PARAMEDIAL QUASIGROUPS OF PRIME AND PRIME SQUARE ORDER

ŽANETA SEMANIŠINOVÁ

Abstract. We prove that, for every odd prime number \( p \), there are \( 2p - 1 \) paramedial quasigroups of order \( p \) and \( 6p^2 - p - 1 \) paramedial quasigroups of order \( p^2 \), up to isomorphism. We present a complete list of those which are simple.

1. Introduction

A binary operation \( * \) on a set \( A \) is called paramedial, if it satisfies the identity

\[(x * y) * (u * v) = (v * y) * (u * x).\]

For example, subtraction in abelian groups is paramedial. A binary algebraic structure \((A, *)\) with a paramedial operation will be called a paramedial groupoid. The structure will be called paramedial quasigroup, if the operation \( * \) is uniquely divisible from both sides (and thus forms a latin square). It is unknown to us where the paramedial law originated. It was considered, for example, in [11] under the nickname \( \beta_2 \), for purely syntactic reasons, being, in a sense, dual to the more famous medial law \((x * y) * (u * v) = (x * u) * (y * v)\). A systematic study of paramedial groupoids was initiated by Cho, Ježek and Kepka in [2]. The identity also appears in the context of Abel-Grassmann groupoids [15].

In [3], Cho, Ježek and Kepka initiated the classification of simple paramedial groupoids. They proved that finite simple paramedial groupoids come in four mutually exclusive types: quasigroups, zeropotent groupoids, commutative non-zeropotent non-quasigroups, and certain isotopes of rectangular bands. For the latter three types, a complete classification is available [3, 4, 5]. However, the only paper addressing the quasigroup case is [13] (exploiting the observation that the equivalence defined by \( x \sim y \Leftrightarrow x * x = y * y \) is a congruence), but it does not contain any classification results.

Our goal is to enumerate paramedial quasigroups of small order and determine those which are simple. The fundamental tool to study paramedial quasigroups (and many other classes of quasigroups) is their affine representation over abelian groups [11, Theorem 9]. Therefore, using the methods of [6], the enumeration reduces to an analysis of square roots and conjugacy classes in (certain subgroups of) automorphism groups of abelian groups; in the finite case, one can restrict to groups of prime power order. In the present paper, we focus on cyclic groups and on elementary abelian groups of dimension 2.

A similar approach was taken to enumerate medial quasigroups of order \( p \) [9, 17], \( p^2 \) [16], \( p^3 \) and \( p^4 \) in the idempotent case [8], and \( 64 \neq p^k < 128 \) [17] (\( p \) prime). One of our motivations was, whether it is feasible to use the same methods in the paramedial setting. As it turns out, it is, however, the analysis is much more complicated, and in one case, we rely on a non-trivial result from number theory.

1991 Mathematics Subject Classification. 20N05, 05A15.

Key words and phrases. Paramedial quasigroups, affine quasigroups, enumeration of quasigroups, simple quasigroups.

Research partly supported by the project SVV-2020-260589 and by an institutional SFG grant.
Let $pq(n)$ denote the number of paramedial quasigroups of order $n$ and $pq(G)$ the number of paramedial quasigroups that admit an affine form over a group $G$, up to isomorphism (see Section 2 for the definition of an affine form). The main result of the present paper can be stated as follows.

**Theorem 1.1.** For every odd prime $p$,

\[
pq(Z_p^k) = 2^{p^k} - p^k - 1 + k - 2 \sum_{i=0}^{k-2} p^i,
\]

\[
pq(Z_2^2) = 4p^2 - 2.
\]

Moreover, $pq(Z_{2^k}) = 2^{k+1}$ for $k > 2$, $pq(Z_4) = 4$, $pq(Z_2) = 1$ and $pq(Z_2^2) = 7$.

**Corollary 1.2.** For every odd prime $p$,

\[
pq(p) = 2p - 1,
\]

\[
pq(p^2) = 6p^2 - p - 1.
\]

The affine forms of the quasigroups over $Z_p^2$ can be found in Table 2, except for one case, in which the quasigroups were enumerated using Burnside’s lemma without finding them explicitly.

The proof of Theorem 1.1 occupies most of the paper. In Section 2 we describe the enumeration method. In Section 3 we apply the method to cyclic groups and in Section 4 to elementary abelian groups of dimension 2.

All quasigroups of prime order are simple. Simple paramedial quasigroups of prime square order will be classified in Section 5, the results are summarized in Table 3.

2. **Enumeration method**

Given an abelian group $G = (G, +)$, automorphisms $\varphi, \psi$ of $G$ and an element $c \in G$, define a new operation $\ast$ on the set $G$ by

\[ x \ast y = \varphi(x) + \psi(y) + c. \]

The resulting quasigroup $(G, \ast)$ is said to be affine over the group $G$ and it will be denoted by $\text{Aff}(G, +, \varphi, \psi, c)$; the quintuple $(G, +, \varphi, \psi, c)$ is called an affine form of $(G, \ast)$.

**Theorem 2.1** (Němec and Kepka [11, Theorem 9]). A quasigroup $(Q, \ast)$ is paramedial if and only if there is an abelian group $G = (G, +)$, a pair of automorphisms $\varphi, \psi$ of $G$ satisfying $\varphi^2 = \psi^2$, and $c \in G$ such that $Q = \text{Aff}(G, +, \varphi, \psi, c)$.

It follows from the classification of finite abelian groups that $pq(G \times H) = pq(G) \cdot pq(H)$ whenever $G, H$ are abelian groups of coprime order (see [7] for a gentle introduction into automorphisms of finite abelian groups). Since isotopic groups are isomorphic [14, Proposition 1.4], a paramedial quasigroup cannot admit affine forms over two non-isomorphic groups, and thus $pq(n) = \sum pq(G)$ where the sum runs over all isomorphism representatives of abelian groups of order $n$. These two observations imply that the function $pq(n)$ is multiplicative.

We will follow the enumeration procedure described in detail in [17]. It is based on the following theorem, which is a special case of [6, Theorem 3.2] for paramedial quasigroups.

**Theorem 2.2.** Let $G$ be an abelian group. The isomorphism classes of paramedial quasigroups affine over $G$ are in one-to-one correspondence with the elements of the set

\[ \{(\varphi, \psi, c) : \varphi \in X, \psi \in Y_{\varphi}, c \in G_{\varphi, \psi}\}, \]

where

- $X$ is a set of conjugacy class representatives of the group $\text{Aut}(G)$,
• $Y_\varphi$ is a set of orbit representatives of the conjugation action of the centralizer $C_{\text{Aut}(G)}(\varphi)$ on the set $S_\varphi = \{\psi \in \text{Aut}(G) : \psi^2 = \varphi^2\}$,

• $G_{\varphi,\psi}$ is a set of orbit representatives of the natural action of $C_{\text{Aut}(G)}(\varphi) \cap C_{\text{Aut}(G)}(\psi)$ on the set $G/\text{Im}(1 - \varphi - \psi)$.

Every triple $(\varphi, \psi, c)$ yields a paramedial quasigroup $\text{Aff}(G, \varphi, \psi, c)$, hence, an explicit construction of the sets $X, Y_\varphi, G_{\varphi,\psi}$ provides an explicit construction of the quasigroups.

3. Enumeration over cyclic groups

In the present section, we apply Theorem 2.2 on the cyclic group $G = \mathbb{Z}_{p^k}$ for $p$ prime number. We will identify automorphisms with the corresponding invertible elements modulo $p^k$, i.e., $\text{Aut}(\mathbb{Z}_{p^k}) = \mathbb{Z}^*_p = \{a \in \mathbb{Z}_{p^k} : p \nmid a\}$.

Proof of Theorem 1.1: case $pq(\mathbb{Z}_{p^k})$. Since the automorphism group is commutative, the conjugation action is trivial and we have to consider every pair $(\varphi, \psi) \in \mathbb{Z}^*_{p^k} \times \mathbb{Z}^*_{p^k}$ such that $\varphi^2 = \psi^2$. For each pair, we consider a complete set of orbit representatives $G_{\varphi,\psi}$ of the action of $\mathbb{Z}^*_p$ on $\mathbb{Z}^*_p/\text{Im}(1 - \varphi - \psi)$.

Case $p$ odd. The equality $\varphi^2 = \psi^2$ in $\mathbb{Z}_{p^k}$ is equivalent to $(\varphi + \psi)(\varphi - \psi) = 0$, therefore the only possible cases are:

1. $\psi = -\varphi$
2. $\psi = \varphi$
3. $p \mid \varphi + \psi$ and $p \mid \varphi - \psi$

The last case implies that $p \mid 2\varphi$. Since $p$ is odd, we have a contradiction with $\varphi \in \mathbb{Z}^*_p$. We will consider the first two cases.

Case $\psi = -\varphi$. The group $\mathbb{Z}^*_p/\text{Im}(1 - \varphi - \psi)$ is trivial, hence we choose $G_{\varphi,\psi} = \{0\}$ and the number of possible triples $(\varphi, \psi, c)$ is

$$p^k - p^{k-1}.$$

Case $\psi = \varphi$. Then $\text{Im}(1 - 2\varphi) = p^i\mathbb{Z}_{p^k}$, where $p^i = \gcd(1 - 2\varphi, p^k)$.

Subcase $i = 0$: $\text{Im}(1 - 2\varphi) = \mathbb{Z}_{p^k}$ and $p \nmid 1 - 2\varphi$, hence $\varphi \equiv 2^{-1} \pmod{p}$. The group $\mathbb{Z}^*_p/\text{Im}(1 - 2\varphi)$ is trivial and we choose $G_{\varphi,\psi} = \{0\}$. The number of possible automorphisms $\varphi$ and also the number of corresponding triples $(\varphi, \psi, c)$ is

$$p^k - 2p^{k-1}.$$

Subcase $i \in \{1, \ldots, k-1\}$ (only for $k > 1$):

$\text{Im}(1 - 2\varphi)$ is equal to $p^i\mathbb{Z}_{p^k}$ if and only if $p^i \mid 1 - 2\varphi$ and $p^{i+1} \nmid 1 - 2\varphi$, equivalently $\varphi \equiv 2^{-1} \pmod{p^i}$ and $\varphi \neq 2^{-1} \pmod{p^{i+1}}$. The elements of $\mathbb{Z}^*_p$ act on the representatives of cosets in $\mathbb{Z}^*_p/\text{Im}(1 - 2\varphi)$ by multiplication, therefore we can choose the set $G_{\varphi,\psi}$ consisting of zero and the powers of $p$, in particular $G_{\varphi,\psi} = \{0, p^0, \ldots, p^{i-1}\}$. The number of possible triples $(\varphi, \psi, c)$ in this case is

$$(p^{k-i} - p^{k-i-1})(i + 1).$$

Subcase $i = k$:

$\text{Im}(1 - 2\varphi) = \{0\}$, which occurs if and only if $\varphi = 2^{-1}$ in $\mathbb{Z}^*_p$. Similarly to the previous case, we can choose $G_{\varphi,\psi} = \{0, p^0, \ldots, p^{k-1}\}$. The number of possibilities in this case is equal to the number of possible constants $c$, which is

$$k + 1.$$
We will show that the number of pairs \((k, l)\) is
\[
\frac{1}{2}k^2 - kl + \frac{1}{2}l^2 = k^2 - 2k + 1 + \frac{1}{2}l^2 - 2l + 1
\]
which, after rearrangement, gives
\[
2p^k - 3p^{k-1} + (2p^{k-1} + p^{k-2} + p^{k-3} + \cdots + p + 1) = 2p^k - p^{k-1} + \sum_{i=0}^{k-2} p^i,
\]
which is the value of \(pq(Z_p^k)\).

**Case** \(p = 2\). The special cases with \(k = 1, 2\) are straightforward and left to the reader. We count the number \(pq(Z_{2^k})\) for \(k > 2\). The automorphism group decomposes as \(\text{Aut}(Z_{2^k}) = Z_{2^k}^+ \rtimes Z_2 \times Z_2\), let us denote the isomorphism \(f : Z_{2^k}^+ \rightarrow Z_2 \times Z_2\). Then every pair of automorphisms \((\varphi, \psi)\) corresponds to the pair \((f(\varphi), f(\psi))\), where \(f(\varphi) = (a_1, a_2), f(\psi) = (b_1, b_2), a_1, b_1 \in Z_2\) and \(a_2, b_2 \in Z_2\). Reformulating the condition \(\varphi^2 = \psi^2\) in terms of this isomorphism, we get the equality \(2(a_1, a_2) = 2(b_1, b_2)\), which holds if and only if
\[
a_2 \equiv b_2 \pmod{2^{k-3}}.
\]

For a fixed element \(\varphi \in \text{Aut}(Z_{2^k})\), there are precisely two elements \(b_2 \in Z_2\) satisfying the stated condition. Since the element \(b_1 \in Z_2\) can be chosen arbitrarily, there are four possible choices of the automorphism \(\psi \in \text{Aut}(Z_{2^k})\).

It remains to determine the set \(G_{\varphi, \psi}\). Since \(2 \nmid 1 - \varphi - \psi\), we get \(\text{Im}(1 - \varphi - \psi) = Z_{2^k}\), hence \(Z_{2^k}/\text{Im}(1 - \varphi - \psi)\) is a trivial group and we can choose \(G_{\varphi, \psi} = \{0\}\). Therefore, the number of possible triples \((\varphi, \psi, c)\) is
\[
(2^k - 2^{k-1}) \cdot 4 = 2^{k+1}.
\]

\[\square\]

4. **Enumeration over elementary abelian groups of dimension 2**

4.1. **An auxiliary number-theoretic result.** In this subsection we state a number-theoretic result about the number of solutions of a particular equation in the field \(Z_p\), which will be used in Subsection 4.3. The result is obtained by methods from [II Section 2].

Let \(p\) be an odd prime number and \(a \in Z_p\) a non-square modulo \(p\) (in particular, \(a \neq 0\)). We want to determine the number of solutions of the equation
\[
q(k, l) = k^2 - al^2 + (1 - 2a)l - a = 0.
\]
We will show that the number of pairs \((k, l) \in Z_p^2\) satisfying the equation is \(p + 1\).

Let us denote \(x = (k, l)^T\) and \(M = \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}\). Then we can restate the equation as follows:
\[
q(x) = x^T M x + (0, 1 - 2a)x - a = 0.
\]
For any vector \(s\), the equations \(q(x) = 0\) and \(q'(x) = q(x + s) = 0\) have the same number of solutions. Let \(s = -\frac{1}{2}M^{-1} \begin{pmatrix} 0 \\ 1 - 2a \end{pmatrix}\). Simplifying the equation, we obtain (we use symmetry of the matrices \(M\) and \(M^{-1}\))
\[
q'(x) = (x + s)^T M (x + s) + (0, 1 - 2a)(x + s) - a
= x^T M x + (s^T M s + (0, 1 - 2a)s - a)
= k^2 - al^2 + (2^{-2}a^{-1} - 1).
\]
The number of solutions \((k, l)\) follows from the following theorem \((2^{-2}a^{-1} - 1 \neq 0\), since \(a\) is a non-square).
Theorem 4.1 \([\mathbb{I}]\) \(\text{Theorem 2.9}\). Let \(p\) be an odd prime and \(g(x, y) = rx^2 + sy^2 + t\) be a polynomial over \(\mathbb{Z}_p\) satisfying the following:

- \(t \neq 0\),
- \(-rs\) is a non-square modulo \(p\) (in particular \(rs \neq 0\)).

Then the number of solutions \((x, y)\) of the equation \(g(x, y) = 0\) is \(p + 1\).

4.2. Calculating square roots of matrices. We will introduce a method for calculating square roots of \(2 \times 2\) matrices over the field \(\mathbb{Z}_p\) for odd primes \(p\). The method is based on the Cayley-Hamilton theorem and is adopted from \([12]\).

Let \(A\) be a \(2 \times 2\) matrix over \(\mathbb{Z}_p\), our aim is to find all matrices \(\sqrt{A}\) satisfying \((\sqrt{A})^2 = A\). In this context, the identity matrix will be denoted by \(I\).

The Cayley-Hamilton theorem for \(2 \times 2\) matrices asserts that

\[
M^2 - \text{tr}(M)M + \text{det}(M)I = 0.
\]

Let us denote \(\tau = \text{tr}(\sqrt{A})\), \(\delta = \text{det}(\sqrt{A})\), \(T = \text{tr}(A)\), \(\Delta = \text{det}(A)\). Clearly \(\delta^2 = \Delta\). Setting \(M = \sqrt{A}\) in (1) yields

\[
(2) \quad A = \tau \sqrt{A} - \delta I.
\]

If we assume \(\tau \neq 0\), we obtain

\[
(3) \quad \sqrt{A} = \frac{1}{\tau}(A + \delta I).
\]

In order to express \(\tau\), we use the Cayley-Hamilton theorem for \(M = A\), which gives

\[
(4) \quad TA - \Delta I = A^2 = (\tau \sqrt{A} - \delta I)^2 = \tau^2 A - 2\tau \delta \sqrt{A} + \delta^2 I = \tau^2 A - 2\delta(A + \delta I) + \delta^2 I = \tau^2 A - 2\delta A - \Delta I,
\]

and thus \(TA = (\tau^2 - 2\delta)A\), which implies \(T = \tau^2 - 2\delta\). For every square \(x \in \mathbb{Z}_p\), we choose an element \(y\) such that \(y^2 = x\) and denote it by \(\sqrt{x}\). If the corresponding square roots in \(\mathbb{Z}_p\) exist, we can express the square roots of \(A\) in the form

\[
(5) \quad \sqrt{A} = \frac{\pm 1}{\sqrt{T + 2\delta}}(A + \delta I),
\]

where \(\delta = \pm \sqrt{\Delta}\). Therefore, we obtain at most four square roots of \(A\) with \(\tau \neq 0\).

Case \(A \neq cI\), \(c \in \mathbb{Z}_p\): Since \(A\) is not a multiple of the identity matrix, it follows from (2) that \(\tau \neq 0\). Therefore we obtain all square roots of \(A\) from (5).

Case \(A = cI\) for \(c \in \mathbb{Z}_p\): We will search for all matrices \(\sqrt{A}\) in the following form:

\[
\sqrt{A} = \begin{pmatrix} k & l \\ m & n \end{pmatrix}, \quad \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} = \begin{pmatrix} k & l \\ m & n \end{pmatrix}^2 = \begin{pmatrix} k^2 + lm & l(k + n) \\ m(k + n) & n^2 + lm \end{pmatrix}
\]

If \(\tau \neq 0\), then it follows from (2) that \(\delta \neq -c\), hence \(\delta = c\). Then if \(c\) is a square, by (5) we obtain square roots in the form

\[
\frac{\pm 1}{\sqrt{2c + 2c}}(cI + cI) = \pm \begin{pmatrix} \sqrt{c} & 0 \\ 0 & \sqrt{c} \end{pmatrix}
\]

Otherwise, \(\tau = 0\), i.e., \(n = -k\), so we obtain square roots in the form

\[
\begin{pmatrix} k & l \\ m & -k \end{pmatrix}, \quad k, l, m \in \mathbb{Z}_p, \quad k^2 + lm = c.
\]
\[
\begin{array}{|c|c|}
\hline
\varphi & C(\varphi) \\
\hline
\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, a \neq 0 & GL(2,p) \\
\hline
\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, 0 < a < b & \left\{ \begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix} : u, v \neq 0 \right\} \\
\hline
\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}, a \neq 0 & \left\{ \begin{pmatrix} u & v \\ 0 & u \end{pmatrix} : u \neq 0 \right\} \\
\hline
\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}, x^2 - bx - a \text{ irreducible} & \left\{ \begin{pmatrix} u & v \\ av & u + bv \end{pmatrix} : u \neq 0 \text{ or } v \neq 0 \right\} \\
\hline
\end{array}
\]

Table 1. Conjugacy class representatives in \( GL(2,p) \) and their centralizer subgroups.

4.3. Enumeration. Now, we are ready to apply Theorem 2.2 on the group \( G = \mathbb{Z}_p^2 \). We will identify automorphisms with their matrices, considering \( Aut(G) = GL(2,p) \).

**Proof of Theorem 2.1.** Let \( G = \mathbb{Z}_p^2 \) with \( p \) odd (the case \( p = 2 \) is left to the reader)

The set \( X \) of conjugacy class representatives in \( Aut(G) = GL(2,p) \) can be chosen as in Table 1. The four types of representatives correspond to the diagonalizable matrices with one eigenvalue, the diagonalizable matrices with two distinct eigenvalues, the non-diagonalizable matrices with an eigenvalue in \( \mathbb{Z}_p \), and the non-diagonalizable matrices with eigenvalues in the quadratic extension, respectively. The last case is represented by matrices \( \begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix} \) such that the polynomial \( x^2 - bx - a \) is irreducible over \( \mathbb{Z}_p \).

The centralizer subgroups are also displayed in Table 1 (here and later on, we will omit the index in the centralizer notation).

For every matrix \( \varphi \in X \) we will do the following: We determine the set \( S_\varphi \), using the method from Subsection 4.2 for calculating the square roots \( \psi \) of the matrices \( \varphi^2 \). Then we will choose the orbit representatives of the conjugation action of the centralizer \( C(\varphi) \) on the set \( S_\varphi \) and form the set \( Y_\varphi \). Finally, we will determine the set \( G_{\varphi,\psi} \) and calculate the number of triples \( (\varphi, \psi, c) : \varphi \in X, \psi \in Y_\varphi, c \in G_{\varphi,\psi} \). The results are summarized in Table 2.

The size of the set \( G_{\varphi,\psi} \) will be determined by the following procedure: If \( 1 - \varphi - \psi \) is a regular matrix, then \( G/Im(1 - \varphi - \psi) \) is a trivial group and we can choose \( G_{\varphi,\psi} = \{0\} \). If the rank of the matrix \( 1 - \varphi - \psi \) is one, then \( G/Im(1 - \varphi - \psi) \cong \mathbb{Z}_p \) and since all of the centralizer subgroups contain all matrices \( \begin{pmatrix} u & 0 \\ 0 & u \end{pmatrix}, u \neq 0 \), we can take \( G_{\varphi,\psi} = \{0, w\} \), where \( |w| \) is any non-zero element of \( G/Im(1 - \varphi - \psi) \) (i.e., \( w \notin Im(1 - \varphi - \psi) \)). If the rank of the matrix \( 1 - \varphi - \psi \) is zero, then the situation depends on the centralizers \( C(\varphi), C(\psi) \) and will be discussed separately in that case.

**Case** \( \varphi = \begin{pmatrix} a \\ 0 \\ a \end{pmatrix} \):

\[
S_\varphi = \left\{ \begin{pmatrix} \pm a & 0 \\ 0 & \pm a \end{pmatrix} : \begin{pmatrix} k & 1 \\ m & -k \end{pmatrix} : k^2 + lm = a^2 \right\}
\]

All matrices in \( S_\varphi \) are diagonalizable and the non-diagonal matrices have eigenvalues \( a \) and \( -a \). The centralizer \( C(\varphi) \) is the whole \( GL(2,p) \), therefore we can choose the set of representatives of the conjugation action of \( C(\varphi) \) on \( S_\varphi \) as

\[
Y_\varphi = \left\{ \begin{pmatrix} a \\ 0 \\ a \end{pmatrix}, \begin{pmatrix} a \\ 0 \\ -a \end{pmatrix}, \begin{pmatrix} a \\ 0 \\ -a \end{pmatrix} \right\}.
\]

Now, we will determine the set \( G_{\varphi,\psi} \) for every admissible pair \((\varphi, \psi)\):

- \( \psi = \begin{pmatrix} a \\ 0 \\ a \end{pmatrix}, 1 - \varphi - \psi = \begin{pmatrix} 1 - 2a \\ 0 \\ 1 - 2a \end{pmatrix} \)

The matrix \( 1 - \varphi - \psi \) is regular if and only if \( a \neq 2^{-1} \). Then \( |G_{\varphi,\psi}| = 1 \) and this case contributes to \( pq(G) \) by \( p - 2 \) possible triples \((\varphi, \psi, c)\). Otherwise, \( rank(1 - \varphi - \psi) = 0 \) and necessarily \( a = 2^{-1} \). Since \( C(\varphi) \cap C(\psi) = GL(2,p) \), it is possible to choose \( G_{\varphi,\psi} = \{0, w\} \),
where \( w \) is an arbitrary non-zero vector. Therefore, this case contributes to \( pq(G) \) by 2 possible triples.

- \( \psi = \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}, \quad 1 - \varphi - \psi = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \)
  
  For any \( a \) is rank\((1 - \varphi - \psi)\) = 2, so \( |G_{\varphi,\psi}| = 1 \) and the number of possible triples \((\varphi, \psi, c)\) in this case is \( p - 1 \).

- \( \psi = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad 1 - \varphi - \psi = \begin{pmatrix} 1 - 2a & 0 \\ 0 & 1 \end{pmatrix} \)
  
  Similarly as in the first case, rank\((1 - \varphi - \psi)\) = 2 if and only if \( a \neq 2^{-1} \) and then there are \( p - 2 \) admissible triples \((\varphi, \psi, c)\). Otherwise, rank\((1 - \varphi - \psi)\) = 1 and we choose \( G_{\varphi,\psi} = \{0, w\}, \ w \notin \text{Im}(1 - \varphi - \psi), \) and get 2 other triples.

Summing up the contributions in this case we get \((p - 2) + 2 + (p - 1) + (p - 2) + 2 = 3p - 1 \).

**Case** \( b \neq 0 \): We need to distinguish two subcases.

**Subcase** \( b = -a \):

\[ S_{\varphi} = \left\{ \begin{pmatrix} \pm a & 0 \\ 0 & \mp b \end{pmatrix}, \begin{pmatrix} \pm a & 0 \\ 0 & \mp b \end{pmatrix} \right\} \]

Every \( \psi \in S_{\varphi} \) commutes with the elements of \( C(\varphi) \), therefore we choose \( Y_{\varphi} = S_{\varphi} \).

**Subcase** \( b = -a \):

\[ S_{\varphi} = \left\{ \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}, \begin{pmatrix} k & 0 \\ 0 & -k \end{pmatrix}; \ k^2 + lm = a^2 \right\} \]

All diagonal matrices in \( S_{\varphi} \) commute with the elements of \( C(\varphi) \), hence they are all elements of \( Y_{\varphi} \).

In the non-diagonal matrices, we can change the non-zero non-diagonal elements by conjugation to any non-zero value, therefore we include a representative for matrices with \( l = 0 \) and representatives for matrices with \( l \neq 0 \). Hence we can choose the set

\[ Y_{\varphi} = \left\{ \begin{pmatrix} \pm a & 0 \\ 0 & \mp a \end{pmatrix}, \begin{pmatrix} \pm a & 0 \\ 0 & \mp a \end{pmatrix}; \begin{pmatrix} k & 0 \\ 0 & -k \end{pmatrix} \right\} \]

Now, we are ready to discuss the structure of the set \( G_{\varphi,\psi} \) depending on the choice of automorphisms \( \varphi, \psi \). Firstly we count the triples \((\varphi, \psi, c)\) where the matrix \( \psi \) is diagonal for both subcases together, independently of the value of \( b \).

- \( \psi = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, \quad 1 - \varphi - \psi = \begin{pmatrix} 1 - 2a & 0 \\ 0 & 1 - 2b \end{pmatrix} \)
  
  The matrix \( 1 - \varphi - \psi \) is regular if and only if \( a, b \neq 2^{-1} \). Under these conditions, \( |G_{\varphi,\psi}| = 1 \) and number of admissible triples \((\varphi, \psi, c)\) is \( \binom{p-2}{2} \). If this condition is not satisfied, rank\((1 - \varphi - \psi)\) = 1 (because \( a < b \)) and \( a = 2^{-1} \) or \( b = 2^{-1} \). In this case we choose \( G_{\varphi,\psi} = \{0, w\}, \ w \notin \text{Im}(1 - \varphi - \psi) \), and number of possible triples is \( 2(p - 2) \).

- \( \psi = \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}, \quad 1 - \varphi - \psi = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \)
  
  Rank of the matrix \( 1 - \varphi - \psi \) is always two, therefore \( |G_{\varphi,\psi}| = 1 \) and this case contributes to \( pq(G) \) by \( \binom{p-2}{1} \).

- \( \psi = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, \quad 1 - \varphi - \psi = \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix} \)
  
  If \( b \neq 2^{-1} \), then rank\((1 - \varphi - \psi)\) = 2 and we have \( |G_{\varphi,\psi}| = 1 \). This gives \( c_1 \) admissible triples \((\varphi, \psi, c)\), where by \( c_1 \) we denote the number of pairs \((a, b)\) satisfying \( 0 < a < b \) and \( b \neq 2^{-1} \). If \( b = 2^{-1} \), rank\((1 - \varphi - \psi)\) = 1 and we choose \( G_{\varphi,\psi} = \{0, w\}, \ w \notin \text{Im}(1 - \varphi - \psi) \), which yields \( 2d_1 \) triples \((\varphi, \psi, c)\), where \( d_1 \) denotes the number of possibilities to choose \( a \) that satisfies \( 0 < a < 2^{-1} \).

- \( \psi = \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}, \quad 1 - \varphi - \psi = \begin{pmatrix} 1 - 2a & 0 \\ 0 & 1 \end{pmatrix} \)
  
  Analogously to the previous case, if \( a \neq 2^{-1} \), then the number of possible triples is \( c_2 \), which denotes the number of pairs \((a, b)\) satisfying \( 0 < a < b \) and \( a \neq 2^{-1} \). Conversely, if \( a = 2^{-1} \), we get \( 2d_2 \) possible triples, where \( d_2 \) denotes the number of possible choices of \( b \) satisfying \( 2^{-1} < b \).

Now we can calculate the values \( c_1 + c_2 \) and \( d_1 + d_2 \). The value \( c_1 + c_2 = 2\binom{p-2}{2} + (p - 2) \) corresponds to the choice of \( 0 < a < b \) satisfying that \( a \neq 2^{-1} \) or \( b \neq 2^{-1} \), with the choices where
a \neq 2^{-1} and b \neq 2^{-1} counted twice. The value \( d_1 + d_2 = p - 2 \) is equal to the number of pairs \((a, b)\), where \( a = 2^{-1} \) or \( b = 2^{-1} \).

We can now move to the pairs of automorphisms \((\varphi, \psi)\), which are specific for the subcase \( b = -a \), therefore we will consider \( \varphi = \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix} \).

- \( \psi = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, 1 - \varphi - \psi = \begin{pmatrix} 1 - 2a & 0 \\ 0 & 1 - 2a \end{pmatrix} \)

  Matrix \( 1 - \varphi - \psi \) is regular if and only if \( a \neq \pm 2^{-1} \). Then \( |G_{\varphi, \psi}| = 1 \) and the number of contributed triples \((\varphi, \psi, c)\) is equal to the number of possible automorphisms \( \varphi \), which is \( \frac{a - 1}{2} - 1 = \frac{a - 3}{2} \), because \( 0 < a < -a \). Otherwise, rank\((1 - \varphi - \psi) = 1 \) and \( a = \pm 2^{-1} \). Since \( 0 < a < -a \), there is only one possible choice of \( a \). Under these conditions, we choose \( G_{\varphi, \psi} = \{0, w\} \), where \( w \notin \text{Im}(1 - \varphi - \psi) \), and get 2 possible triples.

- \( \psi = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, 1 - \varphi - \psi = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \)

  The matrix \( 1 - \varphi - \psi \) is always regular, therefore \( |G_{\varphi, \psi}| = 1 \) and this case contributes to \( \text{pq}(G) \) by \( \frac{p - 1}{2} \), because condition \( 0 < a < -a \) is satisfied by half of the non-zero elements in \( \mathbb{Z}_p \).

- \( \psi = \begin{pmatrix} 1 & 0 \\ a & -1 \end{pmatrix} \), \( k \in \mathbb{Z}_p \), \( 1 - \varphi - \psi = \begin{pmatrix} 1 - a - k & -1 \\ k^2 - a^2 & 1 + a + k \end{pmatrix} \)

  Clearly, we have rank\((1 - \varphi - \psi) > 0 \). In particular, rank\((1 - \varphi - \psi) = 2 \) if and only if \( \det(1 - \varphi - \psi) \neq 0 \), equivalently \( k \neq 2^{-1}a^{-1} - a \). Then \( |G_{\varphi, \psi}| = 1 \) and contribution to the value \( \text{pq}(G) \) is \( \frac{(p - 1)^2}{2} \), because \( 0 < a < -a \). Conversely, if \( \det(1 - \varphi - \psi) = 0 \), then rank\((1 - \varphi - \psi) = 1 \) and \( k = 2^{-1}a^{-1} - a \). Hence we choose \( G_{\varphi, \psi} = \{0, w\} \), where \( w \notin \text{Im}(1 - \varphi - \psi) \), and the number of admissible triples \((\varphi, \psi, c)\) is \( 2 \cdot \frac{p - 1}{2} = p - 1 \).

Using the values of the expressions \( c_1 + c_2 \) and \( d_1 + d_2 \) calculated above, we count the total number of contributed triples \((\varphi, \psi, c)\) in this case: \( p^{-2} + 2(p - 2) = \left(\frac{p - 1}{2}\right) + 1 + 2 + 2 + 2 + \frac{p - 3}{2} + 2 + \frac{p - 1}{2} + \frac{(p - 1)^2}{2} = \frac{5}{2}p^2 - 3p - \frac{1}{2} \).

Case \( \varphi = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} \): Using the method introduced in Subsection 4.2 we obtain

\[ S_\varphi = \{ \pm \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} \} \]

Since both matrices in \( S_\varphi \) commute with the matrices in \( C(\varphi) \), we choose \( Y_\varphi = S_\varphi \).

Finally, we can choose the sets \( G_{\varphi, \psi} \) for the pairs of the automorphisms \((\varphi, \psi)\) and find the number of contributed quasigroups.

- \( \psi = \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}, 1 - \varphi - \psi = \begin{pmatrix} 1 - 2a & -2 \\ 0 & 1 - 2a \end{pmatrix} \)

  We have rank\((1 - \varphi - \psi) = 2 \) if and only if \( a \neq 2^{-1} \). Then \( |G_{\varphi, \psi}| = 1 \) and the number of contributed triples is \( p - 2 \). Otherwise, it holds that rank\((1 - \varphi - \psi) = 1 \) and \( a = 2^{-1} \), hence we choose \( G_{\varphi, \psi} = \{0, w\} \), where \( w \notin \text{Im}(1 - \varphi - \psi) \), and get 2 possible triples.

- \( \psi = \begin{pmatrix} a & -1 \\ 0 & a \end{pmatrix}, 1 - \varphi - \psi = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \)

  For every \( a \) holds that rank\((1 - \varphi - \psi) = 2 \), therefore there are as many admissible triples \((\varphi, \psi, c)\) as possible values of \( a \), which is \( p - 1 \).

This case contributes to \( \text{pq}(G) \) the total of \( (p - 2) + 2 + (p - 1) = 2p - 1 \) triples \((\varphi, \psi, c)\).

Case \( \varphi = \begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix} \): The set \( S_\varphi \) clearly contains the matrices \( \pm \varphi \). Both matrices commute with the elements of \( C(\varphi) \) and therefore have to be elements of the set \( Y_\varphi \).

Consider \( \psi \in Y_\varphi \). We distinguish the following two cases.

Subcase \( \psi = \pm \varphi \):

- \( \psi = \begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}, 1 - \varphi - \psi = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \)

  Determinant of the matrix \( 1 - \varphi - \psi = 1 - 2b - 4a \), hence it is singular if and only if \( 4a = 1 - 2b \), equivalently \( b^2 + 4a = (b - 1)^2 \), which contradicts irreducibility of the polynomial \( x^2 - bx - a \). Therefore, \( |G_{\varphi, \psi}| = 1 \). Since there are \( \frac{1}{2}(p^2 - p) \) monic irreducible polynomials of degree 2 over \( \mathbb{F}_p \), this case yields \( \frac{1}{2}(p^2 - p) \) triples \((\varphi, \psi, c)\).
• $\psi = \left( \begin{smallmatrix} 0 & -1 \\ a & b \end{smallmatrix} \right)$, $1 - \varphi - \psi = \left( \begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix} \right)$

The matrix $1 - \varphi - \psi$ is regular for all $a, b$, therefore, $|G_{\varphi, \psi}| = 1$ and similarly to the previous case, this case contributes to $pq(G)$ by $\frac{1}{2}(p^2 - p)$.

Subcase $\psi \neq \pm \varphi$: Using the method from Subsection 4.2 and that $b^2 + 4a$ is a non-square modulo $p$ (because of the irreducibility of $x^2 - bx - a$), we observe that if $b \neq 0$, then $Y_{\varphi} = S_{\varphi} = \{ \pm \left( \begin{smallmatrix} 0 & 1 \\ a & b \end{smallmatrix} \right) \}$. Therefore necessarily $b = 0$ in this case and $\varphi = \left( \begin{smallmatrix} 0 & 1 \\ a & 0 \end{smallmatrix} \right)$ with a non-square modulo $p$. The set of all square roots of $\varphi^2$ (including $\pm \varphi$) is then

$$S_{\varphi} = \left\{ \left( l^{-1}(a-k^2) \begin{array}{c} k \\ -l \end{array} \right) : l \neq 0 \right\}.$$

In this case, we are not able to list the orbit representatives of the conjugation action of $C(\varphi)$ on the set $S_{\varphi}$. Instead, we will use Burnside’s lemma to find the number of triples $(\varphi, \psi, c)$. Firstly, we find the number of the conjugacy classes and their cardinalities. Then, independently of the particular conjugacy class representatives, we find the cardinality of the set $G_{\varphi, \psi}$ depending on the conjugacy class of $\psi$.

If we set $k = 0$, $l = 1$ in the matrix $\left( l^{-1}(a-k^2) \begin{array}{c} 1 \\ -l \end{array} \right)$, we get $\left( \begin{smallmatrix} 0 & 1 \\ a & 0 \end{smallmatrix} \right)$. Similarly, the choice $k = 0$, $l = -1$ leads to the matrix $\left( \begin{smallmatrix} 0 & -1 \\ -a & 0 \end{smallmatrix} \right)$. These two matrices are equal to $\pm \varphi$ and represent single element conjugacy classes.

Let us denote matrices $C(u, v) = \left( \begin{smallmatrix} u & v \\ av & u \end{smallmatrix} \right)$ from $C(\varphi)$ and $S(k, l) = \left( l^{-1}(a-k^2) \begin{array}{c} 1 \\ -l \end{array} \right)$ from $S_{\varphi}$. It is straightforward to find for which values of $u, v, k, l$ the equality $C(u, v)S(k, l)C(u, v)^{-1} = S(k, l)$ holds. If $v = 0$, then the equality holds for all admissible values $k, l$. Then $C(u, 0)$ commutes with all elements in $S_{\varphi}$. If $v \neq 0$, then the equality holds if and only if $k = 0$ and $l = \pm 1$.

This observation has two crucial consequences. Firstly, we can use it to determine the number of orbits of the conjugation action of $C(\varphi)$ on $S_{\varphi}$. The centralizer $C(\varphi)$ contains $p - 1$ matrices of the form $C(u, 0)$, each of them with $|S_{\varphi}| = p(p - 1)$ fixed points. The remaining $p(p - 1)$ matrices in $C(\varphi)$ are in the form $C(u, v)$, where $v \neq 0$, and have only 2 fixed points, in particular $S(0, 1)$ and $S(0, -1)$. For a matrix $C \in C(\varphi)$ denote $f_C$ the number of its fixed points of the conjugation action. Then we obtain from Burnside’s lemma that the number of orbits of this action is

$$\frac{1}{|C(\varphi)|} \sum_{C \in C(\varphi)} |f_C| = \frac{1}{p^2 - 1} \left( p(p - 1)(p - 1) + 2p(p - 1) \right) = p.$$

The second consequence is the sizes of the orbits. We already know that the matrices $S(0, \pm 1)$ have single element orbits. Using the observation above, we obtain that the other elements in $S_{\varphi}$ are stabilized only by $p - 1$ diagonal matrices $C(u, 0)$, $u \neq 0$. Therefore, the sizes of the remaining $p - 2$ orbits are equal to $|C(\varphi)|/(p - 1) = p + 1$. Overall, the conjugation action of $C(\varphi)$ on $S_{\varphi}$ has two single element orbits and $p - 2$ orbits with $p + 1$ elements.

Now we are able to find the size of the set $G_{\varphi, \psi}$ for the pairs of automorphisms $(\varphi, \psi)$, $\psi \in Y_{\varphi} \setminus \{ \pm \varphi \}$. Consider $\psi = \psi(k, l) = \left( l^{-1}(a-k^2) \begin{array}{c} k \\ -l \end{array} \right)$ for some $k, l$. Then we have

$$1 - \varphi - \psi = \left( \begin{smallmatrix} 1 - k \\ -a - l^{-1}(a-k^2) \end{smallmatrix} \begin{array}{c} -1 - l \\ 1 + k \end{array} \right).$$

At least one of the values $1 - k$ a $1 + k$ is nonzero, hence the rank of the matrix $1 - \varphi - \psi$ is either one or two, and the rank is one if and only if $\det(1 - \varphi - \psi) = 0$. If the matrix is regular, then $|G_{\varphi, \psi}| = 1$ and there is only one possible constant $c$ for the pair $(\varphi, \psi)$. Otherwise, we choose $G_{\varphi, \psi} = \{ 0, w \}$, $w \notin \text{Im}(1 - \varphi - \psi)$, so there are two possible constants $c \in G_{\varphi, \psi}$.

The determinant

$$\det(1 - \varphi - \psi) = (1 - k)(1 + k) - (-1 - l)(-a - l^{-1}(a-k^2))$$

is determined by the choice $k, l$. Then

$$\det(1 - \varphi - \psi) = (1 - k)(1 + k) - (-1 - l)(-a - l^{-1}(a - k^2)) = p + 1 \quad \text{or} \quad (1 - k)(1 + k) - (-1 - l)(-a - l^{-1}(a - k^2)) = 0.$$
is equal to zero if and only if

\[(6) \quad k^2 - al^2 + (1 - 2a)l - a = 0.\]

In Subsection 4.1 we showed that there are precisely \(p + 1\) pairs \((k, l) \in \mathbb{Z}_p^2\) satisfying the equation. Since \(a\) is a non-square, every solution \((k, l)\) satisfies \(l \neq 0\), and therefore correspond to a matrix from \(S_\varphi\). Furthermore, the pairs \((0, 1)\) and \((0, -1)\) do not satisfy the equation \((6)\), hence all solutions \((k, l)\) correspond to matrices \(\psi(k, l)\) with orbits with \(p + 1\) elements in the conjugation action of \(C(\varphi)\) on \(S_\varphi\).

The size of the set \(G_{\varphi, \psi}\), where \(\psi = \psi(k, l)\), depends on whether the pair \((k, l)\) satisfies the equation \((6)\). Also, \(|G_{\varphi, \psi}|\) does not depend on the choice of a particular representative \(\psi\) in its orbit, according to Theorem 2.2. Since the equation \((6)\) has precisely \(p + 1\) solutions, all these solutions correspond to the elements of the same orbit, that is, to the one element of the set of orbit representatives \(Y_\varphi\).

We can now find the number of the remaining paramedial quasigroups (i.e., the remaining possible triples \((\varphi, \psi, c)\)). There are \((p - 1)/2\) possible choices of the matrix \(\varphi\) (corresponding to non-squares modulo \(p\)). For every \(\varphi\), there are \(p - 2\) choices of automorphism \(\psi \in Y_\varphi \setminus \{\pm \varphi\}\), and for precisely one \(\psi^* \in Y_\varphi\) holds that \(|G_{\varphi, \psi^*}| = 2\), while for the remaining \(p - 3\) we have \(|G_{\varphi, \psi}| = 1\). The number of the remaining triples \((\varphi, \psi, c), c \in G_{\varphi, \psi}\), is therefore

\[
\frac{p - 1}{2}(1 \cdot 2 + (p - 3) \cdot 1) = \frac{1}{2}p^2 - p + \frac{1}{2}.
\]

Summarized, the case dealing with automorphism \(\varphi\) without eigenvalues in \(\mathbb{Z}_p\) contributes to \(pq(G)\) by \(\frac{p^2 - p + 1}{2} + \frac{p^2 - p + 1}{2} = \frac{3}{2}p^2 - 2p + \frac{1}{2}\).

Summing up all the contributions (see the last column of Table 2), we obtain that the total number is

\[
(3p - 1) + \left(\frac{5}{2}p^2 - 3p - \frac{1}{2}\right) + (2p - 1) + \left(\frac{3}{2}p^2 - 2p + \frac{1}{2}\right) = 4p^2 - 2.
\]

\[\square\]
| \(\varphi\) | \(\psi\) | \(c\) | number |
|---|---|---|---|
| \((a \ 0)\) \(0 < a < b\) | \((0 \ a)\) | \((0 \ 0), \text{ if } a, b \neq 2^{-1}\) | \((p-2)^2\) |
| \((0 \ b)\) | \((0 \ 0)\) | \((1 \ 1), \text{ if } a = 2^{-1} \lor b = 2^{-1}\) | \(2(p-2)\) |
| \((-a \ 0)\) \(0 < a < -b\) | \((0 \ 0)\) | \((0 \ 0), \text{ if } a \neq 2^{-1} \lor b \neq 2^{-1}, \text{ resp.}\) | \((p-1)^2\) |
| \((0 \ -b)\) | \((0 \ 0)\) | \((1 \ 1), \text{ if } a = 2^{-1} \lor b = 2^{-1}, \text{ resp.}\) | \(2(p-2)\) |
| \((\pm a \ 0)\) \(0 < a < b\) | \((0 \ 0)\) | \((0 \ 0), \text{ if } a \neq 2^{-1} \lor b \neq 2^{-1}, \text{ resp.}\) | \((p-2)^2 + p - 2\) |
| \((0 \ \mp b)\) | \|(depends on the choice of the signs)\| | \|(depends on the choice of the signs)\| | \(2(p-2)\) |
| \((a \ 0)\) \(0 < a < -a\) | \((a \ 1)\) | \((0 \ 0), \text{ if } a \neq \pm 2^{-1}\) | \(\frac{p-3}{2}\) |
| \((0 \ -a)\) | \((1 \ -a)\) | \((0 \ 0), \text{ if } a = 2^{-1} \lor a = -2^{-1}, \text{ resp.}\) | \(2\) |
| \((-a \ 0)\) \(0 < a < -a\) | \((0 \ 0)\) | \((0 \ 0), \text{ if } a = 2^{-1} \lor a = -2^{-1}, \text{ resp.}\) | \(\frac{p-1}{2}\) |
| \((0 \ a)\) | \((a \ 1)\) | \((0 \ 0), \text{ if } a \neq 2^{-1}\) | \(p - 1\) |
| \((0 \ a)\) \(a \neq 0\) | \((0 \ a)\) | \((0 \ 0), \text{ if } a = 2^{-1}\) | \(2\) |
| \(-a \ -1\) | \((0 \ 0)\) | \(\frac{p-1}{2}\) | \(p - 1\) |
| \((0 \ 1)\) \(a \neq 0\) | \((0 \ 1)\) | \((0 \ 0), \text{ if } a = 2^{-1}\) | \(p - 1\) |
| \((a \ b)\) \(x^2 - bx - a\) irreducible | \((0 \ -1)\) | \((0 \ 0)\) | \(\frac{p^2-p}{2}\) |
| \((a \ b)\) | \((0 \ -1)\) | \((0 \ 0)\) | \(\frac{p^2-p}{2}\) |
| \((a \ 0)\) \(x^2 - a\) irreducible | \((0 \ 0)\) | \((0 \ 0), \text{ if } a \neq \pm 2^{-1}\) | \(\frac{(p-1)(p-3)}{2}\) |
| \((0 \ 0)\) | \((0 \ 0)\) | \(\text{1 matrix of the form}\) | \(p - 1\) |
| \((0 \ 0)\) \(x^2 - a\) irreducible | \((0 \ 0)\) | \(\text{1 matrix of the form}\) | 
| \((a \ 0)\) \(x^2 - a\) irreducible | \((0 \ 0)\) | \(\text{1 matrix of the form}\) | 
| \((0 \ 0)\) \(x^2 - a\) irreducible | \((0 \ 0)\) | \(\text{1 matrix of the form}\) | 
| \((0 \ 0)\) \(x^2 - a\) irreducible | \((0 \ 0)\) | \(\text{1 matrix of the form}\) | 
| \((0 \ 0)\) \(x^2 - a\) irreducible | \((0 \ 0)\) | \(\text{1 matrix of the form}\) | 
| \((0 \ 0)\) \(x^2 - a\) irreducible | \((0 \ 0)\) | \(\text{1 matrix of the form}\) | 

**Table 2.** Affine forms of simple paramedial quasigroups of order \(p^2\), up to isomorphism \((a, b \in \mathbb{Z}_p)\)
5. Simple paramedial quasigroups of prime square order

In affine quasigroups, quasigroup congruences correspond to subgroups of the underlying group invariant with respect to the defining automorphisms. Formally, it can be stated as follows (and proved fairly easily).

**Proposition 5.1** ([10] Theorems 41 and 42). Let \( Q = \text{Aff}(G, \varphi, \psi, c) \) be an affine quasigroup and \( \alpha \) an equivalence on \( Q \). Then \( \alpha \) is a congruence of \( Q \) if and only if there is a subgroup \( N \leq G \) satisfying \( \varphi(N) = \psi(N) = N \) such that

\[
(a, b) \in \alpha \iff a - b \in N
\]

A quasigroup \( Q \) is called *simple* if it possesses no proper congruences (i.e., every homomorphism from \( Q \) is injective or trivial).

**Corollary 5.2.** An affine quasigroup \( Q = \text{Aff}(G, \varphi, \psi, c) \) is simple if and only if the group \( G \) contains no proper subgroup \( N \) satisfying \( \varphi(N) = \psi(N) = N \).

In particular, the underlying abelian group must not contain any proper characteristic subgroups, hence, must be elementary abelian.

In the rest of the paper, we classify simple paramedial quasigroups over the group \( \mathbb{Z}_p^2 \) by sorting out Table 2. The method is based on the following observation: \( Q = \text{Aff}(\mathbb{Z}_p^2, \varphi, \psi, c) \) is not simple if and only if there is a proper subgroup \( N \leq \mathbb{Z}_p^2 \), i.e., a subspace of dimension 1, which is invariant with respect to \( \varphi, \psi \). In other words, if \( \varphi, \psi \) share a common eigenvector.

The automorphisms \( \varphi \) and \( \psi \), where \( \varphi \) is a matrix without eigenvalues in \( \mathbb{Z}_p \), trivially do not share an eigenvector. For all other choices of \( \varphi \) we can easily conclude from Table 2 that the automorphisms \( \varphi \) and \( \psi \) do not share an eigenvector if and only if \( \varphi = \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix} \) and \( \psi = \begin{pmatrix} k & 1 \\ a^2-k^2 & -k \end{pmatrix} \), \( k \neq \pm a \). In this case, we need to calculate the number of quasigroups \( \text{Aff}(G, \varphi, \psi, c) \), where \( \varphi, \psi \) satisfy the stated condition.

| \( \varphi \) | \( \psi \) | \( c \) | number |
|----------------|----------------|------------|--------|
| \[
\begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}
\] | \[
\begin{pmatrix} k & 1 \\ a^2-k^2 & -k \end{pmatrix}
\] | \[
\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}
\], if \( k \neq 2^{-1}a^{-1} - a \) | \( p^2 - 4p + 5 \) |
| \[
\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}
\] | \[
\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}
\] | \[
\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}
\] | \( p^2 - p \) |
| \[
\begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}
\] | \[
\begin{pmatrix} 0 & 1 \\ l^{-1}(a-k^2) & -k \end{pmatrix}
\] | \[
\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}
\], \( l \neq 0, (k, l) \neq (0, \pm 1) \) | \( (p-1)(p-3) \) |

| \( \varphi \) | \( \psi \) | \( c \) | number |
|----------------|----------------|------------|--------|
| \[
\begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}
\] | \[
\begin{pmatrix} 0 & 1 \\ l^{-1}(a-k^2) & -k \end{pmatrix}
\] | \[
\begin{pmatrix} 0 & w \notin \text{Im}(1-\varphi-\psi) \end{pmatrix}
\] | \( p - 1 \) |

Table 3. Affine forms of simple paramedial quasigroups of order \( p^2 \), up to isomorphism.

Firstly, we observe that \( a = 2^{-1}a^{-1} - a \) if and only if \( a = \pm 2^{-1} \) and for all \( a \in \mathbb{Z}_p \setminus \{0\} \), \(-a \neq 2^{-1}a^{-1} - a \). If \( a = \pm 2^{-1} \) (only one choice satisfies \( 0 < a < -a \)), then \( k \neq \pm a \) implies
\[ k \neq 2^{-1}a^{-1} - a, \] therefore there is only one possible constant \( c \) and the number of admissible triples \((\varphi, \psi, c)\) is \( p - 2 \), which is the number of possible choices of \( k \neq \pm a \). For \( a \neq \pm 2^{-1} \), there are \( \frac{p - 1}{2} - 1 \) values of \( a \) satisfying \( 0 < a < -a \). Then the number of possible constants \( c \) depends on the value of \( k \). If \( k \neq 2^{-1}a^{-1} - a \), there are \( p - 3 \) possible values of \( k \) and only one possible constant \( c \), hence the number of possible triples \((\varphi, \psi, c)\) is \( \left( \frac{p - 1}{2} - 1 \right) \cdot (p - 3) \). Otherwise, there are two possible choices of constant \( c \) and the number of triples \((\varphi, \psi, c)\) is \( \left( \frac{p - 1}{2} - 1 \right) \cdot 2 \).

References

[1] J. Baek, A. Deopurkar, K. Redfield, Points on conics modulo \( p \), https://cs.stanford.edu/people/jbaek/18.821.paper3.pdf, Accessed 26 April 2019.
[2] J. R. Cho, J. Ježek, T. Kepka, Paramedial groupoids. Czech. Math. J. 49/2 (1999), 277–290.
[3] J. R. Cho, J. Ježek, T. Kepka, Simple paramedial groupoids. Czech. Math. J. 49/2 (1999), 391–399.
[4] J. R. Cho, T. Kepka, Finite simple zeropotent paramedial groupoids. Czechoslovak Math. J. 52/1 (2002), 41–53.
[5] J. R. Cho, T. Kepka, Infinite simple zeropotent paramedial groupoids. Czech. Math. J. 53/4 (2003), 769–775.
[6] A. Drápal, Group isotopes and a holomorphic action, Resultat. Math. 54 (2009), no. 3–4, 253–272.
[7] C. J. Hillar, D. L. Rhea, Automorphisms of finite abelian groups, Amer. Math. Monthly 114 (2007), 917–923.
[8] X. Hou, Finite modules over \( \mathbb{Z}[t, t^{-1}] \), J. Knot Theory Ramifications 21 (2012), no. 8, 1250079, 28 pp.
[9] O. U. Kirnasovsky, Binary and n-ary isotopes of groups: fundamental algebraic properties and characterizations, PhD thesis, Kiev 2001 (Ukrainian).
[10] T. Kepka, P. Němec, T-quasigroups II, Acta Univ. Carolin. Math. Phys. 12 (1971), no. 2, 31–49.
[11] P. Němec, T. Kepka, T-quasigroups I, Acta Univ. Carolin. Math. Phys. 12 (1971), no. 1, 39–49.
[12] S. Northshield, Square roots of \( 2 \times 2 \) matrices, https://dspace.sunyconnect.suny.edu/bitstream/handle/1951/69937/fulltext.pdf, 2010. Accessed 25 February 2019.
[13] V. A. Shcherbacov, D. I. Pushkashu, On the structure of finite paramedial quasigroups. Comment. Math. Univ. Carolin. 51 (2010), no. 2, 357–370.
[14] J. D. H. Smith, An introduction to quasigroups and their representations, Chapman & Hall/CRC, 2007.
[15] D. Stanovský, Linear representation of Abel-Grassmann groups, Carpathian J. Math. 33/2 (2017), 257–263
[16] D. Stanovský, Medial quasigroups of prime square order, Comment. Math. Univ. Carolinae. 57/4 (2016), 585–590.
[17] D. Stanovský, P. Vojtěchovský, Central and medial quasigroups of small order, Buletinul Academiei de Științe a Republicii Moldova, Matematica, 80/1 (2016), 24–40.

Department of Algebra, Faculty of Mathematics and Physics, Charles University, Prague, Czech Republic

E-mail address: zaneta.semanisinova@gmail.com