Paramedial quasigroups of prime and prime square order

Žaneta Semanišinová

Institute of Algebra
TU Dresden

Fall School of Algebra, 4.11.2021

Definition of a quasigroup

Definition (quasigroup)

Let Q be a set equipped with a binary operation $*$. $(Q, *)$ is a quasigroup, if for all $a, b \in Q$, there exist unique $x, y \in Q$ such that

$$a * x = b \text{ and } y * a = b$$

$(Q, *)$ is a quasigroup iff the multiplication table of $*$ is a latin square (possibly infinite).

$-$	0	1	2
0	0	2	1
1	1	0	2
2	2	1	0

Table: Multiplication table of $(\mathbb{Z}_3, -)$

Paramedial quasigroups

Definition (paramedial quasigroup)

A quasigroup $(Q, *)$ is called paramedial, if for all $x, y, u, v \in Q$ the following holds

$$(x * y) * (u * v) = (v * y) * (u * x).$$

Example: If $(G, +, -, 0)$ is an abelian group, then $(G, -)$ is a paramedial quasigroup.

$$(x - y) - (u - v) = x - y - u + v$$
$$(v - y) - (u - x) = v - y - u + x$$

Motivation

- enumeration of algebraic structures up to isomorphism (groups, quasigroups, medial quasigroups)
- in the case of quasigroups it is natural to focus on a specific class
- inspired by the results of the enumeration of medial quasigroups (Kirnasovsky, Stanovský)

	groups									
1..10	1	1	1	2	1	2	1	5	2	2
11..20	1	5	1	2	1	14	1	5	1	5
21..30	2	2	1	15	2	2	5	4	1	4
31..40	1	51	1	2	1	14	1	2	2	14
41..50	1	6	1	4	2	2	1	52	2	5
51..60	1	5	1	15	2	13	2	2	1	13
61..70	1	2	4	267	1	4	1	5	1	4
71..80	1	50	1	2	3	4	1	6	1	52
81..90	15	2	1	15	1	2	1	12	1	10
91..100	1	4	2	2	1	231	1	5	2	16

	quasigroups
1	1
2	1
3	5
4	35
5	1411
6	1130531
7	12198455835
8	2697818331680661
9	15224734061438247321497
10	2750892211809150446995735533513

Main result

Theorem

Let p be an odd prime. Then the number of paramedial quasigroups (up to isomorphism) of:

- *order p is*
$$2p - 1.$$
- *order p^2 is*
$$6p^2 - p - 1.$$

The number of paramedial quasigroups of order 2 *is* 1 *and of order* 4 *is* 11.

Main result

Theorem

Let p be an odd prime. Then the number of paramedial quasigroups (up to isomorphism) of:

- *order p is*
$$2p - 1.$$
- *order p^2 is*
$$6p^2 - p - 1.$$

The number of paramedial quasigroups of order 2 is 1 and of order 4 is 11.

n	2	3	4	5	6	7	8	9	10	11	12	13	14
$\mathrm{pq}(n)$	1	5	11	9	5	13	?	50	9	21	55	25	13

Affine representation

Definition (affine quasigroup)

Let $(G, +, -, 0)$ be an abelian group and φ, $\psi \in \text{Aut}(G)$, $c \in G$. Define $*$ on G by

$$x * y = \varphi(x) + \psi(y) + c.$$

The resulting quasigroup $(G, *)$ is said to be affine over $(G, +)$ and denoted by $\mathrm{Aff}(G, +, \varphi, \psi, c)$.

Example: $G = \mathbb{Z}_5$, $\varphi(x) = 2x$, $\psi(x) = 3x$, $c = 1$
The quasigroup operation $*$ in $\mathrm{Aff}(\mathbb{Z}_5, +, \varphi, \psi, 1)$ is defined by

$$x * y = 2x + 3y + 1.$$

Affine representation

Theorem (T. Kepka, P. Němec, 1971)

A quasigroup $(G, *)$ is paramedial iff it is affine over an abelian group $(G, +)$ and

$$\varphi^2 = \psi^2.$$

Example (continued): $G = \mathbb{Z}_5$, $\varphi(x) = 2x$, $\psi = 3x$, $c = 1$
$\varphi^2(x) = \psi^2(x)$ since $\psi = -\varphi$, and the paramedial identity is satisfied:

$$(2x + 3y + 1) * (2u + 3v + 1) = (4x + y + 2) + (u + 4v + 3) + 1,$$
$$(2v + 3y + 1) * (2u + 3x + 1) = (4v + y + 2) + (u + 4x + 3) + 1,$$

which are both equal to $4x + y + u + 4v + 1$.

Properties of counting functions

- $\mathrm{pq}(G)$ – the number of paramedial quasigroups over G
- $\mathrm{pq}(n)$ – the number of paramedial quasigroups of order n

The following holds:

$$\mathrm{pq}(n) = \sum_{|G|=n} \mathrm{pq}(G),$$

Properties of counting functions

- $\mathrm{pq}(G)$ – the number of paramedial quasigroups over G
- $\mathrm{pq}(n)$ – the number of paramedial quasigroups of order n

The following holds:

$$\mathrm{pq}(n) = \sum_{|G|=n} \mathrm{pq}(G),$$

If H a K are finite abelian groups such that $\gcd(|H|, |K|) = 1$, then

$$\mathrm{pq}(H \times K) = \mathrm{pq}(H) \cdot \mathrm{pq}(K).$$

In particular, for $k, l \in \mathcal{N}$ satisfying $\gcd(k, l) = 1$ holds

$$\mathrm{pq}(k \cdot l) = \mathrm{pq}(k) \cdot \mathrm{pq}(l).$$

Enumeration algorithm

Algorithm (Drápal, 2009):
Let $(G, +, -, 0)$ be an abelian group.

1. Choose a set X of orbit representatives of the conjugation action of $\mathrm{Aut}(G)$ on itself.
2. For every $\varphi \in X$:
   - Determine the set $S_\varphi = \{\psi : \psi^2 = \varphi^2\}$.
   - Choose a set $Y_\varphi \subseteq S_\varphi$ of orbit representatives of the conjugation action of $C_{\mathrm{Aut}(G)}(\varphi)$ on S_φ.
   - For every $\psi \in Y_\varphi$ choose a set $G_{\varphi,\psi}$ of orbit representatives of the natural action of $C_{\mathrm{Aut}(G)}(\varphi) \cap C_{\mathrm{Aut}(G)}(\psi)$ on $G/\mathrm{Im}(1 - \varphi - \psi)$.
3. The representatives of the isomorphisms classes of paramedial quasigroups over G are

$$\mathrm{Aff}(G, +, \varphi, \psi, c) : \varphi \in X, \psi \in Y_\varphi, c \in G_{\varphi,\psi}.$$

Enumeration over cyclic groups

Case $G = \mathbb{Z}_{p^k}$:

- $\mathrm{Aut}(\mathbb{Z}_{p^k}) \simeq \mathbb{Z}_{p^k}^*$, therefore the group is commutative.
- Hence, the conjugation action and centralizers are trivial.
- The first part of calculation reduces to solving the equation $\varphi^2 = \psi^2$ in $\mathbb{Z}_{p^k}^*$ for a fixed φ.
- Then we determine $\mathrm{Im}(1 - \varphi - \psi)$ for the pairs (φ, ψ).
- $\mathbb{Z}_{p^k}^*$ acts on $\mathbb{Z}_{p^k}/\mathrm{Im}(1 - \varphi - \psi)$ by multiplication, so we can choose orbit representatives as 0 and the powers of p.

Enumeration over cyclic groups

Case $G = \mathbb{Z}_{p^k}$**:**

- $\mathrm{Aut}(\mathbb{Z}_{p^k}) \simeq \mathbb{Z}^*_{p^k}$, therefore the group is commutative.
- Hence, the conjugation action and centralizers are trivial.
- The first part of calculation reduces to solving the equation $\varphi^2 = \psi^2$ in $\mathbb{Z}^*_{p^k}$ for a fixed φ.
- Then we determine $\mathrm{Im}(1 - \varphi - \psi)$ for the pairs (φ, ψ).
- $\mathbb{Z}^*_{p^k}$ acts on $\mathbb{Z}_{p^k}/\mathrm{Im}(1 - \varphi - \psi)$ by multiplication, so we can choose orbit representatives as 0 and the powers of p.

Result:

$$\mathrm{pq}(\mathbb{Z}_{p^k}) = 2p^k - p^{k-1} + \sum_{i=0}^{k-2} p^i,$$

in particular, $\mathrm{pq}(p) = \mathrm{pq}(\mathbb{Z}_p) = 2p - 1$.

Enumeration over the group $\mathbb{Z}_p^2$

Case $G = \mathbb{Z}_p^2$**:**

- $\mathrm{Aut}(\mathbb{Z}_p^2) \simeq GL(2,p)$
- We choose the representatives of the conjugacy classes in $GL(2,p)$.

φ	$C(\varphi)$
$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, $a \neq 0$	$GL(2,p)$
$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, $0 < a < b$	$\left\{ \begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix} : u, v \neq 0 \right\}$
$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$, $a \neq 0$	$\left\{ \begin{pmatrix} u & v \\ 0 & u \end{pmatrix} : u \neq 0 \right\}$
$\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}$, $x^2 - bx - a$ irreducible	$\left\{ \begin{pmatrix} u & v \\ av & u + bv \end{pmatrix} : u \neq 0 \vee v \neq 0 \right\}$

Enumeration over the group $\mathbb{Z}_p^2$

- For a fixed φ we determine the set $S_\varphi = \{\psi : \psi^2 = \varphi^2\}$, i.e., we find the square roots of the matrix φ^2.
  - Two methods for finding square roots of 2×2 matrices:
    - a method based on Cayley-Hamilton theorem (a matrix is a root of its characteristic polynomial) for $\varphi^2 \neq cI$, $c \in \mathbb{Z}_p$
    - a straightforward calculation for the remaining matrices
- Then (if possible) we choose orbit representatives ψ of the conjugation action of $C(\varphi)$ on S_φ.
- We discuss the dimension of $\mathrm{Im}(1 - \varphi - \psi)$.

Affine forms of paramedial quasigroups over $\mathbb{Z}_p^2$

φ	ψ	c	number
$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ $a \neq 0$	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$, if $a \neq 2^{-1}$	$p-2$
		$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$, if $a = 2^{-1}$	2
	$\begin{pmatrix} -a & 0 \\ 0 & -a \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$p-1$
	$\begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$, if $a \neq 2^{-1}$	$p-2$
		$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$, if $a = 2^{-1}$	2

φ	ψ	c	number
$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ $0 < a < b$	$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$, if $a, b \neq 2^{-1}$	$\binom{p-2}{2}$
		$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$, if $a = 2^{-1} \vee b = 2^{-1}$	$2(p-2)$
	$\begin{pmatrix} -a & 0 \\ 0 & -b \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$\binom{p-1}{2}$
	$\begin{pmatrix} \pm a & 0 \\ 0 & \mp b \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$, if $a \neq 2^{-1}$ or $b \neq 2^{-1}$, resp. (depends on the signs)	$2\binom{p-2}{2} + p - 2$
		$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$, if $a = 2^{-1}$ or $b = 2^{-1}$, resp. (depends on the signs)	$2(p-2)$

φ	ψ	c	number
$\begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}$ $0 < a < -a$	$\begin{pmatrix} a & 0 \\ 1 & -a \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$, if $a \neq \pm 2^{-1}$	$\frac{p-3}{2}$
		$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$, if $a = 2^{-1}$ or $a = -2^{-1}$, resp. (must satisfy $0 < a < -a$)	2
	$\begin{pmatrix} -a & 0 \\ 1 & a \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$\frac{p-1}{2}$
	$\begin{pmatrix} k & 1 \\ a^2 - k^2 & -k \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$, if $k \neq 2^{-1}a^{-1} - a$	$\frac{(p-1)^2}{2}$
		$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, if $k = 2^{-1}a^{-1} - a$	$p-1$

$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$ $a \neq 0$	$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$, if $a \neq 2^{-1}$	$p - 2$
		$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, if $a = 2^{-1}$	2
	$\begin{pmatrix} -a & -1 \\ 0 & -a \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$p - 1$
$\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}$ $x^2 - bx - a$ irreducible	$\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$\frac{p^2 - p}{2}$
	$\begin{pmatrix} 0 & -1 \\ -a & -b \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$\frac{p^2 - p}{2}$
$\begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}$ $x^2 - a$ irreducible	?	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$\frac{(p-1)(p-3)}{2}$
	?	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$, $\mathbf{w}$, $\mathbf{w} \notin \mathrm{Im}(1 - \varphi - \psi)$	$p - 1$

Thank you for your attention