# SOME REMARKS ON TWO-TRANSITIVE PERMUTATION GROUPS AS MULTIPLICATION GROUPS OF QUASIGROUPS

GERHARD HISS AND FRANK LÜBECK

Abstract. We explore the question of which finite two-transitive permutation groups are multiplication groups of quasigroups.

## 1. Introduction

A quasigroup is a finite set $Q$ with a binary operation such that the equation $x \cdot y = z$ in $Q$ has a unique solution, whenever two of $x, y, z$ are given. The quasigroup $Q$ is called a loop, if it has a neutral element, and commutative if $x \cdot y = y \cdot x$ for all $x, y \in Q$. The multiplication table $T$ of $Q = \{q_1, \ldots, q_n\}$ is the $(n \times n)$-matrix whose rows and columns are labelled by $q_1, \ldots, q_n$ (in this order), and the entry in row $q_i$ and column $q_j$ equals the product $q_i \cdot q_j$. The axioms of a quasigroup simply say that $T$ is a Latin square.

Row $i$ of $T$ contains the images of $q_1, \ldots, q_n$ under the left multiplication $L(q_i)$: $q_j^{L(q_i)} = q_i \cdot q_j$. Similarly, column $j$ of $T$ contains the images of $q_1, \ldots, q_n$ under the right multiplication $R(q_j)$: $q_i^{R(q_j)} = q_i \cdot q_j$. The multiplication group $M(Q)$ of $Q$ is, by definition, the permutation group on $Q$ generated by $L(q_i), R(q_i)$, $1 \leq i \leq n$. It is clearly transitive on $Q$.

It has been shown by Smith (see [16, Theorem 523]) that the multiplication group of a quasigroup is multiplicity free, i.e. the permutation character of $M(Q)$ corresponding to its transitive action on $Q$ is multiplicity free. Equivalently, the centraliser algebra of the permutation representation is commutative.

It is thus a natural question to ask which multiplicity free transitive permutation groups are multiplication groups of quasigroups. The diploma thesis of Sebastian Köhler [13] answers this question for all permutation groups up to degree 10. In this survey we restrict this question to the two-transitive permutation groups.

1991 *Mathematics Subject Classification.* 20N05, 20B20, 20B40.

*Key words and phrases.* Quasigroups, multiplication groups, two-transitive groups.

We first collect some basic facts and reductions which are useful to decide if a given permutation group is the multiplication group of a quasigroup. Then we consider the two-transitive permutation groups systematically and explore which of them are multiplication groups of quasigroups. Here, we can settle some previously unknown cases, mainly with computational methods. It is perhaps worth mentioning that we found a commutative loop on 24 points whose multiplication group is the Mathieu group $M_{24}$. A non-commutative loop with this multiplication group had previously been found by Nagy [15].

Section 2 gives an account of Ihringer's results of [10]. We have reformulated these in terms of permutation groups, since this appears to be more appropriate to our computational approach. Section 3 contains a sufficient condition for a permutation group to be a multiplication group of a quasigroup. Our condition is a consequence of Ihringer's criterion [10, Theorem 1], but easier to check. Section 4 contains a systematic account on the knowledge about two-transitive permutation groups with respect to this question. In the last section we comment on some of the computational methods we applied.

## 2. Permutation groups

Let $n$ be a positive integer and put $Q_n := \{1, \ldots, n\}$. In order to simplify notation, we only consider quasigroups with underlying sets $Q_n$, usually writing $*$ for the multiplication to avoid confusion with integer multiplication. The multiplication group of a quasigroup $(Q_n, *)$ will thus be a subgroup of $S_n$, the group of permutations of $Q_n$.

For $\rho_1, \ldots, \rho_n \in S_n$ consider the matrix

$$T := T_{\rho_1,\ldots,\rho_n} := (i^{\rho_j})_{1 \le i,j \le n},$$

i.e. column $j$ of $T$ contains the images of $1, 2, \ldots, n$ under $\rho_j$.

The following lemma is obvious.

**Lemma 2.1.** *Let $\rho_1, \ldots, \rho_n \in S_n$ and put $T := T_{\rho_1,\ldots,\rho_n}$.*

(a) *The following statements are equivalent.*

(i) *$T$ is the multiplication table of a quasigroup on $Q_n$.*

(ii) *Every row of $T$ contains all the numbers $1, \ldots, n$.*

(iii) *For all $1 \le i \ne j \le n$, the permutation $\rho_i \rho_j^{-1}$ has no fixed points.*

(b) *Suppose $T$ satisfies the conditions of* (a)*. Let $Q$ be the quasigroup on the set $Q_n$ with multiplication table $T$. Then*

$$M(Q) = \langle \lambda_1, \ldots, \lambda_n, \rho_1, \ldots, \rho_n \rangle,$$

*where for* $1 \le i \le n$, $\lambda_i$ *is left multiplication by* $i$, *given by*

$$j^{\lambda_i} = i^{\rho_j}, \qquad 1 \le j \le n. \tag{1}$$

An alternative way of phrasing Condition (a)(ii) of Lemma 2.1 is to say that $R = \{\rho_1, \dots, \rho_n\}$ is a *driving sequence* in the sense of [2]. Similarly, Condition (a)(iii) is the same as saying that $R$ constitutes a *sharply transitive subset* of $G$, i.e. for every pair $(i, j)$ with $1 \le i, j \le n$, there is a unique $\rho \in R$ with $i^\rho = j$.

The direct product $S_n \times S_n \times S_n$ acts on the set of matrices satisfying the conditions of Lemma 2.1(a) as follows. Let $T = T_{\rho_1,\dots,\rho_n} =: (t_{ij})$ be such a matrix and let $(\pi, \sigma, \tau) \in S_n \times S_n \times S_n$. Then define $T^{\pi,\sigma,\tau} = (t'_{ij})$ by

$$t'_{ij} := t^{\tau}_{i'j'}$$

with $(i', j') := (i^{\pi^{-1}}, j^{\sigma^{-1}})$. Thus the first two components of $(\pi, \sigma, \tau)$ act by permuting the rows and columns of $T$, respectively, and the last component acts by renumbering its entries. We consider the effect of these actions on the multiplication group.

**Lemma 2.2.** *Let* $\rho_1, \dots, \rho_n \in S_n$ *such that* $T = T_{\rho_1,\dots,\rho_n}$ *satisfies the conditions of* Lemma 2.1(a), *and let* $(\pi, \sigma, \tau) \in S_n \times S_n \times S_n$.

*Let* $\rho'_1, \dots, \rho'_n, \lambda'_1, \dots, \lambda'_n \in S_n$ *such that* $T^{\pi,\sigma,\tau} = T_{\rho'_1,\dots,\rho'_n}$, *and such that* $\lambda'_1, \dots, \lambda'_n$ *are defined by* (1) *with respect to* $\rho'_1, \dots, \rho'_n$. *Fix* $1 \le i \le n$.

(a) *If* $\sigma = \tau = 1$, *then* $\rho'_i = \pi^{-1}\rho_i$ *and* $\lambda'_i = \lambda_{i'}$ *with* $i' = i^{\pi^{-1}}$.
(b) *If* $\pi = \tau = 1$, *then* $\rho'_i = \rho_{i'}$ *with* $i' = i^{\sigma^{-1}}$ *and* $\lambda'_i = \sigma^{-1}\lambda_i$.
(c) *If* $\pi = \sigma = 1$, *then* $\lambda'_i = \lambda_i\tau$, *and* $\rho'_i = \rho_i\tau$.

**Proof.** We only prove (a), since the other parts are proven similarly. Let $T = (t_{ij})$. Putting $i' = i^{\pi^{-1}}$, we have

$$i^{\rho'_j} = t_{i'j} = (i')^{\rho_j} = i^{\pi^{-1}\rho_j}$$

for all $1 \le i, j \le n$. Thus $\rho'_j = \pi^{-1}\rho_j$ for all $1 \le j \le n$. We also have

$$j^{\lambda'_i} = t_{i'j} = (i')^{\rho_j} = j^{\lambda_{i'}}$$

for all $1 \le i, j \le n$. Thus $\lambda'_i = \lambda_{i'}$ for all $1 \le i \le n$. □

Two quasigroups on $Q_n$ whose multiplication tables are in the same orbit under the action of $S_n \times S_n \times S_n$ are called *isotopic*. This relation can be used to construct inclusions between multiplication groups. The following lemma, which rephrases [10, Proposition 3], provides examples of such inclusions.

**Lemma 2.3.** [10, Proposition 3] *Let $Q = (Q_n, *)$ be a quasigroup. Then there are quasigroups $Q'$ and $Q''$ on the same underlying set $Q_n$, isotopic to $Q$, with $M(Q'') \leq M(Q') \leq M(Q)$ such that $Q'$ has a left unit and $Q''$ is a loop.*

**Proof.** For $1 \leq i \leq n$, write $\rho_i$ and $\lambda_i$ for the right and left multiplication with $i$, respectively. Let $T$ denote the multiplication table of $Q$. If $\lambda_1 = 1$, put $Q' = Q$. Otherwise, define $Q'$ by its multiplication table $T^{(1,\lambda_1,1)}$. Then $Q'$ has a left unit, and by Lemma 2.2(b) we have

$$\begin{aligned} M(Q') &= \langle \lambda_1^{-1}\lambda_1, \ldots, \lambda_1^{-1}\lambda_n, \rho'_1, \ldots, \rho'_n \rangle \\ &\leq \langle \lambda_1, \ldots, \lambda_n, \rho_1, \ldots, \rho_n \rangle = M(Q) \end{aligned}$$

(where $(\rho'_1, \ldots, \rho'_n)$ is a permutation of $(\rho_1, \ldots, \rho_n)$).

If $\rho'_1 = 1$, put $Q'' = Q'$. Otherwise, define $Q''$ by its multiplication table $T^{(\rho'_1,\lambda_1,1)}$. Then $Q''$ is a loop and

$$\begin{aligned} M(Q'') &= \langle \lambda_1^{-1}\lambda_1, \ldots, \lambda_1^{-1}\lambda_n, (\rho'_1)^{-1}\rho'_1, \ldots, (\rho'_1)^{-1}\rho'_n \rangle \\ &\leq M(Q') \leq M(Q). \end{aligned}$$

□

**Corollary 2.4.** ([10, Theorem 1]) *Let $G \leq S_n$. Then $G$ is the multiplication group of a quasigroup on $Q_n$, if and only if there is a loop $Q = (Q_n, *)$ and $\rho, \lambda \in S_n$ such that $G = \langle M(Q), \rho, \lambda \rangle$.*

**Proof.** If $G$ is the multiplication group of a quasigroup $Q$, let $Q''$ be as in Lemma 2.3. Then $M(Q) = \langle M(Q''), \rho_1, \lambda_1 \rangle$. Conversely, if $G = \langle M(Q), \rho, \lambda \rangle$, where $Q$ is a loop with multiplication table $T$, define the quasigroup $Q'$ by its multiplication table $T^{(\rho^{-1},\lambda^{-1},1)}$. By Lemma 2.2, $M(Q') = G$. □

Thus if $G \leq S_n$ does not contain a subgroup which is the multiplication group of a loop on $Q_n$, then $G$ is not the multiplication group of any quasigroup.

## 3. A sufficient condition

We continue with the notation from Section 2. The following corollary contains a sufficient condition for a permutation group to be the multiplication group of a quasigroup. It is a special case of Corollary 2.4, but its purely group theoretical condition is easier to check.

**Corollary 3.1.** *Let $G \leq S_n$. Suppose that $G$ contains an abelian subgroup $H$ acting regularly on $Q_n$.*

*If $G = \langle H, \rho, \lambda \rangle$ for some $\rho, \lambda \in G$, then $G$ is the multiplication group of a quasigroup on $Q_n$. If $G = \langle H, \rho \rangle$ for some $\rho \in G$, this quasigroup can be chosen to have a left or right unit.*

**Proof.** Number the elements of $H$ as $\rho_1, \rho_2, \ldots, \rho_n$ such that $1^{\rho_i} = i$ for $1 \leq i \leq n$. Then the multiplication table of $H$ with respect to the ordering $\rho_1, \ldots, \rho_n$ equals $T_{\rho_1,\ldots,\rho_n}$ (identifying an entry $i$ with $\rho_i$). Since $H$ is abelian, it is equal to the multiplication group $M(Q)$ of the loop on $Q_n$ with multiplication table $T_{\rho_1,\ldots,\rho_n}$. The first statement follows from Corollary 2.4. For the second statement use the construction in the proof of Lemma 2.3. □

The condition in Corollary 3.1 is not necessary. For example, the alternating group $A_6$, acting naturally on 6 letters, does not have a regular subgroup, but is the multiplication group of a quasigroup (see Section 4 below).

In [11, Theorem 1.1] the primitive permutation groups containing an abelian regular subgroup were determined. This gives a wealth of examples for groups satisfying the hypotheses of Corollary 3.1.

If $G \leq S_n$ satisfies the hypothesis of Corollary 3.1, then the Corollary together with the theorem of Smith show that $G$ is a multiplicity free permutation group. This can easier be shown directly.

**Lemma 3.2.** *Let the assumptions be as in* Corollary 3.1. *Then the permutation character corresponding to the natural action of $G$ on $Q_n$ is multiplicity free.*

**Proof.** Let $V$ denote the permutation $\mathbb{C}G$-module arising from the embedding $G \to S_n$. We have to show that $\mathrm{End}_{\mathbb{C}G}(V)$ is commutative. Since $\mathrm{End}_{\mathbb{C}G}(V)$ is contained in $\mathrm{End}_{\mathbb{C}H}(V{\downarrow_H})$ as a subalgebra, it suffices to show that the latter is commutative. Since $H$ acts regularly on $\{1, \ldots, n\}$, we have $\mathrm{End}_{\mathbb{C}H}(V{\downarrow_H}) \cong \mathbb{C}H$ as $\mathbb{C}$-algebra, and the result follows. □

## 4. Two-transitive groups

Using the classification of the finite simple groups, the two-transitive groups have been enumerated. These groups come in two types: Those with an elementary abelian socle, the affine groups, and those with a nonabelian simple socle, the almost simple groups. The tables in Cameron's book [1, Sections 7.3, 7.4] contain a complete description of all two-transitive groups. (We thank the referee for pointing out an omission in Cameron's table of the affine groups. A correct list can be found in [12, Appendix 1].)

4.1. **The almost simple two-transitive groups.** We summarize the known results for these groups, enumerating them by their simple socles. We have tried to locate all references to previously known cases. A missing reference for a particular result indicates that we are not aware of a corresponding publication. Most of the cases described below were treated by explicit computations, the strategy of which is explained in Section 5 at the end of our paper.

4.1.1. $A_n$. The groups $A_n$ and $S_n$ in their natural permutation representation are multiplication groups of quasigroups (even if they are not two-transitive). This is due to Ihringer [10, Theorem 2]. An $n$-cycle generates a regular subgroup of $S_n$. Except in case $n = 2m$, and $m$ odd, $A_n$ has a regular abelian subgroup. In the latter case, Ihringer constructs a commutative loop $Q$ on $Q_n$ with $M(Q) \leq A_n$. Since $S_n$ and $A_n$ are 2-generated, the result follows from Corollary 2.4.

A stronger result is due to Drápal and Kepka. They show in [6, Theorem (4.1)], that with the (true) exception of $n = 4, 5$, there is a loop of order $n$ whose multiplication (left, right ore two-sided) group is isomorphic to $A_n$.

Our computations suggest that for $n \geq 6$ there is always a commutative loop on $Q_n$ with multiplication group $S_n$. We are not aware of any general construction or reference supporting this observation.

4.1.2. $\mathrm{PSL}(d, q)$. If $G = \mathrm{PGL}(d, q)$ acting on the space of lines or on the space of hyperplanes of $\mathbb{F}_q^d$, then $G$ is the multiplication group of a quasigroup. Again, this is due to Ihringer [10, Theorem 2] and follows from the fact that $G$ is 2-generated and a Singer cycle is a regular subgroup.

For $d \geq 3$ and $q^d > 8$ (i.e. $q \neq 2$ if $d = 3$), Nagy has constructed in [15, Theorem 3.1] a loop $Q$ on $\mathbb{P}(\mathbb{F}_q^d)$ such that $\mathrm{PSL}(d, q) \leq M(Q) \leq \mathrm{PGL}(d, q)$. The case $d = 3$ and $q = 2$ is a true exception: There is no quasigroup on 7 points with multiplication group $\mathrm{PSL}(3, 2) = \mathrm{PGL}(3, 2)$. Our computations have shown that there are no quasigroups on the corresponding projective lines with multiplication groups $\mathrm{PSL}(3, 4)$ or $\mathrm{PSL}(3, 7)$, so that in these cases, the multiplication groups of Nagy's loop are $\mathrm{PGL}(3, 4)$ and $\mathrm{PGL}(3, 7)$, respectively.

Drápal [5] has shown that if $Q$ is a loop on the projective line $\mathbb{P}(\mathbb{F}_q)$ with multiplication group contained in $\mathrm{P\Gamma L}(2, q)$, then $M(Q)$ is isomorphic to a Singer cycle (unless $q = 3$ or 4). In particular, $\mathrm{PGL}(2, q)$ is not the multiplication group of a loop (the cases $q = 2, 3, 4$ do not provide exceptions to this latter statement). Together with Ihringer's criterion Drápal's result (or rather a weaker form of it) can be used to

show that $\mathrm{PSL}(2,q)$ is not the multiplication group of a quasigroup, if $q$ is odd and $> 3$.

**Proposition 4.1.** *If $q > 3$ is odd, $\mathrm{PSL}(2,q)$ is not the multiplication group of a quasigroup.*

**Proof.** Assume the contrary. By Ihringer's criterion (see Corollary 2.4), there is a loop $Q$ on $\mathbb{P}(\mathbb{F}_q)$ with $M(Q) \leq \mathrm{PSL}(2,q)$. Since $\mathrm{PSL}(2,q)$ is not triply transitive and every element fixes at most 2 points, it follows from [4, Proposition 2.5] that $Q$ is an abelian group. Hence $Q = M(Q) \leq \mathrm{PSL}(2,q)$ and $Q$ is a regular subgroup. However, $\mathrm{PSL}(2,q)$ does not have a regular subgroup for $q > 3$. □

We remark that $\mathrm{PSL}(2,3)$ is an exception to the above proposition. Indeed, $\mathrm{PSL}(2,3)$ is permutation equivalent to $A_4$ acing on 4 letters. The latter is the multiplication group of a quasigroup by Corollary 3.1.

4.1.3. $\mathrm{Sp}(2d,2)$, *$d \geq 2$, $n = 2^{2d-1} \pm 2^{d-1}$.* Here we only have information on the smallest cases $d = 2, 3$. Suppose first that $d = 2$. We have $\mathrm{Sp}(4,2) \cong S_6$. The action of $\mathrm{Sp}(4,2)$ on $2^{2\cdot 2-1} - 2^{2-1} = 6$ letters is permutation equivalent to the natural action of $S_6$, and thus $\mathrm{Sp}(4,2)$ is the multiplication group of a quasigroup on 6 points, in fact even of a commutative loop. On the other hand, there is no quasigroup on $2^{2\cdot 2-1} + 2^{2-1} = 10$ points with multiplicatin group $\mathrm{Sp}(4,2)$.

Let us now turn to the case $d = 3$, i.e. to the group $\mathrm{Sp}(6,2)$ acting on 28 or 36 points. Computer calculations have shown that this group is not the multiplication group of any quasigroup on 28 or 36 points.

4.1.4. $\mathrm{PSU}(3,q)$ *acting on $q^3 + 1$ points.* The groups $\mathrm{PSU}(3,2)$ and $\mathrm{PGU}(3,2)$ acting on 9 points, have regular abelian normal subgroups. The quotient groups are the quaternion group and $\mathrm{SL}(2,3)$, respectively. Since each of these can be generated by two elements, $\mathrm{PSU}(3,2)$ and $\mathrm{PGU}(3,2)$ are multiplication groups of quasigroups by Corollary 3.1.

The groups $\mathrm{PSU}(3,3)$ and $\mathrm{PSU}(3,4)$ acting on 28 and 65 points, respectively, are not multiplication groups of quasigroups.

4.1.5. $\mathrm{Sz}(q)$, *$q = 2^{2m+1}$, $m \geq 0$, acting on $q^2 + 1$ points.* The same argument as for $\mathrm{PSL}(2,q)$, $q$ odd, settles the following case.

**Proposition 4.2.** *If $q = 2^{2m+1}$, $m \geq 1$, then $\mathrm{Sz}(q)$ is not the multiplication group of a quasigroup.*

**Proof.** Analogous to the proof of Proposition 4.1. □

Note that $\mathrm{Sz}(2)$, being a Frobenius group on 5 points, is an exception to the above proposition.

4.1.6. $\mathrm{Ree}(q)$, $q = 3^{2m+1}$, $m \geq 0$, *acting on* $q^3 + 1$ *points.* We have only investigated the smallest case $q = 3$. Here, $\mathrm{Ree}(3) \cong \mathrm{P\Gamma L}(2, 8)$ acting on 28 points. Neither $\mathrm{P\Gamma L}(2, 8)$ nor its subgroup $\mathrm{PSL}(2, 8)$ are multiplication groups of quasigroups in this action.

4.1.7. $\mathrm{PSL}(2, 11)$ *and* $M_{11}$ *acting on* 11 *points.* Each of the groups $\mathrm{PSL}(2, 11)$ and $M_{11}$ acting on 11 points contain two conjugacy classes of 11-cycles acting fixed-point freely. In each case, the group is generated by two such 11-cycles. On the other hand, neither $\mathrm{PSL}(2, 11)$ nor $M_{11}$ are multiplication groups of loops. The results for $M_{11}$ are due to Ihringer [10, Theorem 2] and Drápal [5, p. 257], respectively.

4.1.8. $M_{11}$ *acting on* 12 *points.* This is not the multiplication group of any quasigroup.

4.1.9. $M_{12}$ *acting on* 12 *points.* This group is the multiplication group of a quasigroup, since it is generated by a regular subgroup and an additional element. It is also the multiplication group of a loop, the arithmetic progression loop constructed by Conway [3, p. 327].

4.1.10. $A_7$ *acting on* 15 *points.* This is not the multiplication group of any quasigroup.

4.1.11. $M_{22}$ *acting on* 22 *points.* This group is not the multiplication group of any quasigroup (see [5], [14]).

4.1.12. $M_{23}$ *acting on* 23 *points.* This group is the multiplication group of a quasigroup with a left unit, since it is generated by a regular subgroup and an additional element [10]. It is not the multiplication group of a loop [5, 15].

4.1.13. $M_{24}$ *acting on* 24 *points.* This is the multiplication group of a commutative loop. A non-commutative loop with multiplication group $M_{24}$ was found in [15]. We explicitly state one of the commutative loops we have found in Table 1.

4.1.14. $\mathrm{PSL}(2, 8)$ *acting on* 28 *points.* This has already been treated in the subsection on the Ree groups.

4.1.15. HS *acting on* 176 *points.* This is not the multiplication group of any quasigroup.

4.1.16. $\mathrm{Co}_3$ *acting on* 276 *points.* This case is still open. By a computer search we could prove, however, that no subgroup of $\mathrm{Co}_3$ is the multiplication group of a commutative loop.

TABLE 1. A commutative loop with multiplication group $M_{24}$

| | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| 2 | 23 | 16 | 9 | 21 | 7 | 11 | 12 | 8 | 17 | 14 | 19 | 1 | 5 | 6 | 20 | 18 | 4 | 3 | 22 | 13 | 10 | 24 | 15 |
| 3 | 16 | 24 | 12 | 13 | 17 | 23 | 7 | 19 | 2 | 22 | 20 | 10 | 4 | 21 | 15 | 11 | 5 | 8 | 18 | 14 | 1 | 6 | 9 |
| 4 | 9 | 12 | 1 | 6 | 10 | 2 | 23 | 3 | 22 | 17 | 15 | 24 | 16 | 14 | 18 | 21 | 19 | 7 | 11 | 5 | 13 | 8 | 20 |
| 5 | 21 | 13 | 6 | 24 | 1 | 10 | 22 | 16 | 23 | 2 | 18 | 3 | 12 | 8 | 14 | 15 | 20 | 11 | 9 | 4 | 17 | 19 | 7 |
| 6 | 7 | 17 | 10 | 1 | 24 | 20 | 19 | 23 | 18 | 13 | 11 | 12 | 22 | 3 | 21 | 4 | 9 | 14 | 8 | 15 | 16 | 5 | 2 |
| 7 | 11 | 23 | 2 | 10 | 20 | 24 | 18 | 17 | 15 | 21 | 3 | 9 | 8 | 1 | 6 | 12 | 16 | 4 | 14 | 22 | 19 | 13 | 5 |
| 8 | 12 | 7 | 23 | 22 | 19 | 18 | 1 | 10 | 9 | 16 | 14 | 6 | 21 | 17 | 11 | 5 | 24 | 20 | 13 | 2 | 15 | 4 | 3 |
| 9 | 8 | 19 | 3 | 16 | 23 | 17 | 10 | 1 | 5 | 24 | 2 | 20 | 15 | 18 | 4 | 6 | 13 | 21 | 7 | 12 | 14 | 22 | 11 |
| 10 | 17 | 2 | 22 | 23 | 18 | 15 | 9 | 5 | 1 | 4 | 13 | 14 | 11 | 7 | 24 | 20 | 12 | 6 | 16 | 19 | 21 | 3 | 8 |
| 11 | 14 | 22 | 17 | 2 | 13 | 21 | 16 | 24 | 4 | 1 | 7 | 8 | 19 | 20 | 5 | 9 | 10 | 15 | 6 | 23 | 3 | 18 | 12 |
| 12 | 19 | 20 | 15 | 18 | 11 | 3 | 14 | 2 | 13 | 7 | 23 | 17 | 6 | 4 | 9 | 16 | 21 | 1 | 5 | 8 | 24 | 10 | 22 |
| 13 | 1 | 10 | 24 | 3 | 12 | 9 | 6 | 20 | 14 | 8 | 17 | 23 | 18 | 11 | 22 | 19 | 15 | 5 | 21 | 7 | 2 | 16 | 4 |
| 14 | 5 | 4 | 16 | 12 | 22 | 8 | 21 | 15 | 11 | 19 | 6 | 18 | 24 | 13 | 2 | 10 | 3 | 23 | 1 | 20 | 9 | 7 | 17 |
| 15 | 6 | 21 | 14 | 8 | 3 | 1 | 17 | 18 | 7 | 20 | 4 | 11 | 13 | 23 | 19 | 22 | 2 | 16 | 24 | 9 | 5 | 12 | 10 |
| 16 | 20 | 15 | 18 | 14 | 21 | 6 | 11 | 4 | 24 | 5 | 9 | 22 | 2 | 19 | 1 | 23 | 8 | 10 | 12 | 3 | 7 | 17 | 13 |
| 17 | 18 | 11 | 21 | 15 | 4 | 12 | 5 | 6 | 20 | 9 | 16 | 19 | 10 | 22 | 23 | 24 | 7 | 13 | 3 | 1 | 8 | 2 | 14 |
| 18 | 4 | 5 | 19 | 20 | 9 | 16 | 24 | 13 | 12 | 10 | 21 | 15 | 3 | 2 | 8 | 7 | 23 | 22 | 17 | 6 | 11 | 14 | 1 |
| 19 | 3 | 8 | 7 | 11 | 14 | 4 | 20 | 21 | 6 | 15 | 1 | 5 | 23 | 16 | 10 | 13 | 22 | 24 | 2 | 17 | 12 | 9 | 18 |
| 20 | 22 | 18 | 11 | 9 | 8 | 14 | 13 | 7 | 16 | 6 | 5 | 21 | 1 | 24 | 12 | 3 | 17 | 2 | 23 | 10 | 4 | 15 | 19 |
| 21 | 13 | 14 | 5 | 4 | 15 | 22 | 2 | 12 | 19 | 23 | 8 | 7 | 20 | 9 | 3 | 1 | 6 | 17 | 10 | 24 | 18 | 11 | 16 |
| 22 | 10 | 1 | 13 | 17 | 16 | 19 | 15 | 14 | 21 | 3 | 24 | 2 | 9 | 5 | 7 | 8 | 11 | 12 | 4 | 18 | 23 | 20 | 6 |
| 23 | 24 | 6 | 8 | 19 | 5 | 13 | 4 | 22 | 3 | 18 | 10 | 16 | 7 | 12 | 17 | 2 | 14 | 9 | 15 | 11 | 20 | 1 | 21 |
| 24 | 15 | 9 | 20 | 7 | 2 | 5 | 3 | 11 | 8 | 12 | 22 | 4 | 17 | 10 | 13 | 14 | 1 | 18 | 19 | 16 | 6 | 21 | 23 |

4.2. **The two-transitive groups with elementary abelian socle.** Let $G$ be a two-transitive group with elementary abelian socle $V$. Then $V$ acts regularly and $G$ is the semidirect product $G = VH$ with $H$ a point stabilizer. Thus, whenever $H$ can be generated by two elements, $G$ is the multiplication group of a quasigroup by Corollary 3.1.

Hering has classified these two-transitive groups in [8, 9]. The list of occurring point stabilizers $H$ is contained in [8, §5] and in [12, Appendix 1]. These groups come in three infinite series, and a finite number of exceptional cases.

Using GAP, we have checked that all exceptional point stabilizers occurring in Part IV of Hering's list can be generated by two elements. A point stabilizer $H$ lying in an infinite series has a unique non-abelian composition factor $S$ which is normal in $H$, and $H/S$ is soluble. It would be a possible but tedious task to check which of the occurring point stabilizers are 2-generated. It is well known that every finite simple groups is 2-generated. Thus in case $H = S$ is simple, $G = VH$ is indeed the multiplication group of a quasigroup.

## 5. Searching for quasigroups by computer

Given a permutation group $G$ on $n$ points we used GAP [7] to search for a quasigroup with $G$ as multiplication group. We either want to find such a quasigroup or prove that such a quasigroup does not exist.

Using Lemma 2.2 there are some easy reductions of the problem: If there is a quasigroup with multiplication group $G$ then there is a loop with a subgroup of $G$ as multiplication group. And also the converse is true when $G$ is generated by two elements, see Corollary 2.4.

So, we want to search for a quasigroup whose multiplication table is given by row permutations $(\lambda_1, \ldots, \lambda_n)$ which also imply column permutations $(\rho_1, \ldots, \rho_n)$, such that $\lambda_1, \ldots, \lambda_n, \rho_1, \ldots, \rho_n \in G$. We can assume $\lambda_1 = \rho_1 = 1$. Furthermore, using $\pi = \sigma = \tau \in G$ in Lemma 2.2, we need to consider for $\lambda_2$ only representatives of conjugacy classes of fixed point free elements of $G$.

Given partial information $(\lambda_1, \ldots, \lambda_l)$ and $(\rho_1, \ldots, \rho_k)$ of a possible multiplication table we try to extend it as follows: If $l \leq k$ we find all possible $\lambda_{l+1}$, otherwise we first change the roles of the $\lambda_i$ and $\rho_i$. Such $\lambda_{l+1}$ must map the points $1, \ldots, k$ to $(l+1)^{\rho_1}, \ldots, (l+1)^{\rho_k}$. GAP can easily find out if such an element exists. If yes, the other such elements are obtained by left multiplication with the elements in the stabilizer of the tuple $(1, \ldots, k)$. For each such candidate for $\lambda_{l+1}$ we check if $\lambda_{l+1}\lambda_i^{-1}$ is fixed point free for $1 \leq i \leq l$. For each $\lambda_{l+1}$ fulfilling these conditions we recursively try to extend the table further.

Starting with the various $(\lambda_1 = 1, \lambda_2)$ and $(\rho_1 = 1)$ as described above this backtrack algorithm will either produce multiplication tables of quasigroups we are looking for, or it will show that such quasigroups do not exist.

This algorithm performs quite well in the examples mentioned in the last section. It seems that extending the $\lambda$'s and $\rho$'s alternately often shows quite early in the recursion that a partial table cannot be extended further.

Compared to the algorithms described in [14] and in [15] our variant needs very little memory and is easy to distribute to several machines. As examples, our program needed less than 4 minutes to check that the Mathieu group $M_{22}$ on 22 points is not the multiplication group of a quasigroup. The result for HS on 176 points only needed 30 seconds.

We noticed that many groups with a subgroup which is the multiplication group of a loop also have such a subgroup which is the multiplication group of a commutative loop. By setting $\rho_i = \lambda_i$ for all $i$ in our backtrack search we can restrict the search to commutative loops.

## Acknowledgement

We thank Barbara Baumeister for bringing reference [11] to our attention. Thanks are also due to Michael Guidici and Cheryl Praeger for discussions on the subject of this paper. Finally, we are indebted to Klaus Lux for suggesting a connection to permutation arrays (which was not pursued further).

## References

[1] P. J. Cameron, Permutation groups, London Mathematical Society Student Texts, 45. Cambridge University Press, Cambridge, 1999.

[2] J. J. Carroll, G. A. Fisher, A. M. Odlyzko and N. J. A. Sloane, What are the Latin Square Groups? *Amer. Math. Monthly* **80** (1973), 1045–1046.

[3] J. H. Conway, The Golay codes and the Mathieu groups, in: J. H. Conway and N. J. A. Sloane, Sphere packings, lattices and groups, 3rd ed., Springer, 1999, Chapter 11, pp. 299–330.

[4] A. Drápal, Multiplication groups of finite loops that fix at most two points, *J. Algebra* **235** (2001), 154–175.

[5] A. Drápal, Multiplication groups of loops and projective semilinear transformations in dimension two, *J. Algebra* **251** (2002), 256–278.

[6] A. Drápal and T. Kepka, Alternating groups and Latin squares, *European J. Combin.* **10** (1989), 175–180.

[7] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4.12, 2008, (`http://www.gap-system.org`).

[8] C. Hering, Transitive linear groups and linear groups which contain irreducible subgroups of prime order, *Geom. Dedicata* **2** (1974), 425–460.

[9] C. Hering, Transitive linear groups and linear groups which contain irreducible subgroups of prime order, II, *J. Algebra* **93** (1985), 151–164.

[10] T. Ihringer, On multiplication groups of quasigroups, *European J. Combin.* **5** (1984), 137–141.

[11] C. H. Li, The finite primitive permutation groups containing an abelian regular subgroup, *Proc. London Math. Soc.* **87** (2003), 725–747.

[12] M. W. Liebeck, The affine permutation groups of rank three, *Proc. London Math. Soc.* **54** (1987), 477–516.

[13] S. Köhler, Multiplikationsgruppen von Quasigruppen, Diploma thesis, RWTH Aachen University, 2007.

[14] P. Müller and G. P. Nagy, A note on the group of projectivities of finite projective planes, *Innov. Incidence Geom.* **6/7** (2007/08), 291–294.

[15] G. P. Nagy, On the multiplication groups of semifields, *European J. Combin.* **31** (2010), 18–24.

[16] J. D. H. Smith, Representation theory of infinite groups and finite quasigroups, Séminaire de Mathématiques Supérieures, 101. Presses de l'Université de Montréal, Montreal, QC, 1986, 132 pp.

LEHRSTUHL D FÜR MATHEMATIK, RWTH AACHEN UNIVERSITY, 52056 AACHEN, GERMANY

*E-mail address*: gerhard.hiss@math.rwth-aachen.de

*E-mail address*: frank.luebeck@math.rwth-aachen.de