(i, j) \in \Omega_\beta(\mu)$, $\mu = \psi(\alpha, \beta)$. Then $d_0 = d_1 = \dots = d_{p-1}$ and $(u_0/p) = (u_1/p) = \dots = (u_{p-1}/p)$.

Proof. By Lemma 2.8(i), $\bigcup_{(i,j) \in \Omega_\beta(\mu)} u_i \Gamma + d_i$ contains exactly $\frac{p+1}{2}$ distinct elements. Assume $d_i \neq d_j$ for some $i, j \in I_p$. Applying Lemmas 2.8(i) and 2.9 we have

$$2 \cdot \frac{p+1}{2} - \left(\frac{p - \varepsilon}{4} + \frac{1 + \varepsilon}{2} + \frac{\varepsilon\left(\left(\frac{a}{p}\right) + \varepsilon\right)\left(\left(\frac{b}{p}\right) - \varepsilon\right)}{4} \right) \leq \frac{p+1}{2}.$$

From this,

$$\frac{p+1}{2} \leq \frac{p - \varepsilon}{4} + \frac{1 + \varepsilon}{2} + \frac{\varepsilon\left(\left(\frac{a}{p}\right) + \varepsilon\right)\left(\left(\frac{b}{p}\right) - \varepsilon\right)}{4} \leq \frac{p}{4} + \frac{7}{4}.$$

Hence, $p \leq 5$. By Hypothesis 2.10, we have $p = 5$ and therefore $\varepsilon = (-1/5) = 1$. Thus $((a/5) + 1)((b/5) - 1)/4 \geq 1$, a contradiction. Therefore $d_i = d_j$ for all $i, j \in I_p$. It follows that as a multiset $\bigcup_{(i,j) \in \Omega_\beta(\mu)} u_i \Gamma$ also contains exactly $\frac{p+1}{2}$ distinct elements. This forces $(u_0/p) = (u_1/p) = \dots = (u_{p-1}/p)$. $\square$

Lemma 2.12. Let notations be as in Lemma 2.8(ii). For a fixed $\tau (\neq \mu)$ set $u_i = u_{ij}$ and $d_i = -(k_{ij\beta} + i\alpha + ((i\beta + j)))$, where $(i, j) \in \Omega_\beta(\tau)$. Then $\mathbb{Z}_p = \{d_0, d_1, \dots, d_{p-1}\}$ and $(u_0/p) = (u_1/p) = \dots = (u_{p-1}/p)$.

Proof. By Lemma 2.8(ii),

$$(u_0\Gamma - d_0) \cup \cdots \cup (u_{p-1}\Gamma - d_{p-1}) = \underbrace{\{0, \dots, 0\}}_{p\text{-times}} \cup \cdots \cup \underbrace{\{p-1, \dots, p-1\}}_{p\text{-times}}. \quad (10)$$

Let $c \in \mathbb{Z}_p$ and set $s_i = |\{x \in \mathbb{Z}_p \mid u_i x^2 - d_i = c\}|$ for $i \in \mathbb{Z}_p$. Clearly $s_i \in \{0, 1, 2\}$. As $\sum_{i \in \mathbb{Z}_p} s_i = p \equiv 1 \pmod{2}$ by (10), there exists i such that $s_i = 1$, which implies $d_i = -c$. Since c is arbitrary, $\mathbb{Z}_p = \{d_0, \dots, d_{p-1}\}$.

For all $i \in \mathbb{Z}_p$, put $v_{d_i} = u_i$. Then, by (10), we have

$$(v_0\Gamma - 0) \cup \cdots \cup (v_{p-1}\Gamma - (p-1)) = \underbrace{\{0, \dots, 0\}}_{p\text{-times}} \cup \cdots \cup \underbrace{\{p-1, \dots, p-1\}}_{p\text{-times}}. \quad (11)$$

Let $c \in \mathbb{Z}_p$ and N_j the number of solutions x to $v_j x^2 - j = c$. Then $N_j = (\frac{v_j}{p})(\frac{c+j}{p}) + 1$ ($\in \{0, 1, 2\}$) and $N_0 + \cdots + N_{p-1} = p$ by (11). Moreover, $N_j = 1$ if and only if $j \equiv -c \pmod{p}$. Thus we have

$$\sum_{j \in \mathbb{Z}_p} \left(\frac{v_j}{p}\right) \left(\frac{c+j}{p}\right) = 0 \quad (\forall c \in \mathbb{Z}_p). \quad (12)$$

Let $A = (a_{ij})$ be a $p \times p$ matrix over $\mathbb{Z}$ defined by $a_{ij} = (\frac{i+j}{p})$ ($i, j \in \mathbb{Z}_p$) and let $B = (\vartheta^{ij})$ ($i, j \in \mathbb{Z}_p$) be a $p \times p$ matrix over $\mathbb{C}$, where $\vartheta = e^{2\pi i/p}$ ($= \theta^p$). Since $\sum_{0 \leq x \leq p-1} (x/p) \vartheta^{sx} = (s/p) \sqrt{p^*}$ (Gauss sum), we have

$$\begin{aligned} \sum_{0 \leq k \leq p-1} \left(\frac{i+k}{p}\right) \vartheta^{kj} &= \vartheta^{-ij} \sum_{0 \leq k \leq p-1} \left(\frac{i+k}{p}\right) (\vartheta^j)^{i+k} = \vartheta^{-ij} \sum_{0 \leq x \leq p-1} \left(\frac{x}{p}\right) (\vartheta^j)^x \\ &= \vartheta^{-ij} \left(\frac{j}{p}\right) \sqrt{p^*}. \end{aligned}$$

Thus we have

$$AB = \sqrt{p^*} \begin{bmatrix} 0 & (\frac{1}{p}) & (\frac{2}{p}) & \cdots & \\ 0 & (\frac{1}{p})(\vartheta^{-1}) & (\frac{2}{p})(\vartheta^{-2}) & \cdots & \cdots \\ 0 & (\frac{1}{p})(\vartheta^{-1})^2 & (\frac{2}{p})(\vartheta^{-2})^2 & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & (\frac{1}{p})(\vartheta^{-1})^{p-1} & (\frac{2}{p})(\vartheta^{-2})^{p-1} & & \end{bmatrix}.$$

Since $\det(B) \neq 0$, it follows that $\text{rank}(A) = p-1$ and so $\dim(\ker(A)) = 1$. Hence,

$$\ker(A) = \left\langle \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} \right\rangle.$$

By (12), we have $(v_0/p) = (v_1/p) = \cdots = (v_{p-1}/p)$. Therefore $(u_0/p) = (u_1/p) = \cdots = (u_{p-1}/p)$. $\square$

Lemma 2.13. Let $\gamma \in \mathbb{Z}_p$. If $\gamma \neq \alpha$, then $\psi(\gamma, \beta) \neq \psi(\alpha, \beta)$.

Proof. Set $v = \psi(\gamma, \beta)$ and assume $\mu = v$. Then, $\Omega_\beta(\mu) = \Omega_\beta(v)$ and $(0, \mu) \in \Omega_\beta(\mu)$, $(0, v) \in \Omega_\beta(v)$. It follows from Lemma 2.11 that $k_{0,\mu,\beta} = k_{ij\beta} + i\alpha + ((i\beta + j))$ and $k_{0,\mu,\beta} = k_{ij\beta} + i\gamma + ((i\beta + j))$ for any $(i, j) \in \Omega_\beta(\mu) (= \Omega_\beta(v))$. Thus $\alpha = \gamma$, a contradiction. $\square$

Notation 2.14. Let $\beta \in \mathbb{Z}_p$. By Lemma 2.13, an equation $\psi(x, \beta) = k$ has a unique solution $x \in \mathbb{Z}_p$. We set $x = \alpha(\beta, k)$.

By Definition 2.14 and Lemma 2.13, $\alpha(\beta, k_1) \neq \alpha(\beta, k_2)$ if $k_1 \neq k_2$. Hence,

$$\mathbb{Z}_p = \{\alpha(\beta, 0), \alpha(\beta, 1), \dots, \alpha(\beta, p-1)\}. \quad (13)$$

Set $\Phi_{\alpha\beta ij} = \frac{4u_{ij}w_{ij} - (v_{ij} + \beta)^2}{4u_{ij}} + ((i\beta + j)) + i\alpha$. By Lemmas 2.11 and 2.12, we have shown the following.

Lemma 2.15. For all $\alpha \in \mathbb{Z}_p$ and $\beta \in \mathbb{Z}_p$ the following hold.

- (i) If $(i_1, j_1), (i_2, j_2) \in \Omega_\beta(\psi(\alpha, \beta))$, then $\Phi_{\alpha\beta i_1 j_1} = \Phi_{\alpha\beta i_2 j_2}$.
- (ii) $\mathbb{Z}_p = \{\Phi_{\alpha\beta ij} \mid (i, j) \in \Omega_\beta(v)\}$ for all $v (\neq \psi(\alpha, \beta))$.

Notation 2.16. For all $(i, j) \in \Omega_\beta(\psi(\alpha, \beta))$, we set

$$\Phi_{\alpha\beta} = \frac{4u_{ij}w_{ij} - (v_{ij} + \beta)^2}{4u_{ij}} + ((i\beta + j)) + i\alpha. \quad (14)$$

By Lemma 2.15(i), $\Phi_{\alpha\beta}$ is independent of the choice of $(i, j) \in \Omega_\beta(\psi(\alpha, \beta))$.

If $(i, j) \in \Omega_\beta(\psi(\alpha, \beta))$, then $i\beta + j = \psi(\alpha, \beta)$. Using Notation 2.14, $\alpha = \alpha(\beta, i\beta + j)$. Hence, Eq. (14) can be written in the following form:

$$\Phi_{\alpha\beta} = \frac{4u_{ij}w_{ij} - (v_{ij} + \beta)^2}{4u_{ij}} + ((i\beta + j)) + i\alpha(\beta, i\beta + j). \quad (15)$$

Lemma 2.17. The following hold.

- (i) For each β , $\bigcup_{\alpha \in I_p} \Omega_\beta(\psi(\alpha, \beta)) = I_p \times I_p$.
- (ii) For each (i, j) , we put $\Lambda(i, j) = \{(\alpha', \beta') \mid (i, j) \in \Omega_{\beta'}(\psi(\alpha', \beta'))\}$. Let $\alpha, \beta \in \mathbb{Z}_p$ and set $\mu = \psi(\alpha, \beta)$. If $(i_1, j_1), (i_2, j_2) \in \Omega_\beta(\psi(\alpha, \beta))$ and $(i_1, j_1) \neq (i_2, j_2)$, then $\Lambda(i_1, j_1) \cap \Lambda(i_2, j_2) = \{(\alpha, \beta)\}$.

Proof. By Remark 2.7, it suffices to show that $\Omega_\beta(\mu(\alpha_1, \beta)) \cap \Omega_\beta(\mu(\alpha_2, \beta)) = \emptyset$ if $\alpha_1 \neq \alpha_2$. Let $(i, j) \in \Omega_\beta(\psi(\alpha_1, \beta)) \cap \Omega_\beta(\psi(\alpha_2, \beta))$. As $\alpha_1 \neq \alpha_2$, we have $\psi(\alpha_1, \beta) \neq \psi(\alpha_2, \beta)$ by Lemma 2.13. Hence, $i\beta + j = \psi(\alpha_1, \beta) \neq \psi(\alpha_2, \beta) = i\beta + j$, a contradiction. Thus (i) holds.

By definition of Λ , $(\alpha, \beta) \in \Lambda(i_1, j_1) \cap \Lambda(i_2, j_2)$. Assume $(\gamma, \delta) \in \Lambda(i_1, j_1) \cap \Lambda(i_2, j_2)$. Then $i_1\delta + j_1 = \psi(\gamma, \delta) = i_2\delta + j_2$ and $i_1\beta + j_1 = \psi(\alpha, \beta) = i_2\beta + j_2$. From this, if $i_1 = i_2$, then $j_1 = j_2$, a contradiction. Hence, $i_1 \neq i_2$ and so $\delta = \frac{j_2 - j_1}{i_1 - i_2} = \beta$. Therefore, $\psi(\gamma, \beta) = \psi(\alpha, \beta)$. By Lemma 2.13, $\alpha = \gamma$. Thus (ii) holds. $\square$

3. Proof of Theorem 1.3

We now prove Theorem 1.3.

By Lemma 2.13, $\mathbb{Z}_p = \{\psi(0, 0), \psi(1, 0), \psi(2, 0), \dots, \psi(p-1, 0)\}$. Hence, given $j \in \mathbb{Z}_p$, there exists a unique $\gamma \in \mathbb{Z}_p$ such that $\psi(\gamma, 0) = j$. Since $\Omega_0(\psi(\gamma, 0)) = \{(0, j), (1, j), \dots, (p-1, j)\}$, applying Lemma 2.17(ii), we have

$$\Lambda(i_1, j) \cap \Lambda(i_2, j) = \{(\gamma, 0)\} \quad (i_1 \neq i_2). \quad (16)$$

Set $\Lambda^{(j)} = \Lambda(0, j) \cup \Lambda(1, j) \cup \dots \cup \Lambda(p-1, j)$ as a multiset. By Lemma 2.13, again, $\Lambda(i, j) \cap (\mathbb{Z}_p \times \{0\}) = \{(\gamma, 0)\}$. This, together with (16), gives the following.

$$\Lambda^{(j)} = \underbrace{\{(\gamma, 0), \dots, (\gamma, 0)\}}_{p\text{-times}} \cup \mathbb{Z}_p \times \mathbb{Z}_p^*. \quad (17)$$

We define a function F from $\mathbb{Z}_p$ to $\mathbb{Z}_p$ by

$$F(j) = \sum_{i \in \mathbb{Z}_p} \sum_{(\alpha, \beta) \in \Lambda(i, j)} \Phi(\alpha, \beta).$$

Then,

$$F(j) = \sum_{i \in \mathbb{Z}_p} \left(\sum_{(\alpha, \beta) \in \Lambda(i, j)} \Phi(\alpha, \beta) \right) = \sum_{(\alpha, \beta) \in \Lambda^{(j)}} \Phi(\alpha, \beta).$$

Applying (17),

$$F(j) = p\Phi(\gamma, 0) + \sum_{(\alpha, \beta) \in \mathbb{Z}_p \times \mathbb{Z}_p^*} \Phi(\alpha, \beta) = \sum_{(\alpha, \beta) \in \mathbb{Z}_p \times \mathbb{Z}_p^*} \Phi(\alpha, \beta).$$

Hence, we have,

Lemma 3.1. $F(0) = F(1) = \dots = F(p-1) = \sum_{(\alpha, \beta) \in \mathbb{Z}_p \times \mathbb{Z}_p^*} \Phi(\alpha, \beta).$

On the other hand, by (15),

$$\begin{aligned} F(j) &= \sum_{i \in \mathbb{Z}_p} \sum_{(\alpha, \beta) \in \Lambda(i, j)} \Phi(\alpha, \beta) \\ &= \sum_{i \in \mathbb{Z}_p} \sum_{\beta \in \mathbb{Z}_p} \frac{4u_{ij}w_{ij} - (v_{ij} + \beta)^2}{4u_{ij}} + ((i\beta + j)) + i\alpha(\beta, i\beta + j) \\ &= \sum_{i \in \mathbb{Z}_p} \left(\left(\frac{4u_{ij}w_{ij} - v_{ij}^2}{4u_{ij}} \right) \sum_{\beta \in \mathbb{Z}_p} 1 - \frac{v_{ij}}{2u_{ij}} \sum_{\beta \in \mathbb{Z}_p} \beta - \frac{1}{4u_{ij}} \sum_{\beta \in \mathbb{Z}_p} \beta^2 \right) \\ &\quad + \sum_{i, \beta \in \mathbb{Z}_p} ((i\beta + j)) + \sum_{i, \beta \in \mathbb{Z}_p} i\alpha(\beta, i\beta + j). \end{aligned}$$

Clearly $\sum_{\beta \in \mathbb{Z}_p} 1 = \sum_{\beta \in \mathbb{Z}_p} \beta = 0$. Moreover, as $p > 3$, $\sum_{\beta \in \mathbb{Z}_p} \beta^2 = 0$. Hence,

$$\begin{aligned}
 F(j) &= \sum_{i, \beta \in \mathbb{Z}_p} ((i\beta + j)) + \sum_{i, \beta \in \mathbb{Z}_p} i\alpha(\beta, i\beta + j) \\
 &= \sum_{i, \beta \in \mathbb{Z}_p} ((i\beta + j)) + \sum_{i \in \mathbb{Z}_p} i\alpha(0, j) + \sum_{\beta \in \mathbb{Z}_p^*} \left(\sum_{k \in \mathbb{Z}_p} \beta^{-1}(k - j)\alpha(\beta, k) \right).
 \end{aligned}$$

$$\text{As } \sum_{i \in \mathbb{Z}_p} i\alpha(0, j) = \frac{p-1}{2} p \cdot \alpha(0, j) = 0,$$

$$F(j) = \sum_{i, \beta \in \mathbb{Z}_p} ((i\beta + j)) + \sum_{\beta \in \mathbb{Z}_p^*} \beta^{-1} \left(\sum_{k \in \mathbb{Z}_p} (k\alpha(\beta, k) - j\alpha(\beta, k)) \right).$$

As $\sum_{k \in \mathbb{Z}_p} \alpha(\beta, k) = 0$ by (13), we have

$$F(j) = \sum_{i, \beta \in \mathbb{Z}_p} ((i\beta + j)) + \sum_{\beta \in \mathbb{Z}_p^*} \beta^{-1} \sum_{k \in \mathbb{Z}_p} k\alpha(\beta, k). \quad (18)$$

We note that the second term of the right-hand side of (18) is independent of j . This, together with Lemma 3.1, gives the following.

Lemma 3.2. Set $g(t) = \sum_{i, j \in I_p} ((ij + t)) \pmod{p}$. If there is a (p^3, p, p^3, p^2) -difference set in $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$, then $g(0) = g(1) = \dots = g(p-1)$.

We can check the following.

Lemma 3.3. Let $i, j, t \in I_p$. Then the following three conditions are equivalent.

- (i) $((ij + t)) \neq ((ij + t + 1))$.
- (ii) $((ij + t)) + 1 = ((ij + t + 1))$.
- (iii) $ij + t + 1 \equiv 0 \pmod{p}$.

Lemma 3.4. Let $t \in I_p$ and set $S_t = \{(i, j) \mid i, j \in I_p, ij + t + 1 \equiv 0 \pmod{p}\}$. Then,

$$|S_t| = \begin{cases} 2p-1 & \text{if } t = p-1, \\ p-1 & \text{otherwise.} \end{cases}$$

By Lemmas 3.3 and 3.4, we have

Lemma 3.5. $g(n) = \sum_{i, j \in I_p} ((ij + n)) \equiv \frac{p-1}{2} - n \pmod{p}$.

Proof. By Lemmas 3.3 and 3.4, $g(t+1) = g(t) + p-1 \equiv g(t) - 1 \pmod{p}$ for $t \in I_p \setminus \{p-1\}$. We now compute $g(0)$. Put $M_k = \{(i, j) \mid i, j \in I_p, ij \equiv k \pmod{p}\}$ for each $k \in I_p$. Then $M_0 = \{(i, 0) \mid i \in I_p\} \cup \{(0, j) \mid j \in I_p\}$. Moreover, for given k and i with $k, i \in I_p \setminus \{0\}$ there exists a unique $j \in I_p \setminus \{0\}$ such that $ij \equiv k \pmod{p}$. In particular $|M_k| = p-1$ for $k \in I_p \setminus \{0\}$. Hence,

$$\begin{aligned}
 g(0) &= \sum_{k \in I_p} \sum_{(i, j) \in M_k} \frac{ij - k}{p} = \sum_{0 \neq k \in I_p} \sum_{(i, j) \in M_k} \frac{ij - k}{p} \\
 &= \sum_{1 \leq k \leq p-1} \left(\sum_{(i, j) \in M_k} \frac{ij}{p} - \sum_{(i, j) \in M_k} \frac{k}{p} \right)
 \end{aligned}$$

$$\begin{aligned}
&= \frac{(1 + 2 + \cdots + (p-1))^2}{p} + \frac{p-1}{p}(1 + 2 + \cdots + (p-1)) \\
&= \frac{p-1}{2} \left(1 + \frac{p-3}{2}p \right) \equiv \frac{p-1}{2}.
\end{aligned}$$

Thus $g(0) = \frac{p-1}{2}$ and so $g(n) \equiv \frac{p-1}{2} - n \pmod{p}$ for $n \in I_p$. $\square$

Proof of Theorem. By Lemmas 3.2 and 3.5 the theorem holds. $\square$

Remark 3.6. In their paper [6] S.L. Ma and B. Schmidt defined a function $F : I_{p^{c+1}} \times I_{p^c} \times I_p \rightarrow \mathbb{N} \cup \{0\}$ using a putative $(p^{2c+1}, p, p^{2c+1}, p^{2c})$ -relative difference set R in $\mathbb{Z}_{p^{c+1}} \times \mathbb{Z}_{p^{c+1}}$ (see §5 of [6]). They conjectured that $(*) F(r, s, \ell) = 1$ for all r, s and ℓ and proved this for $c = 1$, on which Result 1.2 is based. They also showed that if the conjecture is true, then there exists a $(p^{2c-1}, p, p^{2c-1}, p^{2c-2})$ -relative difference set R in $\mathbb{Z}_{p^c} \times \mathbb{Z}_{p^c}$ (see p. 17 of [6]). Hence, we note that our theorem implies that if $(*)$ is true for all $c (\geq 1)$, then there is no $(p^{2c+1}, p, p^{2c+1}, p^{2c})$ -relative difference set in $\mathbb{Z}_{p^{c+1}} \times \mathbb{Z}_{p^{c+1}}$ for all odd primes p and integers $c (\geq 1)$.

References

- [1] Ya.G. Berkovich, E.M. Zhmud, Characters of Finite Groups, Part I, Transl. Math. Monogr., 1998.
- [2] B.C. Berndt, R.J. Evans, K.S. Williams, Gauss and Jacobi Sums, Wiley–Interscience, New York, 1998.
- [3] J.A. Davis, J.A. Jedwab, A unifying construction for difference sets, J. Combin. Theory, Ser. A 80 (1997) 13–78.
- [4] K. Kawamoto, On relative difference sets in finite groups, Master thesis, Kumamoto University, 2005 (in Japanese).
- [5] S.L. Ma, B. Schmidt, On (p^a, p, p^a, p^{a-1}) -relative difference sets, Des. Codes Cryptogr. 6 (1995) 57–71.
- [6] S.L. Ma, 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 (2000) 1–22.