FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

Žaneta Semanišinová

Paramedial quasigroups of prime and prime square order

LOOPS 2019

9 July 2019

Definition of paramedial quasigroup

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.

Motivation

Theorem (Kirnasovsky, 1995; Stanovský, 2016)

Let p be a prime. Then the number of medial quasigroups (up to isomorphism) of:

- order p is
$$p^2 - p - 1.$$
- order p^2 is
$$2p^4 - p^3 - p^2 - 3p - 1.$$

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
$$\frac{11}{2}p^2 + \frac{3}{2}p - 4.$$

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

Affine representation

Definition (affine quasigroup)

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

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

The resulting quasigroup $(G, *)$ is said to be affine over $(G, +)$.

Theorem (T. Kepka, P. Němec, 1971)

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

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

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 $k, l \in \mathbb{N}$ satisfying $\gcd(k, l) = 1$ holds

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

Enumeration algorithm

Theorem (A. Drápal, 2009)

Let $(G, +, -, 0)$ be an abelian group. The isomorphism classes of paramedial quasigroups 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 complete set of orbit representatives of the conjugation action of $\mathrm{Aut}(G)$ on itself,
- Y_φ is a complete set of orbit representatives of the conjugation action of $C_{\mathrm{Aut}(G)}(\varphi)$ on $S_\varphi = \{\psi \in \mathrm{Aut}(G) : \psi^2 = \varphi^2\}$,
- $G_{\varphi,\psi}$ is a complete set of orbit representatives of the natural action of $C_{\mathrm{Aut}(G)}(\varphi) \cap C_{\mathrm{Aut}(G)}(\psi)$ on $G/\mathrm{Im}(1 - \varphi - \psi)$.

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, so the first part of calculation reduces to solving the equation $\varphi^2 = \psi^2$ in $\mathbb{Z}^*_{p^k}$ for fixed φ.
- We need to analyze $\mathrm{Im}(1 - \varphi - \psi)$ depending on 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: $\mathrm{pq}(\mathbb{Z}_{p^k}) = 2p^k - p^{k-1} + \sum_{i=0}^{k-2} p^i$

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 element φ we determine the set S_φ of all elements $\psi \in GL(2,p)$ satisfying that $\psi^2 = \varphi^2$, i.e., we find the square roots of the matrix φ^2.
  - We use two methods for finding square roots of 2×2 matrices:
    - a method based on Cayley-Hamilton theorem for the matrices that are not a multiple of identity matrix
    - a straightforward calculation for the remaining matrices
- Then (if possible) we choose orbit representatives ψ of the conjugation action of the centralizer $C(\varphi)$ on S_φ.
- We discuss the dimension of $\mathrm{Im}(1 - \varphi - \psi)$.

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)	$\binom{p-2}{2} + p - 2$
		$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$, 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

Žaneta Semanišinová

e-mail: zaneta.semanisinova@gmail.com