Medial quasigroups of prime square order

David Stanovský

Abstract. We prove that, for any prime p, there are precisely $2p^4-p^3-p^2-3p-1$ medial quasigroups of order p^2, up to isomorphism.

Keywords: medial quasigroup; quasigroup affine over abelian group; classification of quasigroups; enumeration of quasigroups

Classification: 20N05, 05A15

1. Introduction

Medial quasigroups, i.e., quasigroups satisfying the medial law

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

are one of the classical subjects of quasigroup theory. Yet there are very few enumeration results in literature. The aim of the present paper is to extend earlier results of [4], [7], [9], by enumerating medial quasigroups of prime square order.

The fundamental tool to study medial quasigroups (and many other classes of quasigroups), is affine representation. Given an abelian group $G=(G,+)$, automorphisms φ,ψ of G, and an element $c\in G$, define a new operation $*$ on the set G by

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

The resulting quasigroup $(G,*)$ is said to be *affine over the group* G, and it will be denoted by $\mathcal{Q}(G,+,\varphi,\psi,c)$; the quintuple $(G,+,\varphi,\psi,c)$ is called an *affine form* of $(G,*)$. The fundamental Toyoda-Bruck theorem [8, Theorem 3.1] states that a quasigroup is medial if and only if there is an abelian group $G=(G,+)$, a pair of *commuting* automorphisms φ,ψ of G, and $c\in G$ such that $Q=\mathcal{Q}(G,+,\varphi,\psi,c)$. We refer to [8] for a detailed account on various kinds of affine representations of quasigroups.

Let $mq(n)$ denote the number of medial quasigroups of order n, and $mq(G)$ the number of medial quasigroups that admit an affine form over a group G, up to isomorphism. It follows from the classification of finite abelian groups that $mq(G\times H)=mq(G)\cdot mq(H)$ whenever G,H are abelian groups of coprime order.

DOI 10.14712/1213-7243.2015.181

Research partly supported by the GAČR grant 13-01832S.

Therefore, the function $mq(n)$ is multiplicative. In particular, if $n = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}$ is a prime factorization of n, then $mq(n) = mq(p_1^{k_1}) \cdot \ldots \cdot mq(p_m^{k_m})$. Since isotopic groups are isomorphic, a medial quasigroup cannot admit affine forms over two non-isomorphic groups, and thus $mq(n) = \sum mq(G)$ where the sum runs over all isomorphism representatives of abelian groups of order n. For details, we refer to [9].

Quasigroups affine over a cyclic group were enumerated in [4], [9], obtaining an explicit formula

$$mq(\mathbb{Z}_{p^k}) = p^{2k} + p^{2k-2} - p^{k-1} - \sum_{i=k-1}^{2k-1} p^i$$

for every prime p. In particular, we have

$$\begin{aligned} mq(p) = mq(\mathbb{Z}_p) &= p^2 - p - 1 \\ mq(\mathbb{Z}_{p^2}) &= p^4 - p^3 - 2p. \end{aligned}$$

The main result of the present paper is:

Theorem 1.1. *$mq(\mathbb{Z}_p^2) = p^4 - p^2 - p - 1$ for every prime p.*

Corollary 1.2. *$mq(p^2) = mq(\mathbb{Z}_{p^2}) + mq(\mathbb{Z}_p^2) = 2p^4 - p^3 - p^2 - 3p - 1$ for every prime p.*

The proof of Theorem 1.1 occupies the whole Section 2. The affine forms of the quasigroups are explicitly expressed in Table 2. Our formula agrees with the computer calculations of [9] which presents enumeration of all quasigroups affine over an abelian group of order < 64 (of order < 128 with a few exceptions).

An important special case, the *idempotent* medial quasigroups (or *latin affine quandles*, in the quandle terminology [3]), has been studied earlier extensively. The enumeration problem is significantly simpler, since the parameters in the affine form can be taken $c = 0$ and $\psi = id - \varphi$. Therefore, the enumeration of idempotent medial quasigroups up to isomorphism reduces to the enumeration of fixpoint free automorphisms of abelian groups up to conjugacy (cf. Theorem 2.1). The strongest results were obtained by Hou [2], providing explicit formulas for orders p^k with $k \leq 4$. More information about the idempotent case can be found also in [6].

2. Proof of Theorem 1.1

We will follow the enumeration procedure described in detail in [9]. It is based on the following theorem, originally proposed by Drápal [1].

Theorem 2.1 ([1, Theorem 3.2], [9, Theorem 2.5])**.** *Let G be an abelian group. The isomorphism classes of medial 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* $\mathrm{Aut}(G)$*;*
- *Y_φ is a set of conjugacy class representatives of the centralizer subgroup $C_{\mathrm{Aut}(G)}(\varphi)$, for every $\varphi \in X$ (here we consider conjugation inside the group $C_{\mathrm{Aut}(G)}(\varphi)$, not conjugation by all elements of* $\mathrm{Aut}(G)$*);*
- *$G_{\varphi,\psi}$ is a set of orbit representatives of the natural action of $C_{\mathrm{Aut}(G)}(\varphi) \cap C_{\mathrm{Aut}(G)}(\psi)$ on $G/\mathrm{Im}(1-\varphi-\psi)$.*

Indeed, a triple (φ, ψ, c) corresponds to the quasigroup $\mathcal{Q}(G, \varphi, \psi, c)$, hence, an explicit construction of the sets $X, Y_\varphi, G_{\varphi,\psi}$ provides an explicit construction of the quasigroups.

In the rest of the section, we apply Theorem 2.1 on the group $G = \mathbb{Z}_p^2$. We will identify automorphisms with their matrices, considering $\mathrm{Aut}(G) = GL(2,p)$. Most of the proof is a bit sketchy and many sentences could have started with the "it is easy to check that" statement; yet we think that adding more details would not improve readability of the proof.

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	$\left\{ \begin{pmatrix} u & v \\ av & u+bv \end{pmatrix} : u \neq 0 \text{ or } v \neq 0 \right\}$.

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

Proof of Theorem 1.1: Let $G = \mathbb{Z}_p^2$. The set X of conjugacy class representatives in $\mathrm{Aut}(G) = GL(2,p)$ 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 $\mathbb{F}_p$, and the non-diagonalizable matrices with eigenvalues in the quadratic extension, respectively. The last case is represented by matrices $\left(\begin{smallmatrix} 0 & 1 \\ a & b \end{smallmatrix}\right)$ such that the polynomial $x^2 - bx - a$ is irreducible over $\mathbb{F}_p$.

The centralizer subgroups are also displayed in Table 1 (here and later on, we will omit the index in the centralizer notation). In the first case, we can take $Y_\varphi = X$ and we have $C(\varphi) \cap C(\psi) = C(\psi)$ for every $\psi \in Y_\varphi$. In the remaining three cases, the key observation is that the centralizer subgroups are commutative, hence we can take $Y_\varphi = C(\varphi)$, and we have $C(\varphi) \cap C(\psi) = C(\varphi)$ for every $\psi \in Y_\varphi$.

The size of $G_{\varphi,\psi}$ will be determined by the following procedure: if $1-\varphi-\psi$ is a regular matrix, then $|G/\mathrm{Im}(1-\varphi-\psi)|=1$, and thus also $|G_{\varphi,\psi}|=1$. If the rank of the matrix $1-\varphi-\psi$ is one, then $G/\mathrm{Im}(1-\varphi-\psi)\simeq\mathbb{Z}_p$, and since all of the centralizer subgroups contain all scalar matrices $\left(\begin{smallmatrix}u&0\\0&u\end{smallmatrix}\right)$, we can always take $G_{\varphi,\psi}=\{\mathbf{0},\mathbf{w}\}$ where $\mathbf{w}$ is any non-zero vector. If the rank of the matrix $1-\varphi-\psi$ is zero, then $G/\mathrm{Im}(1-\varphi-\psi)\simeq G$, and the situation depends on $C(\varphi)\cap C(\psi)$, to be discussed below in each particular case.

The results are summarized in Table 2. Below we give comments on how the table is calculated.

φ	ψ	c	number
$\begin{pmatrix}a&0\\0&a\end{pmatrix}$ $a\neq 0$	$\begin{pmatrix}u&0\\0&u\end{pmatrix}$ $u\neq 0$	$\begin{pmatrix}0\\0\end{pmatrix}$ if $u\neq 1-a$	p^2-3p+3
		$\begin{pmatrix}0\\0\end{pmatrix},\begin{pmatrix}1\\0\end{pmatrix}$ if $u=1-a$	$2(p-2)$
	$\begin{pmatrix}u&0\\0&v\end{pmatrix}$ $0<u<v$	$\begin{pmatrix}0\\0\end{pmatrix}$ if $u,v\neq 1-a$	$\frac{1}{2}(p-2)(p^2-4p+5)$
		$\begin{pmatrix}0\\0\end{pmatrix},\begin{pmatrix}1\\0\end{pmatrix}$ if $u=1-a$ or $v=1-a$	$2(p-2)^2$
	$\begin{pmatrix}u&1\\0&u\end{pmatrix}$ $u\neq 0$	$\begin{pmatrix}0\\0\end{pmatrix}$ if $u\neq 1-a$	p^2-3p+3
		$\begin{pmatrix}0\\0\end{pmatrix},\begin{pmatrix}1\\0\end{pmatrix}$ if $u=1-a$	$2(p-2)$
	$\begin{pmatrix}0&1\\u&v\end{pmatrix}$ x^2-vx-u irr.	$\begin{pmatrix}0\\0\end{pmatrix}$	$\frac{1}{2}p(p-1)^2$
$\begin{pmatrix}a&0\\0&b\end{pmatrix}$ $0<a<b$	$\begin{pmatrix}u&0\\0&v\end{pmatrix}$ $u,v\neq 0$	$\begin{pmatrix}0\\0\end{pmatrix}$ if $u\neq 1-a,\ v\neq 1-b$	$\frac{1}{2}(p-2)^2(p^2-3p+4)$
		$\begin{pmatrix}0\\0\end{pmatrix},\begin{pmatrix}1\\0\end{pmatrix}$ if $\begin{cases}u=1-a,\ v\neq 1-b\\ u\neq 1-a,\ v=1-b\end{cases}$	$2(p-2)(p^2-4p+5)$
		$\begin{pmatrix}0\\0\end{pmatrix},\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix},\begin{pmatrix}1\\1\end{pmatrix}$ if $(u,v)=(1-a,1-b)$	$2(p-2)(p-3)$
$\begin{pmatrix}a&1\\0&a\end{pmatrix}$ $a\neq 0$	$\begin{pmatrix}u&v\\0&u\end{pmatrix}$ $u\neq 0$	$\begin{pmatrix}0\\0\end{pmatrix}$ if $u\neq 1-a$	$p(p^2-3p+3)$
		$\begin{pmatrix}0\\0\end{pmatrix},\begin{pmatrix}1\\0\end{pmatrix}$ if $u=1-a,\ v\neq -1$	$2(p-1)(p-2)$
		$\begin{pmatrix}0\\0\end{pmatrix},\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix}$ if $u=1-a,\ v=-1$	$3(p-2)$
$\begin{pmatrix}0&1\\a&b\end{pmatrix}$ x^2-bx-a irr.	$\begin{pmatrix}u&v\\av&u+bv\end{pmatrix}$ $u\neq 0$ or $v\neq 0$	$\begin{pmatrix}0\\0\end{pmatrix}$ if $(u,v)\neq(1,-1)$	$\frac{1}{2}(p^2-p)(p^2-2)$
		$\begin{pmatrix}0\\0\end{pmatrix},\begin{pmatrix}1\\0\end{pmatrix}$ if $u=1,\ v=-1$	p^2-p

Table 2. Affine forms of medial quasigroups over the group $\mathbb{Z}_p^2$, up to isomorphism.

Case $\varphi=\left(\begin{smallmatrix}a&0\\0&a\end{smallmatrix}\right)$. Take $Y_\varphi=X$.

Subcase $\psi=\left(\begin{smallmatrix}u&0\\0&u\end{smallmatrix}\right)$. The matrix $1-\varphi-\psi$ is singular iff $u=1-a$. There are $p-2$ such pairs (φ,ψ), and since $C(\varphi)\cap C(\psi)=GL(2,p)$, we can choose $G_{\varphi,\psi}=\{\mathbf{0},\mathbf{w}\}$ with any $\mathbf{w}\neq 0$. In the remaining $(p-1)^2-(p-2)=p^2-3p+3$ cases, the matrix is regular and $|G_{\varphi,\psi}|=1$.

Subcase $\psi=\left(\begin{smallmatrix}u&0\\0&v\end{smallmatrix}\right)$. The matrix $1-\varphi-\psi$ is singular iff $u=1-a$ or $v=1-a$ (we cannot have both at the same time, since $u\neq v$). There are $(p-2)^2$ such pairs (φ,ψ), and since the rank of $1-\varphi-\psi$ is one, we have $|G_{\varphi,\psi}|=2$. In the remaining $(p-1)\cdot\binom{p-1}{2}-(p-2)^2=\frac{1}{2}(p-2)(p^2-4p+5)$ cases, the matrix is regular and $|G_{\varphi,\psi}|=1$.

Subcase $\psi=\left(\begin{smallmatrix} u & 1\\ 0 & u\end{smallmatrix}\right)$. The matrix $1-\varphi-\psi$ is singular iff $u=1-a$. There are $p-2$ such pairs (φ,ψ), and since the rank of $1-\varphi-\psi$ is one, we have $|G_{\varphi,\psi}|=2$. In the remaining $(p-1)^2-(p-2)=p^2-3p+3$ cases, the matrix is regular and $|G_{\varphi,\psi}|=1$.

Subcase $\psi=\left(\begin{smallmatrix} 0 & 1\\ u & v\end{smallmatrix}\right)$. The matrix $1-\varphi-\psi$ is always regular. Since there are precisely $\frac{1}{2}(p^2-p)$ irreducible polynomials of degree 2 over $\mathbb{F}_p$, this case contributes $\frac{1}{2}p(p-1)^2$ triples (φ,ψ,c).

Case $\varphi=\left(\begin{smallmatrix} a & 0\\ 0 & b\end{smallmatrix}\right)$. Take $Y_\varphi=C(\varphi)$, the subgroup of diagonal matrices. The total number of pairs (φ,ψ) is $\binom{p-1}{2}(p-1)^2$. For $\psi=\left(\begin{smallmatrix} u & 0\\ 0 & v\end{smallmatrix}\right)$, the rank of $1-\varphi-\psi$ is

- zero iff $u=1-a$ and $v=1-b$; there are $\binom{p-2}{2}$ such pairs (φ,ψ), each with $|G_{\varphi,\psi}|=4$, since there are four orbits of the action of $C(\varphi)$ on $\mathbb{Z}_p^2$;
- one iff $u=1-a$ or $v\neq 1-b$, or $u\neq 1-a$ and $v=1-b$; for $a=1$, there are $p-2$ choices of b, $p-1$ choices of u and one choice of v; for $a\neq 1$, there are $\binom{p-2}{2}$ choices of φ, and for each of them $2p-4$ choices of ψ; in total, we have $(p-2)(p-1)+\binom{p-2}{2}(2p-4)=(p-2)(p^2-4p+5)$ such pairs (φ,ψ), each with $|G_{\varphi,\psi}|=2$;
- two iff $u\neq 1-a$ and $v\neq 1-b$; these are the remaining pairs (φ,ψ), hence, there is $\binom{p-1}{2}(p-1)^2-\binom{p-2}{2}-(p-2)(p^2-4p+5)=\frac{1}{2}(p-2)^2(p^2-3p+4)$ of them, each with $|G_{\varphi,\psi}|=1$.

Case $\varphi=\left(\begin{smallmatrix} a & 1\\ 0 & a\end{smallmatrix}\right)$. Take $Y_\varphi=C(\varphi)=\{\left(\begin{smallmatrix} u & v\\ 0 & u\end{smallmatrix}\right):u\neq 0\}$. The total number of pairs (φ,ψ) is $p(p-1)^2$. For $\psi=\left(\begin{smallmatrix} u & v\\ 0 & u\end{smallmatrix}\right)$, the rank of $1-\varphi-\psi$ is

- zero iff $u=1-a$ and $v=-1$; there are $p-2$ such pairs (φ,ψ), each with $|G_{\varphi,\psi}|=3$, since there are three orbits of the action of $C(\varphi)$ on $\mathbb{Z}_p^2$;
- one iff $u=1-a$ or $v\neq -1$; there are $(p-2)(p-1)$ such pairs (φ,ψ), each with $|G_{\varphi,\psi}|=2$;
- two iff $u\neq 1-a$; these are the remaining pairs (φ,ψ), hence, there is $p(p-1)^2-(p-2)-(p-2)(p-1)=p(p^2-3p+3)$ of them, each with $|G_{\varphi,\psi}|=1$.

Case $\varphi=\left(\begin{smallmatrix} 0 & 1\\ a & b\end{smallmatrix}\right)$. Take $Y_\varphi=C(\varphi)$. For $\psi=\left(\begin{smallmatrix} u & v\\ av & u+bv\end{smallmatrix}\right)\in C(\varphi)$, the determinant of the matrix $1-\varphi-\psi$ is $(1-u)^2-b(1-u)(1+v)-a(1+v)^2$. Assume the determinant is 0. Then either $1+v=0$, and thus also $1-u=0$, or we can divide by $(1+v)^2$ and obtain the equation $(\frac{1-u}{1-v})^2-b\frac{1-u}{1+v}-a=0$, which has no solution, because the polynomial x^2-bx-a is irreducible. Therefore, the matrix $1-\varphi-\psi$ is singular if and only $u=1$ and $v=-1$. Since $C(\varphi)$ acts transitively on $\mathbb{Z}_p^2-\{\mathbf{0}\}$, we have $|G_{\varphi,\psi}|=2$. There are $\frac{1}{2}(p^2-p)$ irreducible polynomials of degree 2, thus the singular case contributes p^2-p triples. The regular case contributes $\frac{1}{2}(p^2-p)(p^2-2)$ triples.

Summing up all the contributions (see the last column of Table 2), we obtain that the total number is $p^4 - p^2 - p - 1$. □

3. Concluding remarks

In [9, Problem 3.4], we asked to calculate $mq(\mathbb{Z}_p^k)$ for any p, k. In theory, using Macdonald's classification of conjugacy classes in general linear groups [5], one could continue in the fashion of Section 2 to higher dimensions. But the complexity of such calculations would grow rapidly. As an alternative, we propose the following idea.

Conjecture 3.1. *Let k be any natural number.*

(1) *There is an integer polynomial f_k of degree $2k$ such that $mq(\mathbb{Z}_p^k) = f_k(p)$ for every prime p.*
(2) *There is an integer polynomial g_k of degree $2k$ such that $mq(p^k) = g_k(p)$ for every prime p.*

If the conjecture was true, one could interpolate the polynomials from the values of $mq(\mathbb{Z}_p^k)$ and $mq(p^k)$ for the first $2k + 1$ primes.

References

[1] Drápal A., *Group isotopes and a holomorphic action*, Result. Math. **54** (2009), no. 3–4, 253–272.

[2] Hou X., *Finite modules over $\mathbb{Z}[t, t^{-1}]$*, J. Knot Theory Ramifications **21** (2012), no. 8, 1250079, 28 pp.

[3] Hulpke A., Stanovský D., Vojtěchovský P., *Connected quandles and transitive groups*, J. Pure Appl. Algebra **220** (2016), no. 2, 735–758.

[4] Kirnasovsky O.U., *Linear isotopes of small order groups*, Quasigroups Related Systems **2** (1995), no. 1, 51–82.

[5] Macdonald I.G., *Numbers of conjugacy classes in some finite classical groups*, Bull. Austral. Math. Soc. **23** (1981), no. 1, 23–48.

[6] Sim H.-S., Song H.-J., *Revisit to connected Alexander quandles of small orders via fixed point free automorphisms of finite Abelian groups*, East Asian Math. J. **30** (2014), no. 3, 293–302.

[7] Sokhatsky F., Syvakivskij P., *On linear isotopes of cyclic groups*, Quasigroups Related Systems **1** (1994), no. 1, 66–76.

[8] Stanovský D., *A guide to self-distributive quasigroups, or latin quandles*, Quasigroups Related Systems **23** (2015), no. 1, 91–128.

[9] Stanovský D., Vojtěchovský P., *Central and medial quasigroups of small order*, Bul. Acad. Ştiinte Repub. Moldova Mat. **80** (2016), no. 1, 24–40.

Charles University, Faculty of Mathematics and Physics, Department of Algebra, Sokolovská 83, 186 75 Prague 8, Czech Republic

E-mail: stanovsk@karlin.mff.cuni.cz

(*Received* March 14, 2016, *revised* March 29, 2016)