Okubo quasigroups

Jonathan D. H. Smith and Petr Vojtěchovský

Abstract. Paige loops, simple non-associative Moufang loops, were constructed by Paige as quotients of the set of Zorn vector-matrices of unit norm under split octonion multiplication. In this paper, we show that the same quotient set sustains two related simple quasigroup structures, in which the split octonion multiplication is replaced with multiplication from para-octonion and Okubo algebras. The new quasigroups are known respectively as the para-Paige and Okubo quasigroups. We study the properties of these simple quasigroups: their multiplication groups, power structure, generating sets, subquasigroups, and automorphisms. Notably, examination of the power structure in the Okubo quasigroups leads to analysis of a class of hitherto unstudied identities holding in Moufang loops.

2010 Mathematics Subject Classification: 20N05, 17A75
Keywords and Phrases: Quasigroup, Zorn vector matrix, Zorn algebra, para-Zorn algebra, Okubo algebra, Paige loop, para-Paige quasigroup, Okubo quasigroup, semisymmetric quasigroup, Moufang loop, automorphism group, smallest generating set, multiplication group, character table.

1 Introduction

Let K be a commutative unital ring. Consider the split octonion algebra over K realized, for example, by the algebra $\mathsf{Zorn}(K)$ of Zorn vector-matrices [14, 35], cf. Section 4. The underlying free K-module of rank 8 carries three algebra structures of interest:

- The original Zorn vector-matrix multiplication $\cdot$, giving rise to the split octonion algebra $\mathsf{Zorn}(K)$;
- The multiplication $x \circ y = \overline{x} \cdot \overline{y}$, giving rise to the *para-Zorn* algebra $\mathsf{PZorn}(K) = (\mathsf{Zorn}(K), \circ)$ whose properties are closely related to those of the split octonion algebra [5, 8, 26];

- The multiplication $x * y = \overline{x\rho} \cdot \overline{x\rho^2}$, giving rise to the *Okubo algebra* $\mathsf{Okubo}(K) = (\mathsf{Zorn}(K), *)$ [5, 8, 23, 24]. Here, ρ is a certain order-3 automorphism of the split octonion algebra $\mathsf{Zorn}(K)$.

All three of these nonassociative algebras come equipped with a norm that permits composition. Consequently, the elements of norm 1 form a subset closed under multiplication, in fact a quasigroup, cf. Subsection 1.1.

In this paper we are particularly interested in the quasigroups of norm 1 elements in the three algebras, and the quotients of these quasigroups by the congruence identifying x with $-x$. For a field F, the quotient construction yields the *Paige loops* $\mathsf{PSL}_{1+3}(F)$ from $\mathsf{Zorn}(F)$ [25], the *para-Paige quasigroups* $\mathsf{PP}(F)$ from $\mathsf{PZorn}(F)$, and the *Okubo quasigroups* $\mathsf{OQ}(F)$ from $\mathsf{Okubo}(F)$. (The subscript $1+3$ in this notation reflects the structure of the Zorn vector-matrices, with scalars on the diagonal and 3-dimensional vectors off the diagonal.)

Although the three quasigroups $\mathsf{PSL}_{1+3}(F)$, $\mathsf{PP}(F)$ and $\mathsf{OQ}(F)$ are isotopic, their properties are quite different. This is particularly true for the Okubo quasigroups $\mathsf{OQ}(F)$. We obtain many new results for $\mathsf{PP}(F)$ and $\mathsf{OQ}(F)$. The paper is organized as follows:

In Section 2 we show that quasigroups isotopic to simple loops are simple. The argument is not difficult, and we present it in full detail since it does not seem to be available in the literature.

In Section 3 we develop an abstract and purely multiplicative notion of a *norm-supporting triple* that is applicable for all three of the above algebras. In this setting, elements of norm 1 form a semisymmetric quasigroup, while elements whose norm is invertible form a weakly semisymmetric magma. Weak semisymmetry naturally explains the fifth-degree identity discussed by Petersson in [26].

The three algebras are defined in Section 4. For Okubo algebras we use two approaches: directly in terms of a *canonical basis*, and then as an isotope of the Zorn algebra.

In Section 5 we introduce the three quasigroups of norm 1 elements modulo the normal subgroup $\{\pm 1\}$. Using the results of Section 2, we show that they are simple. (In the finite case, an alternative approach to the simplicity may be based on the character tables discussed in Section 9.)

While $\mathsf{PSL}_{1+3}(F)$ is power-associative and diassociative (and indeed, a Moufang loop), $\mathsf{PP}(F)$ is power-associative only if $|F| \in \{2, 3\}$ and it is never diassociative. The Okubo quasigroups $\mathsf{OQ}(F)$ are never power-associative. We present these results in Section 6. The behavior of powers and mono-generated subquasigroups in Okubo quasigroups turns out to be very delicate, depending on certain consequences of the Moufang identities that we present here for the first time.

In Section 7 we recall results about automorphism groups of Paige loops, and transfer them to the setting of para-Paige quasigroups. We prove that the automorphism groups $\mathrm{Aut}(\mathsf{PSL}_{1+3}(F))$ and $\mathrm{Aut}(\mathsf{PP}(F))$ coincide for all fields. In particular, $\mathrm{Aut}(\mathsf{PP}(F))$ is the split extension $\mathsf{G}_2(F) \rtimes \mathrm{Aut}(F)$ when F is a

perfect field. Furthermore, we show that linear automorphisms of the three algebras induce multiplicative automorphisms of the three quasigroups of norm 1 elements modulo the normal subgroup $\{\pm 1\}$, and that this assignment is injective. Finally, we compute the automorphism groups $\mathrm{Aut}(\mathsf{OQ}(2))$ and $\mathrm{Aut}(\mathsf{Okubo}(2))$.

Multiplication groups of the three types of quasigroups are described in Section 8, again taking advantage of the known result that for Paige loops, the multiplication group is $\mathsf{D}_4(F)$. We show that $\mathrm{Mlt}(\mathsf{PP}(F)) = \mathsf{D}_4(F).2 = \mathrm{Mlt}(\mathsf{OQ}(F))$. Furthermore, as observed in Section 9, the character tables of $\mathsf{PSL}_{1+3}(F)$, $\mathsf{PP}(F)$ and $\mathsf{OQ}(F)$ coincide.

The *rank* $r(Q)$ of a quasigroup Q is the smallest cardinality of a generating set of Q. It is known that $r(\mathsf{PSL}_{1+3}(q)) = 3$. We prove that $r(\mathsf{PP}(q)) = 3$ as well. In fact, one may choose a 3-generator subset that simultaneously generates $\mathsf{PSL}_{1+3}(q)$ and $\mathsf{PP}(q)$. We prove that $r(\mathsf{OQ}(q)) = 2$ when $q \not\equiv 1 \pmod 3$, and that $2 \leq r(\mathsf{OQ}(q)) \leq 3$ when $q \equiv 1 \pmod 3$.

In Section 11 we study Hasse diagrams modulo the action of the automorphism group that allow us to illustrate complicated posets of subalgebras by comparatively simple diagrams. Then in Section 12 we examine the subloop structure of $\mathsf{PSL}_{1+3}(2)$, and calculate the subquasigroup structure of $\mathsf{PP}(2)$ and $\mathsf{OQ}(2)$. Open problems are collected in Section 13.

1.1 PRELIMINARIES

A set Q with binary operations $*$, $/$, $\backslash$ is a *quasigroup* $(Q, *, /, \backslash)$ if the identities

$$(x * y)/y = x, \quad (x/y) * y = x, \quad x\backslash(x * y) = y, \quad x * (x\backslash y) = y$$

hold for all $x, y \in Q$. Equivalently, $(Q, *)$ is a quasigroup if the translations

$$L(x) : Q \to Q;\ y \mapsto yL(x) = x * y, \quad R(x) : Q \to Q;\ y \mapsto yR(x) = y * x$$

are bijections of Q, in which case we have $x\backslash y = yL(x)^{-1}$ and $x/y = xR(y)^{-1}$. We will also use the notation $L_*(x)$, $R_*(x)$ for translations if we need to keep track of the multiplication operation. The default multiplication operation will be denoted by $\cdot$ with the usual convention that xy means $x \cdot y$. Moreover, if we use juxtaposition, $\cdot$, $/$ and $\backslash$ in the same expression, then we assume that juxtaposition is more binding than the divisions which are in turn more binding than $\cdot$. For instance $x\backslash y \cdot uv/w$ stands for $(x\backslash y) \cdot ((u \cdot v)/w)$.

The symmetric group on a set Q (the group of bijections $Q \to Q$) is denoted by $Q!$. The *multiplication group* of a quasigroup $(Q, \cdot, /, \backslash)$ is the subgroup $\mathrm{Mlt}(Q) = \langle L_x, R_x \mid x \in Q \rangle_{Q!}$ of $Q!$ generated by all translations.

A quasigroup $(Q, \cdot, /, \backslash)$ is a *loop* if it possesses an identity element, that is, an element $e \in Q$ such that $ex = x = xe$ holds for all $x \in Q$.

The *inner mapping group* $\mathrm{Inn}(Q)$ of a loop Q is the stabilizer of the identity element $e \in Q$ in $\mathrm{Mlt}(Q)$.

2 Isotopes of simple loops

In this brief section we observe that quasigroup isotopes of simple loops are themselves simple. Recall that a "universal" algebra A (in the sense of [27, Appendix B]) is *simple* if it is not the domain of a nonconstant noninjective homomorphism. Also recall that a group G acts *primitively* on a set A if it acts transitively on A and the only partitions of A preserved by the action are $\{\{x\} \mid x \in A\}$ and $\{A\}$ [7].

Proposition 2.1 ([29, Corollary 2.1]). *A quasigroup Q is simple if and only if the multiplication group* $\mathrm{Mlt}(Q)$ *acts primitively on the set Q.*

Let $(Q_1, \cdot)$, $(Q_2, *)$ be quasigroups. A triple (α, β, γ) of bijections $Q_1 \to Q_2$ is an *isotopy* from $(Q_1, \cdot)$ onto $(Q_2, *)$ if for every x, $y \in Q_1$ we have $x\alpha * y\beta = (x \cdot y)\gamma$. An isotopy (α, β, γ) on the same set is *principal* if $\gamma = 1$. By a result of Bruck (see for instance [27, p.5]), every isotopy from $(Q_1, \cdot)$ onto $(Q_2, *)$ is a composition of a principal isotopy from $(Q_1, \cdot)$ onto some quasigroup $(Q_1, \circ)$ and an isomorphism from $(Q_1, \circ)$ onto $(Q_2, *)$.

Lemma 2.2. *Suppose that $(\alpha, \beta, 1)$ is a principal isotopy from a quasigroup Q onto a loop L. Then* $\mathrm{Mlt}(Q) = \langle \mathrm{Mlt}(L), \alpha, \beta \rangle$.

Proof. Let $Q = (X, \cdot)$ and $L = (X, \circ)$. Since $x\alpha \circ y\beta = x \cdot y$, we have $L(x) = \beta L_\circ(x\alpha)$ and $R(y) = \alpha R_\circ(y\beta)$. Then

$$\begin{aligned}\mathrm{Mlt}(Q) &= \langle L(x), R(x) \mid x \in X \rangle \\ &= \langle \beta L_\circ(x\alpha), \alpha R_\circ(x\beta) \mid x \in X \rangle = \langle \beta L_\circ(x),\ \alpha R_\circ(x) \mid x \in X \rangle\end{aligned}$$

because α, β are bijections of X.
Let e be the identity element of the loop L. Then $L_\circ(e) = R_\circ(e) = 1$ and therefore $\alpha = \alpha R_\circ(e)$ and $\beta = \beta L_\circ(e)$ are elements of $\mathrm{Mlt}(Q)$. But then $L_\circ(x) = \beta^{-1}(\beta L_\circ(x))$ and $R_\circ(x) = \alpha^{-1}(\alpha R_\circ(x))$ are elements of $\mathrm{Mlt}(Q)$ for every $x \in X$ and we have $\langle \mathrm{Mlt}(L), \alpha, \beta \rangle \leq \mathrm{Mlt}(Q)$. Conversely, it is clear that $L(x)$, $R(x) \in \langle \mathrm{Mlt}(L), \alpha, \beta \rangle$ and hence $\mathrm{Mlt}(Q) \leq \langle \mathrm{Mlt}(L), \alpha, \beta \rangle$. □

Theorem 2.3. *Let Q be a quasigroup isotopic to a simple loop. Then Q is simple.*

Proof. Let $Q = (X, \cdot)$ be isotopic to a simple loop K. Then there is a quasigroup $L = (X, \circ)$ isomorphic to K, together with bijections α, β of X, such that $(\alpha, \beta, 1)$ is a principal isotopy from Q onto L. In particular, L is a simple loop. By Lemma 2.2, $\mathrm{Mlt}(Q) = \langle \mathrm{Mlt}(L), \alpha, \beta \rangle$. By Proposition 2.1, $\mathrm{Mlt}(L)$ acts primitively on X, so $\mathrm{Mlt}(Q)$ also acts primitively on X, being a supergroup of $\mathrm{Mlt}(L)$. Then applying Proposition 2.1 again, we see that Q is simple. □

Example 2.4. Let L be the underlying abelian group of $\mathsf{GF}(2^2)$. Let Q be the quasigroup defined on $\mathsf{GF}(2^2)$ by the multiplication $x \cdot y = x + \omega y$, where ω is a primitive element of $\mathsf{GF}(2^2)$. Then although L is isotopic to the simple quasigroup Q, the loop L is not simple.

3 Semisymmetry

3.1 Invariant products and forms

Definition 3.2 establishes a purely multiplicative approach to ring-theoretic topics considered by Okubo and Osborn in [24]. A *magma* is a set with a binary operation. A *monoid* is an associative magma with an identity element. If $(M, \cdot, 1)$ is a monoid then a set X with a monoid homomorphism from M to the monoid of all functions $X \to X$ is an *M-set*. (For more on M-sets, see [30, I.1].) A quasigroup is *semisymmetric* if it satisfies the identity $y(xy) = x$. (For a discussion of semisymmetry in quasigroups, see [27, §1.4].)

Proposition 3.1 ([27, Corollary 1.1 and Proposition 1.2]). *If $(Q, \cdot)$ is a magma satisfying $y(xy) = x$ then it is a semisymmetric quasigroup. The following identities are equivalent in quasigroups: $y(xy) = x$, $(yx)y = x$, $x\backslash y = yx$, $x/y = yx$.*

Definition 3.2. A triple (A, M, N) is called *norm-supporting* if

- $A = (A, \cdot)$ is a magma,
- $(M, \cdot, 1)$ is a commutative submonoid of $(A, \cdot)$,
- A is an M-set with respect to the operations $(x, m) \mapsto x \cdot m$, where $x \in A$, $m \in M$,
- A is M-invariant in the sense that $(xm)(yn) = (xy)(mn)$ for every x, $y \in A$ and m, $n \in M$,
- $N : A \times A \to A$ satisfies $N(x, x) \in M$ for every $x \in A$,
- N is M-invariant in the sense that $N(xm, yn) = N(x, y)mn$ for all x, $y \in A$ and m, $n \in M$.

The induced map $N : A \to M; x \mapsto N(x, x)$ is called a *norm*.
A norm-supporting triple (A, M, N) (or just the norm N, if A and M are clear from the context)

- is *semisymmetric* if $y(xy) = (yx)y = xN(y)$ holds for all x, $y \in A$,
- is *associative* if $N(xy, z) = N(x, yz)$ holds for all x, y, $z \in A$,
- *permits composition* if $N : A \to M$ is a magma homomorphism.

Theorem 3.3. *Let (A, M, N) be a norm-supporting triple.*

(a) *If N is associative and semisymmetric, it permits composition.*

(b) *If N permits composition, then the sets*

$$SQ(A) = \{x \in A \mid N(x) = 1\},$$
$$Q(A) = \{x \in A \mid N(x) \text{ is invertible in } M\}$$

are submagmas of $(A, \cdot)$.

(c) *If N permits composition and is semisymmetric, then $SQ(A)$ is a semisymmetric quasigroup.*

(d) *If N permits composition and is semisymmetric, then $Q(A)$ is a quasigroup, and for every $x \in Q(A)$ the translations $L(x)$, $R(x)$ are bijections of A.*

Proof. (a) For elements x, y of A, one has

$$N(xy) = N(xy, xy) = N(x, y(xy)) = N(x, xN(y)) = N(x)N(y)$$

by respective application of the associativity, semisymmetry, and the M-invariance of N.
Part (b) follows on noting that $SQ(A)$ is the preimage of the submagma $\{1\}$ of M under the magma homomorphism $N\colon A \to M$, while $Q(A)$ is the preimage of the group M^* of invertible elements of M.
For (c), by semisymmetry of N, the magma $SQ(A)$ satisfies the identity $y(xy) = xN(y) = x$, and thus $SQ(A)$ is a semisymmetric quasigroup by Proposition 3.1.
Finally, for any $x \in Q(A)$ and $y \in A$, define $x\backslash y = yxN(x)^{-1}$ and $y/x = xyN(x)^{-1}$. Note that $x\backslash y$, y/x are elements of $Q(A)$ if $y \in Q(A)$. In any case, by semisymmetry of N we have

$$\begin{aligned} x(x\backslash y) &= x(yxN(x)^{-1}) = x(yx)N(x)^{-1} = yN(x)N(x)^{-1} = y, \\ x\backslash(xy) &= (xy)xN(x)^{-1} = yN(x)N(x)^{-1} = y \end{aligned}$$

and, similarly, $(y/x)x = y$, $(yx)/x = y$. This proves that $L(x)$, $R(x)$ are bijections of A, and that $Q(A)$ is a quasigroup. □

3.2 Weak semisymmetry

In general, the quasigroups $Q(A)$ that are exhibited in Theorem 3.3(d) are not semisymmetric. Nevertheless, they do satisfy a certain identity.

Definition 3.4. Let $(Q, \cdot)$ be a quasigroup. For each element q of Q, consider the *right bimultiplication*

$$R(q)L(q) = B(q)\colon Q \to Q; x \mapsto q(xq)\,.$$

Then the quasigroup $(Q, \cdot)$ is said to be *weakly right semisymmetric* if

$$B\colon Q \to Q!$$

is a magma homomorphism from $(Q, \cdot)$ to the symmetric group $Q!$. Dually, $(Q, \cdot)$ is said to be *weakly left semisymmetric* if the mapping $q \mapsto L(q)R(q)$ is a magma homomorphism from Q to $Q!$. Then $(Q, \cdot)$ is *weakly semisymmetric* if it is weakly right and left semisymmetric.

The weak right semisymmetry condition of Definition 3.4 may be written in the explicit form

$$z \cdot (y \cdot xy)z = yz \cdot x(yz) \tag{3.1}$$

of a magma identity, expressing the equation $B(y)B(z) = B(yz)$ for elements y, z of Q. Note that (3.1) is the opposite of the fifth-degree identity discussed by Petersson [26, (I)]. Thus that identity may be interpreted in the current terms as expressing weak left semisymmetry.

PROPOSITION 3.5. *Let (A, M, N) be a norm-supporting triple and suppose that N permits composition and is semisymmetric. Then the quasigroups $Q(A)$ exhibited in Theorem 3.3(d) are weakly right semisymmetric.*

Proof. For elements x, y, z of $Q(A)$, one has

$$z \cdot (y \cdot xy)z = xN(y)N(z) = xN(yz) = yz \cdot x(yz)$$

as required. □

EXAMPLE 3.6. The quasigroup with multiplication table

2	4	1	6	3	8	5	7
4	3	7	1	8	2	6	5
1	7	3	5	4	6	2	8
3	1	5	2	7	4	8	6
6	8	4	7	2	5	1	3
8	2	6	4	5	3	7	1
5	6	2	8	1	7	3	4
7	5	8	3	6	1	4	2

is weakly right semisymmetric, but not weakly left semisymmetric. The example was found with the finite-model builder `Mace4` [18].

4 ZORN VECTOR MATRICES

4.1 THE ZORN VECTOR-MATRIX ALGEBRA $\mathsf{Zorn}(K)$

Suppose that K is a commutative unital ring. A *Zorn vector-matrix* over K is a 2×2 matrix

$$z = \begin{bmatrix} \alpha & \mathbf{a} \\ \mathbf{b} & \beta \end{bmatrix} \tag{4.1}$$

in which α and β are scalars from K, while $\mathbf{a}$ and $\mathbf{b}$ are 3-dimensional row vectors over K, elements of the free module K^3 of rank 3. A *Zorn scalar* is a vector-matrix of the form

$$\begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix}$$

for an element α of the ring K. In particular, the *Zorn identity matrix* is the vector-matrix

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

For a Zorn-vector matrix (4.1) we introduce the *Zorn conjugate* $\overline{z}$, *transpose* z^T and *conjugate transpose* $z^* = \overline{z}^T$ as follows:

$$\overline{z} = \begin{bmatrix} \beta & -\mathbf{a} \\ -\mathbf{b} & \alpha \end{bmatrix}, \quad z^T = \begin{bmatrix} \alpha & \mathbf{b} \\ \mathbf{a} & \beta \end{bmatrix}, \quad z^* = \begin{bmatrix} \beta & -\mathbf{b} \\ -\mathbf{a} & \alpha \end{bmatrix}.$$

The *norm* or *Zorn determinant* of the Zorn vector-matrix (4.1) is the ring element

$$|z| = \begin{vmatrix} \alpha & \mathbf{a} \\ \mathbf{b} & \beta \end{vmatrix} = \alpha\beta - \mathbf{a} \cdot \mathbf{b} \tag{4.2}$$

defined using the usual scalar product

$$\mathbf{a} \cdot \mathbf{b} = [a_0\ a_1\ a_2] \cdot [b_0\ b_1\ b_2] = a_0b_0 + a_1b_1 + a_2b_2$$

of row vectors.

DEFINITION 4.1. The *Zorn vector-matrix algebra* $\mathsf{Zorn}(K)$ over the ring K is the free K-module of rank 8 consisting of all the Zorn vector-matrices over K. The module operations are defined componentwise, while the product of two Zorn vector-matrices is given as

$$\begin{bmatrix} \alpha & \mathbf{a} \\ \mathbf{b} & \beta \end{bmatrix} \cdot \begin{bmatrix} \gamma & \mathbf{c} \\ \mathbf{d} & \delta \end{bmatrix} = \begin{bmatrix} \alpha\gamma + \mathbf{a} \cdot \mathbf{d} & \alpha\mathbf{c} + \delta\mathbf{a} - \mathbf{b} \times \mathbf{d} \\ \gamma\mathbf{b} + \beta\mathbf{d} + \mathbf{a} \times \mathbf{c} & \mathbf{b} \cdot \mathbf{c} + \beta\delta \end{bmatrix} \tag{4.3}$$

using the usual vector or cross product

$$[a_0\ a_1\ a_2] \times [b_0\ b_1\ b_2] = [a_1b_2 - a_2b_1 \quad a_2b_0 - a_0b_2 \quad a_0b_1 - a_1b_0]$$

of row vectors.
The ring K is identified with the subalgebra of Zorn scalars; indeed

$$\begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} \cdot \begin{bmatrix} \alpha & \mathbf{a} \\ \mathbf{b} & \beta \end{bmatrix} = \begin{bmatrix} \lambda\alpha & \lambda\mathbf{a} \\ \lambda\mathbf{b} & \lambda\beta \end{bmatrix} = \begin{bmatrix} \alpha & \mathbf{a} \\ \mathbf{b} & \beta \end{bmatrix} \cdot \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} \tag{4.4}$$

for λ in K.
There is a bilinear map

$$N : \mathsf{Zorn}(K) \times \mathsf{Zorn}(K) \to \mathsf{Zorn}(K); \quad (u, v) \mapsto u \cdot \overline{v}.$$

Straightforward computation establishes the following result.

LEMMA 4.2. *Consider* u, $v \in \mathsf{Zorn}(K)$.

(a) $\overline{\overline{u}} = u$ *and* $\overline{u \cdot v} = \overline{v} \cdot \overline{u}$,

(b) $(u^T)^T = u$ *and* $(u \cdot v)^T = v^T \cdot u^T$,

(c) $u^* = \overline{u}^T = \overline{u^T}$, $(u^*)^* = u$ *and* $(u \cdot v)^* = u^* \cdot v^*$.

Recall the *Moufang identities*

$$\begin{aligned}(x \cdot yz)x &= xy \cdot zx,\\ x(yz \cdot x) &= xy \cdot zx,\\ (xy \cdot x)z &= x(y \cdot xz),\\ (xy \cdot z)y &= x(y \cdot zy).\end{aligned}$$

PROPOSITION 4.3 ([25, Lemma 3.2]). *The triple* $(\mathsf{Zorn}(K),K,N)$ *is norm-supporting (cf. Definition 3.2). The Zorn norm* $|\_|$ *is given by* $|u| = N(u,u) = u \cdot \overline{u} = \overline{u} \cdot u$ *and it permits composition. The magma* $(\mathsf{Zorn}(K), \cdot)$ *satisfies the Moufang identities.*

It can be checked directly that the identity

$$\overline{x}(xy) = (\overline{x}x)y = yN(x) = y(x\overline{x}) = (yx)\overline{x} \tag{4.5}$$

holds in the Zorn vector-matrix algebra $\mathsf{Zorn}(K)$.
Let $\mathsf{SL}_3(K)$ denote the group of (3×3)-matrices over K having determinant 1. Write A^{-T} for the transposed inverse of an element $A \in \mathsf{SL}_3(K)$. Then define $A_{\mathsf{Zorn}(K)}$ or

$$A\colon \mathsf{Zorn}(K) \to \mathsf{Zorn}(K); \begin{bmatrix}\alpha & \mathbf{a}\\ \mathbf{b} & \beta\end{bmatrix} \mapsto \begin{bmatrix}\alpha & \mathbf{a}\\ \mathbf{b} & \beta\end{bmatrix}^A = \begin{bmatrix}\alpha & \mathbf{a}A\\ \mathbf{b}A^{-T} & \beta\end{bmatrix}. \tag{4.6}$$

Using the identities $\mathbf{a} \cdot \mathbf{b} = \mathbf{a}A \cdot \mathbf{b}A^{-T}$ and $(\mathbf{a} \times \mathbf{b})A = \mathbf{a}A^{-T} \times \mathbf{b}A^{-T}$ (cf. [5, Proposition 5.7]), it is straightforward to check that $A_{\mathsf{Zorn}(K)}$ is an automorphism of $\mathsf{Zorn}(K)$, $\overline{u}A = \overline{uA}$ for every $u \in \mathsf{Zorn}(K)$, and A is an isometry of $(\mathsf{Zorn}(K), |\ |)$. In particular,

$$\rho = \begin{bmatrix}0 & 1 & 0\\ 0 & 0 & 1\\ 1 & 0 & 0\end{bmatrix} \in \mathsf{SL}_3(K) \tag{4.7}$$

induces an automorphism of $\mathsf{Zorn}(K)$. Note that $\rho^3 = I_3$ and $\rho^{-T} = \rho$.

4.2 THE PARA-ZORN ALGEBRA $\mathsf{PZorn}(K) = (\mathsf{Zorn}(K), \circ)$

DEFINITION 4.4. Let K be a commutative unital ring. Then the *para-Zorn algebra* $\mathsf{PZorn}(K) = (\mathsf{Zorn}(K), \circ)$ is given by the product

$$u \circ v = \overline{u} \cdot \overline{v} \tag{4.8}$$

on the underlying module $\mathsf{Zorn}(K)$ of Zorn vector-matrices.

PROPOSITION 4.5. *Let K be a commutative, unital ring. Then the equation*

$$\begin{bmatrix} \alpha & \mathbf{a} \\ \mathbf{b} & \beta \end{bmatrix} \circ \begin{bmatrix} \gamma & \mathbf{c} \\ \mathbf{d} & \delta \end{bmatrix} = \begin{bmatrix} \beta\delta + \mathbf{a}\cdot\mathbf{d} & -\beta\mathbf{c} - \gamma\mathbf{a} - \mathbf{b}\times\mathbf{d} \\ -\delta\mathbf{b} - \alpha\mathbf{d} + \mathbf{a}\times\mathbf{c} & \mathbf{b}\cdot\mathbf{c} + \alpha\gamma \end{bmatrix}$$

presents an explicit version of the para-Zorn product.
The triple $(\mathsf{PZorn}(K), K, N)$ is norm-supporting. The norm N is semisymmetric, and it permits composition.

Proof. The formula follows by straightforward calculation. Note that $m \circ n = m \cdot n$ for scalar matrices m, n. It is then easy to show that $(\mathsf{PZorn}(K), K, N)$ is norm-supporting. We have

$$y \circ (x \circ y) = \overline{y}(\overline{\overline{x}\,\overline{y}}) = \overline{y}(yx) = xN(y)$$

by Lemma 4.2 and (4.5). Similarly,

$$(y \circ x) \circ y = (\overline{\overline{y}\,\overline{x}})\overline{y} = (xy)\overline{y} = xN(y),$$

proving that N is semisymmetric. Finally, since $N(x) = N(\overline{x})$, we have $N(x \circ y) = N(\overline{x} \cdot \overline{y}) = N(\overline{x})N(\overline{y}) = N(x)N(y)$ by Proposition 4.3. □

PROPOSITION 4.6 ([5, Proposition 5.7]). *Consider $A \in \mathsf{SL}_3(K)$. The induced map $A_{\mathsf{Zorn}(K)}$ of (4.6) is an automorphism of the para-Zorn algebra $\mathsf{PZorn}(K)$.*

4.3 THE SPLIT OKUBO ALGEBRA $\mathsf{Okubo}(K) = (\mathsf{Zorn}(K), *)$

Let K be a commutative unital ring. We will construct the split Okubo algebra $\mathsf{Okubo}(K)$ in two ways: first by defining an explicit multiplication and norm on a canonical basis, and secondly by modification of the Zorn multiplication on $\mathsf{Zorn}(K)$.

4.3.1 THE CANONICAL BASIS

Let $\mathbf{e}_0 = [1\ 0\ 0]$, $\mathbf{e}_1 = [0\ 1\ 0]$, $\mathbf{e}_2 = [0\ 0\ 1]$ be the vectors constituting the standard basis of K^3. Then the Zorn vector-matrices

$$e_\infty = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad e_0 = \begin{bmatrix} 0 & -\mathbf{e}_0 \\ 0 & 0 \end{bmatrix}, \quad e_1 = \begin{bmatrix} 0 & -\mathbf{e}_1 \\ 0 & 0 \end{bmatrix}, \quad e_2 = \begin{bmatrix} 0 & -\mathbf{e}_2 \\ 0 & 0 \end{bmatrix},$$

$$e_{\infty'} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \quad e_{0'} = \begin{bmatrix} 0 & 0 \\ \mathbf{e}_0 & 0 \end{bmatrix}, \quad e_{1'} = \begin{bmatrix} 0 & 0 \\ \mathbf{e}_1 & 0 \end{bmatrix}, \quad e_{2'} = \begin{bmatrix} 0 & 0 \\ \mathbf{e}_2 & 0 \end{bmatrix}$$

are said to constitute the *canonical basis* of $\mathsf{Zorn}(K)$ [5, p.426].
Consider the free K-module K^8 over the 8-element set $\{e_i \mid i \in I\}$ for the index set $I = \{\infty, \infty', 0, 0', 1, 1', 2, 2'\}$. Define a so-called *Okubo algebra* structure

$\mathsf{Okubo}(K) = (K^8, *)$ by the table

$*$	e_∞	$e_{\infty'}$	e_0	$e_{0'}$	e_1	$e_{1'}$	e_2	$e_{2'}$
e_∞	$e_{\infty'}$	0	0	$-e_{2'}$	0	$-e_{0'}$	0	$-e_{1'}$
$e_{\infty'}$	0	e_∞	$-e_2$	0	$-e_0$	0	$-e_1$	0
e_0	$-e_1$	0	$e_{0'}$	0	$-e_{2'}$	0	0	$-e_\infty$
$e_{0'}$	0	$-e_{1'}$	0	e_0	0	$-e_2$	$-e_{\infty'}$	0
e_1	$-e_2$	0	0	$-e_\infty$	$e_{1'}$	0	$-e_{0'}$	0
$e_{1'}$	0	$-e_{2'}$	$-e_{\infty'}$	0	0	e_1	0	$-e_0$
e_2	$-e_0$	0	$-e_{1'}$	0	0	$-e_\infty$	$e_{2'}$	0
$e_{2'}$	0	$-e_{0'}$	0	$-e_1$	$-e_{\infty'}$	0	0	e_2

of basic multiplications. (This is just [9, Table 1], written with a more compact notation for the suffices analogous to the notation of [5, (5.11)], essentially regarding a nonzero vector (a, b) from $\mathsf{GF}(3)^2$ as homogeneous coordinates for a point a/b of the projective line of order 3, and adding a prime if $b = -1$ or $(a, b) = (-1, 0)$. In particular, $\mathsf{Okubo}(\mathbb{Z})$ is the algebra given as $\mathsf{Okubo}_\mathbb{Z}$ in [9].) The construction of $\mathsf{Okubo}(K)$ is the object part of a functor Okubo from the category **CRing** of commutative unital rings to the category **Rnag** of (homomorphisms of) nonassociative nonunital rings, with $\mathsf{Okubo}(\_) = \mathsf{Okubo}(\mathbb{Z}) \otimes_\mathbb{Z} (\_)$.
Consider the bilinear form on $\mathsf{Okubo}(K)$ given by

$$N(x, y) = x_\infty y_{\infty'} + x_0 y_{0'} + x_1 y_{1'} + x_2 y_{2'} \tag{4.9}$$

for $x = \sum_{i\in I} x_i e_i$ and $y = \sum_{i\in I} y_i e_i$. This form is associative, semisymmetric, and K-invariant (cf. [9, (2.8)]). By Theorem 3.3, N permits composition.

4.3.2 Okubo algebras as isotopes of Zorn algebras

Proposition 4.7. *Let K be a commutative unital ring.*

(a) *The product*

$$u * v = u\rho \circ v\rho^2 = \overline{u\rho} \cdot \overline{v\rho^2}, \tag{4.10}$$

on $\mathsf{Zorn}(K)$, namely

$$\begin{bmatrix} \alpha & \mathbf{a} \\ \mathbf{b} & \beta \end{bmatrix} * \begin{bmatrix} \gamma & \mathbf{c} \\ \mathbf{d} & \delta \end{bmatrix} = \begin{bmatrix} \beta\delta + \mathbf{a}\rho \cdot \mathbf{d}\rho^2 & -\beta\mathbf{c}\rho^2 - \gamma\mathbf{a}\rho - \mathbf{b}\rho \times \mathbf{d}\rho^2 \\ -\delta\mathbf{b}\rho - \alpha\mathbf{d}\rho^2 + \mathbf{a}\rho \times \mathbf{c}\rho^2 & \mathbf{b}\rho \cdot \mathbf{c}\rho^2 + \alpha\gamma \end{bmatrix},$$

offers an explicit version of the split Okubo algebra $\mathsf{Okubo}(K)$, with $N(u, v) = u \cdot \overline{v}$ for u, $v \in \mathsf{Zorn}(K)$.

(b) *The mapping ρ is an automorphism of $\mathsf{Okubo}(K)$.*

(c) *The triple $\big(\mathsf{Okubo}(K), K, N\big)$ is norm-supporting.*

(d) *The norm N is semisymmetric, associative, and permits composition.*

Proof. Part (a) is [5, pp.427–8].

(b) By Proposition 4.6, $(x * y)\rho = (x\rho \circ y\rho^2)\rho = x\rho^2 \circ y = x\rho * y\rho$.

(c) The triple $(\mathsf{Okubo}(K), K, N)$ is norm-supporting since $m * n = m \cdot n$ for scalar matrices.

(d) To establish semisymmetry of N in $\mathsf{Okubo}(K)$, recall that ρ is an automorphism of $\mathsf{PZorn}(K)$ by Proposition 4.6, N is semisymmetric in $\mathsf{PZorn}(K)$ by Proposition 4.5, and observe that $N(y) = N(y\rho)$. Then

$$y * (x * y) = y\rho \circ (x\rho \circ y\rho^2)\rho^2 = y\rho \circ (x \circ y\rho) = xN(y\rho) = xN(y),$$
$$(y * x) * y = (y\rho \circ x\rho^2)\rho \circ y\rho^2 = (y\rho^2 \circ x) \circ y\rho^2 = xN(y\rho^2) = xN(y).$$

Associativity $N(x, y * z) = N(x * y, z)$ can be checked directly. The fact that N permits composition is then immediate from Theorem 3.3, or we calculate $N(x * y) = N(x\rho \circ y\rho^2) = N(x\rho)N(y\rho^2) = N(x)N(y)$. □

We conclude this section with two useful formulas for $\mathsf{Okubo}(K)$.

COROLLARY 4.8 ([9, (5.1)]). *The formula*

$$u \cdot v = (I * u) * (v * I) \tag{4.11}$$

holds for u, $v \in \mathsf{Zorn}(K)$.

Proof. Note that

$$I * u = \overline{I\rho} \cdot \overline{u\rho^2} = I \cdot \overline{u\rho^2} = \overline{u\rho^2} \tag{4.12}$$

and

$$v * I = \overline{v\rho} \cdot \overline{I\rho^2} = \overline{v\rho} \cdot I = \overline{v\rho}.$$

Then $(I * u) * (v * I) = \overline{u\rho^2} * \overline{v\rho} = \overline{\overline{u\rho^2}\rho} \cdot \overline{\overline{v\rho}\rho^2} = u \cdot v$ follows. □

COROLLARY 4.9. *The formula*

$$I * (I * u) = u\rho \tag{4.13}$$

holds for $u \in \mathsf{Zorn}(K)$.

Proof. The equation $I * (I * u) = \overline{\overline{u}\rho^2}\rho^2 = (\overline{\overline{u}}\rho^2)\rho^2 = u\rho$ is obtained from (4.12). □

5 QUASIGROUPS OF UNIT NORM ELEMENTS

Throughout this section, let F be a field.

5.1 PAIGE LOOPS $\mathsf{PSL}_{1+3}(F)$

Following Paige [25], let $\mathsf{SL}_{1+3}(F) = SQ(\mathsf{Zorn}(F))$ be the loop of elements of norm 1 in the Zorn algebra $\mathsf{Zorn}(F)$, and let $\mathsf{PSL}_{1+3}(F)$ be the quotient of $\mathsf{SL}_{1+3}(F)$ by the normal subloop $\{\pm I\} = \{I, -I\}$. We call $\mathsf{PSL}_{1+3}(F)$ the *Paige loop* over F.
If the field F has finite order q, then $\mathsf{PSL}_{1+3}(F)$ is also written as $\mathsf{PSL}_{1+3}(q)$. When no confusion is possible, we will identify the elements of $\mathsf{PSL}_{1+3}(F)$ with the elements of $\mathsf{SL}_{1+3}(F)$; that is, we will write $u \in \mathsf{PSL}_{1+3}(F)$ for $u \in \mathsf{SL}_{1+3}(F)$ rather than the formally correct $\pm u = u \cdot \{\pm I\} \in \mathsf{PSL}_{1+3}(F)$.

PROPOSITION 5.1 ([25]). *For each field F, the Paige loop $\mathsf{PSL}_{1+3}(F)$ is simple.*

For a quasigroup Q, consider the *commutant*

$$C(Q) = \{x \in Q \mid xy = yx \text{ for all } y \in Q\}.$$

Note that it is an isomorphism invariant: isomorphic quasigroups have isomorphic commutants. The following result will be needed for the discussion in Section 7.1 of automorphisms of para-Paige quasigroups.

LEMMA 5.2. *The commutant of $\mathsf{PSL}_{1+3}(F)$ is trivial.*

Proof. Let $Q = \mathsf{PSL}_{1+3}(F)$. We certainly have $I \in C(Q)$. For the reverse inclusion, let

$$u = \begin{bmatrix} \alpha & \mathbf{a} \\ \mathbf{b} & \beta \end{bmatrix}, \quad v = \begin{bmatrix} \gamma & \mathbf{c} \\ \mathbf{d} & \delta \end{bmatrix}$$

be elements of $\mathsf{SL}_{1+3}(F)$, and suppose that $u \in C(Q)$. Focusing on the top row, the condition $u \cdot v = v \cdot u$ in $\mathsf{PSL}_{1+3}(F)$ forces

$$\alpha\gamma + \mathbf{a} \cdot \mathbf{d} = \pm(\gamma\alpha + \mathbf{c} \cdot \mathbf{b}),$$
$$\alpha\mathbf{c} + \delta\mathbf{a} - \mathbf{b} \times \mathbf{d} = \pm(\gamma\mathbf{a} + \beta\mathbf{c} - \mathbf{d} \times \mathbf{b}),$$

with a simultaneous choice of the same sign in both conditions.
Suppose first that $\mathbf{a} \neq \mathbf{0}$. Choosing $\mathbf{c} = \mathbf{0}$ (which forces $\gamma\delta = 1$), the first condition becomes $\mathbf{a} \cdot \mathbf{d} \in \{0, -2\alpha\gamma\}$. Choosing further $\mathbf{d}$ so that $\mathbf{a} \cdot \mathbf{d} \neq 0$, we see that the first condition is violated when $\mathrm{char}(F) = 2$. When $\mathrm{char}(F) \neq 2$, we can further choose γ so that $\mathbf{a} \cdot \mathbf{d} \neq -2\alpha\gamma$, again violating the first condition. Thus without loss of generality, we can now assume that $\mathbf{a} = \mathbf{0} = \mathbf{b}$, so $|u| = \alpha\beta = 1$. Then the above conditions reduce to

$$\alpha\gamma = \pm\gamma\alpha, \quad \alpha\mathbf{c} = \pm\beta\mathbf{c},$$

Suppose for a while that $\mathrm{char}(F) \neq 2$. Then any choice of $\gamma \neq 0$ yields $\alpha\gamma \neq -\gamma\alpha$, so the first condition can only be satisfied with a positive sign. We can therefore assume without loss of generality and in any characteristic that the signs are positive in both conditions. Choosing $\mathbf{c} \neq \mathbf{0}$ then forces $\alpha = \beta$, hence $1 = \alpha\beta = \alpha^2$ and $\alpha \in \{\pm 1\}$. □

5.2 PARA-PAIGE QUASIGROUPS $\mathsf{PP}(F)$

DEFINITION 5.3. For a given field F, the isotope of the Paige loop $\big(\mathsf{PSL}_{1+3}(F),\cdot\big)$ induced by $u\circ v=\overline{u}\cdot\overline{v}$ is called the *para-Paige quasigroup* $\mathsf{PP}(F)=(\mathsf{PSL}_{1+3}(F),\circ)$ over F. If F has finite order q, then $\mathsf{PP}(F)$ is also denoted by $\mathsf{PP}(q)$.

PROPOSITION 5.4. *For each field F, the para-Paige quasigroup $\mathsf{PP}(F)$ is simple and semisymmetric.*

Proof. By Proposition 5.1, $\mathsf{PSL}_{1+3}(F)$ is a simple loop. By (4.8), the triple $(^-,^-,1)$ is an isotopy $\mathsf{PSL}_{1+3}(F)\to\mathsf{PP}(F)$. By Theorem 2.3, $\mathsf{PP}(F)$ is a simple quasigroup. By Proposition 4.5, $(\mathsf{PZorn}(F),F,N)$ is semisymmetric and permits composition. By Theorem 3.3(c), the elements of norm 1 in $\mathsf{PZorn}(F)$ form a semisymmetric quasigroup. The quotient $\mathsf{PP}(F)$ is then also semisymmetric. □

LEMMA 5.5. *Consider a field F.*

(a) *Each subloop of $\mathsf{PSL}_{1+3}(F)$ is closed under conjugation.*

(b) *Each subloop of $\mathsf{PSL}_{1+3}(F)$ is a subquasigroup of $\mathsf{PP}(F)$.*

(c) *The multiplication in $\mathsf{PP}(F)$ may be written as*

$$u\circ v=u^{-1}\cdot v^{-1}=(v\cdot u)^{-1} \tag{5.1}$$

with u, $v\in\mathsf{PSL}_{1+3}(F)$ and inverses taken in $\mathsf{PSL}_{1+3}(F)$.

Proof. By Lemma 4.2, $\overline{u}=u^{-1}|u|=u^{-1}$ for every $u\in\mathsf{SL}_{1+3}(F)$. The claims follow. □

5.3 OKUBO QUASIGROUPS $\mathsf{OQ}(F)$

For the Okubo algebra $\mathsf{Okubo}(F)$, consider the semisymmetric quasigroup $SQ(\mathsf{Okubo}(F))$ that is provided by Theorem 3.3.

DEFINITION 5.6. For a given field F, the quotient of $SQ(\mathsf{Okubo}(F))$ by the congruence with classes $\{\{x,-x\}\mid x\in SQ(\mathsf{Okubo}(F))\}$ is called the *Okubo quasigroup* $\mathsf{OQ}(F)$ over F. If F has finite order q then $\mathsf{OQ}(F)$ is also denoted by $\mathsf{OQ}(q)$.

THEOREM 5.7. *Consider a field F.*

(a) *The Okubo quasigroup $\mathsf{OQ}(F)$ is principally isotopic to the Paige loop $\mathsf{PSL}_{1+3}(F)$.*

(b) *The Okubo quasigroup $\mathsf{OQ}(F)$ is simple and semisymmetric.*

(c) *The multiplication in* $\mathsf{OQ}(F)$ *may be written as*

$$u * v = u\rho \circ v\rho^2 = (u\rho)^{-1} \cdot (v\rho^2)^{-1} = u^{-1}\rho \cdot v^{-1}\rho^2$$

with u, $v \in \mathsf{PSL}_{1+3}(F)$ *and inverses taken in* $\mathsf{PSL}_{1+3}(F)$.

Proof. (a) Note that $I \in SQ(\mathsf{Okubo}(F))$. Then for elements u, v of $SQ(\mathsf{Okubo}(F))$, one has

$$u \cdot v = (I * u) * (v * I)$$

by (4.11). Passing to the corresponding $\{\pm I\}$-orbits, there is a principal isotopy

$$\big(L_*(\{\pm I\}), R_*(\{\pm I\}), 1\big) \colon \big(\mathsf{PSL}_{1+3}(F), \cdot, \{\pm I\}\big) \to \big(\mathsf{OQ}(F), *\big)$$

from the Paige loop to the Okubo quasigroup.

(b) The simplicity follows, via the isotopy from (a), by Theorem 2.3. The quasigroup $SQ(\mathsf{Okubo}(F))$ is semisymmetric by Theorem 3.3 and Proposition 4.7. Then the quotient $\mathsf{OQ}(F)$ of the semisymmetric quasigroup $SQ(\mathsf{Okubo}(F))$ is also semisymmetric.

(c) This follows from Proposition 4.7. □

The following result yields the number of Zorn vector matrices of a given norm, as well as the cardinalities of Paige loops, para-Paige quasigroups and Okubo quasigroups over finite fields.

THEOREM 5.8 (compare [25, p.471]). *Let* $F = \mathsf{GF}(q)$ *be the finite field of order* q. *For any* $\lambda \in F$, *let* n_λ *denote the number of elements of norm* λ *in* $\mathsf{Zorn}(F)$. *Then*

$$n_\lambda = \begin{cases} q^7 - q^3, & \text{if } \lambda \neq 0; \\ q^7 + q^4 - q^3, & \text{if } \lambda = 0. \end{cases}$$

In particular,

$$|\mathsf{PSL}_{1+3}(q)| = |\mathsf{PP}(q)| = |\mathsf{OQ}(q)| = \begin{cases} q^7 - q^3, & \text{if } q \text{ is even}; \\ (q^7 - q^3)/2, & \text{if } q \text{ is odd}. \end{cases}$$

Proof. Suppose $0 \neq \lambda \in F$. We will count the elements $z \in \mathsf{Zorn}(F)$ with $N(z) = \lambda$. The top row of z must be nonzero, else $N(z) = 0$. Let i be a position in the bottom row of z that corresponds to a nonzero entry in the top row under the norm calculation. No matter what the values are in the bottom row outside of i, there is a unique choice of the value in i that guarantees $N(z) = \lambda$. Thus $n_\lambda = (q^4 - 1)q^3 = q^7 - q^3$. Then $n_0 = q^8 - (q-1)(q^7 - q^3) = q^7 + q^4 - q^3$. The rest is clear. □

6 Powers, power-associativity and diassociativity

In this section we investigate powers, power-associativity and diassociativity in the three classes of quasigroups just introduced. It turns out that powers are quite intricate in Okubo quasigroups. Section 6.2 presents some previously unknown consequences of the Moufang identities that are required for an understanding of powers in Okubo quasigroups.

6.1 Power-associativity and diassociativity

A universal algebra is said to be *power-associative* if each element generates an associative subalgebra, and *diassociative* if each pair of elements generates an associative subalgebra. Obviously, each diassociative algebra is power-associative. Is it well-known that $\mathsf{Zorn}(F)$ is diassociative, while $\mathsf{PZorn}(F)$ and $\mathsf{Okubo}(F)$ are never power-associative, cf. [6].

A *Moufang quasigroup* is defined as a quasigroup satisfying any one of the Moufang identities. Kunen proved in [17] that a Moufang quasigroup is automatically a loop satisfying all four Moufang identities. By Moufang's Theorem [19], each Moufang loop is diassociative. The Paige loops $\mathsf{PSL}_{1+3}(F)$ in particular, as Moufang loops, are diassociative and power-associative.

From now on, we will adopt the following notational conventions: Since Paige loops are power-associative, the power x^k is well-defined for each $x \in \mathsf{PSL}_{1+3}(F)$ and $k \in \mathbb{Z}$. The quasigroups $\mathsf{PP}(F)$ and $\mathsf{OQ}(F)$ are defined on the same underlying set as $\mathsf{PSL}_{1+3}(F)$. Whenever we use powers of elements of $\mathsf{PP}(F)$ or $\mathsf{OQ}(F)$, we implicitly refer to the powers in $\mathsf{PSL}_{1+3}(F)$.

Lemma 6.1. *Consider the magma $(\mathbb{Z}, \bullet)$ defined by $x \bullet y = -(x+y)$. Then the submagma of $(\mathbb{Z}, \bullet)$ generated by 1 is equal to $3\mathbb{Z}+1$.*

Proof. Suppose that H is the submagma generated by 1. Note that $(3k+1) \bullet (3\ell+1) = -3k-1-3\ell-1 = 3(-(k+\ell+1))+1$, so $H \subseteq 3\mathbb{Z}+1$. Conversely, we have $3(-1)+1 = -2 = 1 \bullet 1 \in H$. The identities $(-2) \bullet (-3k+1) = 3k+1$ and $1 \bullet (3k+1) = -3(k+1)+1$ finish the proof. □

Given a semisymmetric quasigroup $(Q, \cdot, /, \backslash)$ and a subset S of Q, the submagma of $(Q, \cdot)$ generated by S is equal to the subquasigroup of $(Q, \cdot, /, \backslash)$ generated by S: that is, it is not necessary to consider left and right divisions. This is a consequence of Proposition 3.1.

Proposition 6.2. *Let $x \in \mathsf{PP}(F)$. Then the subquasigroup $\langle x \rangle_{\mathsf{PP}(F)}$ of $\mathsf{PP}(F)$ generated by x is equal to $\{x^{3k+1} \mid k \in \mathbb{Z}\}$.*

Proof. We have $x^k \circ x^\ell = x^{-k}x^{-\ell} = x^{-(k+\ell)}$, and the rest follows from Lemma 6.1. □

Lemma 6.3. *The para-Paige quasigroup $\mathsf{PP}(F)$ is power-associative if and only if $x^6 = 1$ holds for every $x \in \mathsf{PP}(F)$.*

Proof. Suppose that $\mathsf{PP}(F)$ is power-associative, and let $x \in \mathsf{PP}(F)$. Since x generates a subgroup of $\mathsf{PP}(F)$, there must be a $y \in \mathsf{PP}(F)$ such that $x \circ y = x$. This is equivalent to $x^{-1} \cdot y^{-1} = x$, i.e., $y = x^{-2}$ by diassociativity of $\mathsf{PSL}_{1+3}(F)$. We must then also have $(x \circ x) \circ x^{-2} = x \circ x$, which is equivalent to $x^{-2} \circ x^{-2} = x^{-2}$, i.e., $x^4 = x^{-2}$, $x^6 = 1$.
Conversely, suppose that the identity $x^6 = 1$ holds in $\mathsf{PSL}_{1+3}(F)$. By Proposition 6.2, the subquasigroup of $\mathsf{PP}(F)$ generated by x is then equal to $\{x^{3k+1} \mid k \in \mathbb{Z}\} = \{x, x^{-2}\}$. But this is a group with identity element x^{-2}. □

PROPOSITION 6.4. *Let F be a field.*

(a) *The quasigroup $\mathsf{PP}(F)$ is power-associative if and only if $|F| \in \{2, 3\}$.*

(b) *The quasigroup $\mathsf{PP}(F)$ is not diassociative. In fact, the right alternative identity $x \circ (y \circ y) = (x \circ y) \circ y$ fails in $\mathsf{PP}(F)$.*

Proof. (a) With

$$y = \begin{bmatrix} 1 & \mathbf{e}_0 \\ 0 & 1 \end{bmatrix} \in \mathsf{PP}(F)$$

we have

$$y \circ (y \circ (y \circ y)) = \begin{bmatrix} 1 & -2\mathbf{e}_0 \\ 0 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 4\mathbf{e}_0 \\ 0 & 1 \end{bmatrix} = (y \circ y) \circ (y \circ y)$$

if $\mathrm{char}(F) \notin \{2, 3\}$, so that $\mathsf{PP}(F)$ is not power-associative in that case. Suppose from now on that $\mathrm{char}(F) \in \{2, 3\}$.
By Lemma 6.3, $\mathsf{PP}(F)$ is power-associative if and only if the identity $x^3 = x^{-3} = \overline{x^3}$ holds. Given a generic element

$$x = \begin{bmatrix} a & (b, c, d) \\ (e, f, g) & h \end{bmatrix}$$

of $\mathsf{PP}(F)$, a calculation using the constraint $ah - be - cf - dg = 1$ shows that

$$x^3 = \begin{bmatrix} a^3 + (2a + h)(ah - 1) & ((a + h)^2 - 1)(b, c, d) \\ ((a + h)^2 - 1)(e, f, g) & h^3 + (2h + a)(ah - 1) \end{bmatrix}.$$

No matter what a, h are, we can certainly choose $b \neq 0$ and $e \neq 0$. Consider the three conditions

$$a^3 + (2a + h)(ah - 1) = h^3 + (2h + a)(ah - 1), \tag{6.1}$$

$$(a + h)^2 - 1 = -((a + h)^2 - 1), \tag{6.2}$$

$$a^3 + (2a + h)(ah - 1) = -h^3 - (2h + a)(ah - 1). \tag{6.3}$$

Conditions (6.1), (6.2) correspond to the equality $x^3 = \overline{x^3}$ for matrices, while condition (6.3) corresponds to the equality $x^3 = -\overline{x^3}$ for matrices. Thus $\mathsf{PP}(F)$

is power-associative if and only if, for every a, h, either both (6.1) and (6.2) hold, or (6.3) holds.
Suppose first that $\mathrm{char}(F) = 2$. Then (6.3) coincides with (6.1), and (6.2) is vacuous. It is easy to see that (6.1) is equivalent to $(a+h)^3 = a+h$. Since we can choose $a+h$ arbitrarily, we deduce that $\mathsf{PP}(F)$ is power-associative if and only if $|F| = 2$.
Now suppose that $\mathrm{char}(F) = 3$. Condition (6.2) is then equivalent to $a+h = \pm 1$, while condition (6.1) holds for both $a+h = 1$ and $a+h = -1$. Finally, (6.3) can be rewritten as $(a+h)^3 = 0$; that is, $a+h = 0$. If $|F| = 3$ then every choice of a, h yields $a+h \in \{0, 1, -1\}$ and thus $\mathsf{PP}(F)$ is power-associative. If $|F| \neq 3$ then we can choose a, h so that $a+h \notin \{0, 1, -1\}$ and thus $\mathsf{PP}(F)$ is not power-associative.

(b) We have $(x \circ I) \circ I = x^{-1} \circ I = x$, while $x \circ (I \circ I) = x \circ I = x^{-1}$. Any $x \in \mathsf{PP}(F)$ with $x \neq x^{-1}$ then demonstrates that the identity $x \circ (y \circ y) = (x \circ y) \circ y$ fails in $\mathsf{PP}(F)$. □

PROPOSITION 6.5. *If F is a field, $\mathsf{OQ}(F)$ is not power-associative. In fact, the identity $x * (x * (x * x)) = (x * x) * (x * x)$ fails in $\mathsf{OQ}(F)$.*

Proof. We have

$$\begin{aligned} y * (y * (y * y)) &= \begin{bmatrix} 1 & -(0,1,1) \\ (1,0,0) & 1 \end{bmatrix} \\ &\neq \begin{bmatrix} 0 & (1,1,1) \\ -(1,0,0) & 0 \end{bmatrix} = (y * y) * (y * y) \end{aligned}$$

with y as in the proof of Proposition 6.4. □

6.2 SOME CONSEQUENCES OF THE MOUFANG IDENTITIES

In this subsection we derive consequences of Moufang identities that were not previously known. The identities obtained should be useful in the study of the free Moufang loop on three generators, a very complicated object.

PROPOSITION 6.6. *The following identities hold in Moufang loops for every $n \geq 0$:*

$$(xy \cdot z)^n \cdot xy = (x \cdot yz)^n x \cdot y, \tag{φ_n}$$
$$(xy \cdot z)^n \cdot xy = x \cdot (y \cdot zx)^n y. \tag{ψ_n}$$

Proof. We prove the two sets of identities simultaneously by induction on n. Both (φ_0), (ψ_0) reduce to $xy = xy$. Substituting xy for u in the valid identity $uzu = ((uz)u)y^{-1} \cdot y = u(z(uy^{-1})) \cdot y$ yields

$$xy \cdot z \cdot xy = (xy)(z(xy \cdot y^{-1})) \cdot y = (xy)(zx) \cdot y = x(yz)x \cdot y,$$

which is (φ_1), and then

$$xy \cdot z \cdot xy = (xy)(zx) \cdot y = x(y \cdot (zx)y) = x \cdot y(zx)y,$$

which is (ψ_1).
Suppose that $n \geq 1$ and (φ_i), (ψ_i) hold for every $i \leq n$. We will establish (φ_{n+1}) and (ψ_{n+1}). The left hand side of (φ_{n+1}) is equal to

$$(xy \cdot z)^{n+1} \cdot xy = xy \cdot (z \cdot xy)^n z \cdot xy = x(y \cdot (z \cdot xy)^n z)x \cdot y,$$

where we have used (φ_1) in the last step. The right hand side of (φ_{n+1}) is equal to

$$(x \cdot yz)^{n+1} x \cdot y = x((yz \cdot x)^n \cdot yz)x \cdot y$$

by diassociativity. Upon canceling y on the right and then x on both sides, we see that (φ_{n+1}) holds if and only if

$$y \cdot (z \cdot xy)^n z = (yz \cdot x)^n \cdot yz,$$

which is (ψ_n).
Similarly, the left hand side of (ψ_{n+1}) is equal to

$$(xy \cdot z)^{n+1} \cdot xy = xy \cdot (z \cdot xy)^n z \cdot xy = x(y \cdot ((z \cdot xy)^n z)x \cdot y),$$

where we have used (ψ_1) in the last step. The right hand side of (ψ_{n+1}) is equal to

$$x \cdot (y \cdot zx)^{n+1} y = x(y \cdot (zx \cdot y)^n \cdot zx \cdot y)$$

by diassociativity. Upon canceling, we see that (ψ_{n+1}) holds if and only

$$(z \cdot xy)^n z \cdot x = (zx \cdot y)^n \cdot zx,$$

which is (φ_n). □

COROLLARY 6.7. *The following identity holds in Moufang loops for every $n \geq 0$:*

$$\begin{aligned}(xy \cdot z)^n \cdot xy &= (x \cdot yz)^n x \cdot y = x \cdot (y \cdot zx)^n y \\ &= xy \cdot (z \cdot xy)^n = x(yz \cdot x)^n \cdot y = x \cdot y(zx \cdot y)^n.\end{aligned}$$

Proof. The first three products coincide by (φ_n) and (ψ_n). The rest follows by diassociativity: the first product is equal to the fourth, the second is equal to the fifth, and the third is equal to the sixth. □

PROPOSITION 6.8. *The following identities hold in Moufang loops for every m, $n \geq 0$:*

$$(x \cdot yz)^m x \cdot (y \cdot zx)^n y = (xy \cdot z)^{m+n} \cdot xy, \qquad (\alpha_{m,n})$$

$$(xy \cdot z)^m (xy) \cdot (zx \cdot y)^n (zx) = (x \cdot yz)^{m+n+1} x. \qquad (\beta_{m,n})$$

Proof. We prove the identities by induction on m. The identity $(\alpha_{0,n})$ is covered by Corollary 6.7. The identity $(\beta_{0,n})$ is

$$(xy)\cdot(zx\cdot y)^n(zx) = (x\cdot yz)^{n+1}x.$$

The left hand side can be written as $(xy)((z\cdot xy)^n z\cdot x)$ by Corollary 6.7 and then as $x(y\cdot(z\cdot xy)^n z)x$ by a Moufang identity. Cancelling x on the left and on the right of both sides yields $y\cdot(z\cdot xy)^n z = yz\cdot(x\cdot yz)^n$, which holds by Corollary 6.7.
Suppose that $m>0$ and both $(\alpha_{m-1,n})$, $(\beta_{m-1,n})$ hold. We can rewrite the left hand side of $(\alpha_{m,n})$ as

$$\begin{aligned}&(x\cdot(yz)(x\cdot yz)^{m-1}\cdot x)\cdot(y\cdot zx)^n y\\ &= x[(yz)(x\cdot yz)^{m-1}\cdot(x\cdot(y\cdot zx)^n y)]\\ &= x[(yz)(x\cdot yz)^{m-1}\cdot(xy\cdot z)^n(xy)]\\ &= x[(yz\cdot x)^{m-1}(yz)\cdot(xy\cdot z)^n(xy)],\end{aligned}$$

while the right hand side is $x\cdot(y\cdot zx)^{m+n}y$. Upon canceling x on the left, we obtain

$$(yz\cdot x)^{m-1}(yz)\cdot(xy\cdot z)^n(xy) = (y\cdot zx)^{m+n}y,$$

which is $(\beta_{m-1,n})$.
The left hand side of $(\beta_{m,n})$ is equal to

$$\begin{aligned}&(xy)(z\cdot xy)^m\cdot(zx\cdot y)^n(zx)\\ &= (xy)(z\cdot xy)^m\cdot((z\cdot xy)^n z\cdot x)\\ &= (x\cdot y(zx\cdot y)^m)\cdot((z\cdot xy)^n z\cdot x)\\ &= x[y(zx\cdot y)^m\cdot(z\cdot xy)^n z]x.\end{aligned}$$

Upon canceling x of both sides, $(\beta_{m,n})$ becomes

$$y(zx\cdot y)^m\cdot(z\cdot xy)^n z = (yz\cdot x)^{m+n}\cdot yz,$$

which is $(\alpha_{m,n})$. □

6.3 Powers in Okubo quasigroups

We have seen that Okubo quasigroups are not power-associative. Now, in this section, we describe powers and mono-generated subquasigroups in Okubo quasigroups.
For any automorphism α of $\mathsf{PSL}_{1+3}(F)$ and any $x\in\mathsf{PSL}_{1+3}(F)$, let us write $x^\alpha = x\alpha$ and $x^{-\alpha} = (x^{-1})^\alpha = (x^\alpha)^{-1}$. With this notational convention, the multiplication in the Okubo quasigroup can be written as $x*y = x^{-\rho}y^{-\rho^2}$.

LEMMA 6.9. *Let F be a field and $x\in\mathsf{OQ}(F)$. Let*

$$a = x,\quad b = x^\rho,\quad c = x^{\rho^2}.$$

For every $n \geq 0$, define the elements w_{3n+1}, $w_{3n+2} \in \mathsf{PSL}_{1+3}(F)$ by

$$\begin{aligned} w_{3n+1} &= a(cb \cdot a)^n, \\ w_{3n+2} &= (b^{-1}c^{-1})(a^{-1} \cdot b^{-1}c^{-1})^n. \end{aligned}$$

Then:

$$\begin{aligned} w_{3m+1} * w_{3n+1} &= w_{3(m+n)+2}, \\ w_{3m+2} * w_{3n+2} &= w_{3(m+n+1)+1}, \\ w_{3m+1} * w_{3n+2} &= \begin{cases} w_{3(n-m)+1}, & \text{if } n \geq m, \\ w_{3(m-n-1)+2}, & \text{if } n < m, \end{cases} \\ w_{3m+2} * w_{3n+1} &= \begin{cases} w_{3(m-n)+1}, & \text{if } m \geq n, \\ w_{3(n-m-1)+2}, & \text{if } m < n. \end{cases} \end{aligned}$$

Proof. We have

$$\begin{aligned} &w_{3m+1} * w_{3n+1} = [a(cb \cdot a)^m] * [a(cb \cdot a)^n] = [a(cb \cdot a)^m]^{-\rho} \cdot [a(cb \cdot a)^n]^{-\rho^2} \\ &= [b(ac \cdot b)^m]^{-1} \cdot [c(ba \cdot c)^n]^{-1} = (b^{-1} \cdot c^{-1}a^{-1})^m b^{-1} \cdot (c^{-1} \cdot a^{-1}b^{-1})^n c^{-1} \\ &= (b^{-1}c^{-1} \cdot a^{-1})^{m+n} \cdot b^{-1}c^{-1} = w_{3(m+n)+2}, \end{aligned}$$

where we have used the identity $(\alpha_{m,n})$ for the penultimate equality. Similarly,

$$\begin{aligned} &w_{3m+2} * w_{3n+2} = [(b^{-1}c^{-1})(a^{-1} \cdot b^{-1}c^{-1})^m] * [(b^{-1}c^{-1})(a^{-1} \cdot b^{-1}c^{-1})^n] \\ &= (ac \cdot b)^m (ac) \cdot (ba \cdot c)^n (ba) = (a \cdot cb)^{m+n+1} a = w_{3(m+n+1)+1}, \end{aligned}$$

where we have used $(\beta_{m,n})$ in the penultimate step.
For the remaining cases, we will need some easy consequences of the identities $(\alpha_{m,n})$, $(\beta_{m,n})$. We have

$$\begin{aligned} w_{3m+1} * w_{3n+2} &= [a(cb \cdot a)^m] * [(b^{-1}c^{-1})(a^{-1} \cdot b^{-1}c^{-1})^n] \\ &= (b^{-1} \cdot c^{-1}a^{-1})^m b^{-1} \cdot (ba \cdot c)^n (ba)\,. \end{aligned}$$

Dividing on the left by $(x \cdot yz)^m x$ in $(\alpha_{m,n})$ yields

$$x^{-1}(z^{-1}y^{-1} \cdot x^{-1})^m \cdot (xy \cdot z)^{m+n}(xy) = (y \cdot zx)^n y$$

for every m, $n \geq 0$. If $n \geq m$, we deduce the identity

$$x^{-1}(z^{-1}y^{-1} \cdot x^{-1})^m \cdot (xy \cdot z)^n (xy) = (y \cdot zx)^{m-n} y\,,$$

and therefore $w_{3m+1} * w_{3n+2} = w_{3(n-m)+1}$. Dividing on the right by $(zx \cdot y)^n (zx)$ in $(\beta_{m,n})$ and reindexing yields the identity

$$(x \cdot yz)^m x \cdot (x^{-1}z^{-1})(y^{-1} \cdot x^{-1}z^{-1})^n = (xy \cdot z)^{m-n-1}(xy)$$

as long as $n < m$. Hence $w_{3m+1} * w_{3n+2} = w_{3(m-n-1)+2}$ in that case.

The case $w_{3m+2} * w_{3n+1}$ is similar. In detail,

$$\begin{aligned} w_{3m+2} * w_{3n+1} &= [(b^{-1}c^{-1})(a^{-1} \cdot b^{-1}c^{-1})^m] * [a(cb \cdot a)^n] \\ &= (ac \cdot b)^m(ac) \cdot (c^{-1} \cdot a^{-1}b^{-1})^n c^{-1}. \end{aligned}$$

Dividing by $(y \cdot zx)^n y$ on the right in $(\alpha_{m,n})$ and reindexing yields

$$(xy \cdot z)^m(xy) \cdot y^{-1}(x^{-1}z^{-1} \cdot y^{-1})^n = (x \cdot yz)^{m-n}x$$

as long as $m \geq n$, in which case we deduce $w_{3m+2} * w_{3n+1} = w_{3(m-n)+1}$. Finally, dividing on the left by $(xy \cdot z)^m(xy)$ in $(\beta_{m,n})$ and reindexing yields

$$(zx \cdot y)^{n-m-1}(zx) = (y^{-1}x^{-1})(z^{-1} \cdot y^{-1}x^{-1})^m \cdot (x \cdot yz)^n x$$

as long as $m < n$, and hence $w_{3m+2} * w_{3n+1} = w_{3(n-m-1)+2}$ in that case. □

PROPOSITION 6.10. *Let $x \in \mathsf{OQ}(F)$. Then the subquasigroup $\langle x \rangle_{\mathsf{OQ}(F)}$ of $\mathsf{OQ}(F)$ generated by x is equal to*

$$\big\{x(x^{\rho^2}x^{\rho} \cdot x)^n,\ (x^{-\rho}x^{-\rho^2})(x^{\rho^2}x^{\rho} \cdot x)^{-n} \,\big|\, n \geq 0\big\}.$$

In particular, the inequality

$$\big|\langle x \rangle_{\mathsf{OQ}(F)}\big| \leq 2\big|\langle x^{\rho^2}x^{\rho} \cdot x \rangle_{\mathsf{PSL}_{1+3}(F)}\big|$$

holds when F is finite.

Proof. We recognize $x(x^{\rho^2}x^{\rho} \cdot x)^n$ as w_{3n+1} and $(x^{-\rho}x^{-\rho^2})(x^{\rho^2}x^{\rho} \cdot x)^{-n}$ as w_{3n+2} from Lemma 6.9.

We claim that any nonempty word w in $(\mathsf{OQ}(F), *)$ on the single generator x is of the form w_{3n+1} or w_{3n+2} for some $n \geq 0$. We prove this by induction on the number $k > 0$ of occurrences of x in w. If $k = 1$, we have $w = x = w_1$. If $k > 1$ and $w = u * v$ for some shorter words u, v, then we are done by the induction assumption and Lemma 6.9.

Moreover, we claim that every product w_{3n+1}, w_{3n+2} with $n \geq 0$ actually appears in $S = \langle x \rangle_{\mathsf{OQ}(F)}$. Indeed, we have $w_1 = x \in S$, $w_{3n+2} = w_1 * w_{3n+1}$, and $w_{3(n+1)+1} = w_2 * w_{3n+2}$ by Lemma 6.9. □

7 AUTOMORPHISMS

We discuss the automorphism groups of Paige loops and para-Paige quasigroups over perfect fields. For Paige loops, this was already done in [21], relating automorphism groups of Paige loops to the groups $\mathsf{G}_2(F)$ of Lie type. While we do not know the automorphism groups of Okubo quasigroups in general (compare Problem 13.2), we do describe a computational determination of $\mathrm{Aut}(\mathsf{OQ}(2))$.

7.1 AUTOMORPHISM GROUPS

We begin by recalling an explicit result about the automorphism groups of certain Paige loops.

THEOREM 7.1 ([21, Theorem 2.3]). *If F is a perfect field, the automorphism group of $\mathsf{PSL}_{1+3}(F)$ is the semidirect product $\mathsf{G}_2(F) \rtimes \mathrm{Aut}(F)$.*

7.1.1 AUTOMORPHISM GROUPS OF PARA-PAIGE QUASIGROUPS

We now show that, for any field F, the automorphism group of the para-Paige quasigroup $\mathsf{PP}(F)$ actually coincides with the automorphism group of the corresponding Paige loop $\mathsf{PSL}_{1+3}(F)$.

LEMMA 7.2. *The element I is fixed by every automorphism of $\mathsf{PP}(F)$.*

Proof. Recall the notation $C(Q)$ for the commutant of a quasigroup Q. Note that $x \in C(\mathsf{PP}(F))$ if and only if $x^{-1} \in C(\mathsf{PSL}_{1+3}(F))$. But $C(\mathsf{PSL}_{1+3}(F)) = \{I\}$ by Lemma 5.2. Hence $C(\mathsf{PP}(F)) = \{I\}$ and I is fixed by every automorphism of $\mathsf{PP}(F)$. □

PROPOSITION 7.3. *Consider a field F.*

(a) *In all cases,* $\mathrm{Aut}(\mathsf{PSL}_{1+3}(F)) = \mathrm{Aut}(\mathsf{PP}(F))$.

(b) *If F is perfect, then the automorphism group* $\mathrm{Aut}(\mathsf{PP}(F))$ *is the semidirect product* $\mathsf{G}_2(F) \rtimes \mathrm{Aut}(F)$.

Proof. (a) Consider a bijection f of the underlying set of $\mathsf{PP}(F)$. In the chain

$$f(u) \circ f(v) = (f(v) \cdot f(u))^{-1} \overset{\text{(i)}}{=} (f(v \cdot u))^{-1} \overset{\text{(ii)}}{=} f((v \cdot u)^{-1}) = f(u \circ v)\,,$$

the undecorated equalities always hold. When f is an automorphism of $\mathsf{PSL}_{1+3}(F)$, the equalities labeled (i) and (ii) do hold, and therefore f is an automorphism of $\mathsf{PP}(F)$. Conversely, suppose that f is an automorphism of $\mathsf{PP}(F)$. Then $f(w)^{-1} \cdot f(w^{-1})^{-1} = f(w) \circ f(w^{-1}) = f(w \circ w^{-1}) = f(w^{-1} \cdot w) = f(I) = I$ by Lemma 7.2, and so $f(w^{-1}) = f(w)^{-1}$. Equality (ii) follows. Since $f(u) \circ f(v) = f(u \circ v)$, we deduce that (i) holds; that is, f is an automorphism of $\mathsf{PSL}_{1+3}(F)$.

Statement (b) now follows from (a) and Theorem 7.1. □

7.1.2 AUTOMORPHISM GROUPS OF OKUBO ALGEBRAS

THEOREM 7.4. *Suppose that F is a field, of characteristic prime to 3, that contains a primitive cube root ω of 1. Then* $\mathrm{Aut}\big(\mathsf{Okubo}(F)\big)$ *is* $\mathsf{PGL}_3(F)$.

Proof. Consider the special Lie algebra $\mathfrak{sl}_3(F)$ of traceless elements of the matrix algebra F_3^3. Define a product $*$ on the 8-dimensional vector space $\mathfrak{sl}_3(F)$ by

$$x * y = \omega xy - \omega^2 yx - (\omega - \omega^2)\mathrm{tr}(xy)3^{-1} \tag{7.1}$$

(compare (2.1) of [9]). Then the Okubo algebra $\mathsf{Okubo}(F)$ is isomorphic to the algebra $\big(\mathfrak{sl}_3(F), *\big)$, with bilinear form

$$N(x, y) = -\mathrm{tr}(xy)$$

corresponding to (4.9) [9, pp.2–7]. Now consider the restriction map

$$\mathrm{res}\colon \mathsf{PGL}_3(F) = \mathrm{Aut}(F_3^3) \to \mathrm{Aut}\big(\mathfrak{sl}_3(F), *\big) \tag{7.2}$$

with two-sided inverse extending automorphisms of $\mathfrak{sl}_3(F)$ by fixing the identity matrix. Then (7.2) is an isomorphism (cf. [9, Theorem 12]). □

7.2 Induced multiplicative automorphisms

Let F be a field. Let $\bullet$ be one of the three multiplication operations $\cdot$, $\circ$, $*$ on $\mathsf{Zorn}(F)$, giving rise to

(a) the Zorn algebra $(\mathsf{Zorn}(F), \cdot)$ of §4.1,

(b) the para-Zorn algebra $\mathsf{PZorn}(F) = (\mathsf{Zorn}(F), \circ)$ of §4.2, and

(c) the Okubo algebra $\mathsf{Okubo}(F) = (\mathsf{Zorn}(F), *)$ of §4.3,

respectively. Then $(\mathsf{PSL}_{1+3}(F), \bullet)$ is either the Paige loop $\mathsf{PSL}_{1+3}(F)$, the para-Paige quasigroup $\mathsf{PP}(F)$ or the Okubo quasigroup $\mathsf{OQ}(F)$. We will show that for each of the operations $\bullet \in \{\cdot, \circ, *\}$, a (linear) automorphism φ of $(\mathsf{Zorn}(F), +, \bullet)$ induces a (multiplicative) automorphism φ' of $(\mathsf{PSL}_{1+3}(F), \bullet)$. Moreover, the assignment $\varphi \mapsto \varphi'$ is injective.
Note that if F is a field then the multiplication $\bullet \in \{\cdot, \circ, *\}$ is linear in $(\mathsf{Zorn}(F), +, \bullet)$.

Lemma 7.5. *Let F be a field, $\bullet \in \{\cdot, \circ, *\}$ and $A(F) = (\mathsf{Zorn}(F), +, \bullet)$. For $\varphi \in \mathrm{Aut}(A(F))$, let φ' be the restriction of φ to the quasigroup $SQ(A(F))$ of elements of norm 1. Then $\varphi' \in \mathrm{Aut}(SQ(A(F)), \bullet)$. Moreover, the assignment $\varphi \mapsto \varphi'$ is injective.*

Proof. Let $\varphi \in \mathrm{Aut}(A)$. Since $SQ(A(F))$ is closed under the multiplication $\bullet$, and $\varphi(u \bullet v) = \varphi(u) \bullet \varphi(v)$ for all $u, v \in \mathsf{Zorn}(F)$, it follows that $\varphi' \in \mathrm{Aut}(SQ(A(F)), \bullet)$. The linear automorphism φ is determined by its values on the canonical basis $\{e_i, e_{i'} \mid i \in \{\infty, 0, 1, 2\}\}$ of $\mathsf{Zorn}(F)$. The canonical basis consists of vectors of norm 0, but each basis vector can be written as a difference of two vectors of norm 1. Indeed,

$$e_i = \begin{cases} (e_i + e_\infty + e_{\infty'}) - (e_\infty + e_{\infty'}), & \text{if } i \in \{0, 0', 1, 1', 2, 2'\}, \\ (e_i + e_0 + e_0') - (e_0 + e_{0'}), & \text{if } i \in \{\infty, \infty'\}. \end{cases}$$

Therefore φ is determined by its values on $SQ(A(F))$: the assignment $\varphi \mapsto \varphi'$ is injective. □

Corollary 7.6. *Suppose that F is a field, $\bullet \in \{\cdot, \circ, *\}$, and $A(F) = (\mathsf{Zorn}(F), +, \bullet)$. Then the group $\mathrm{Aut}(A(F))$ of linear automorphisms of the algebra $A(F)$ embeds into the group $\mathrm{Aut}(SQ(A(F)), \bullet)$ of automorphisms of the quasigroup $SQ(A(F))$ of norm 1 elements of $\mathsf{Zorn}(F)$.*

Lemma 7.7. *Let F be a field, $\bullet \in \{\cdot, \circ, *\}$, and $A(F) = (\mathsf{Zorn}(F), +, \bullet)$. Suppose that φ, $\psi \in \mathrm{Aut}(A(F))$ are such that $\varphi(d) \in \{\psi(d), -\psi(d)\}$ for every $d \in SQ(A(F))$. Then $\varphi = \psi$.*

Proof. If F has characteristic 2 then φ and ψ coincide on $SQ(A(F))$ and therefore $\varphi = \psi$ by Lemma 7.5. For the rest of the proof, suppose that $\mathrm{char}(F) \neq 2$. For $\varepsilon \in \{+, -\}$ consider the subspace $V^\varepsilon = \{d \in A(F) \mid \varphi(d) = \varepsilon\psi(d)\}$ and note that $SQ(A(F)) \subseteq V^+ \cup V^-$ by the assumption. We will say that two elements have the *same parity* if they both belong to V^+ or if they both belong to V^-.
Consider the elements $u = e_\infty + e_{\infty'}$, $v = e_0 + u$, $w = e_{0'} + u$, $z = e_0 + e_{0'}$ of $SQ(A(F))$, and note that $z = v + w - 2u$, whence $\psi(z) = \psi(v) + \psi(w) - 2\psi(u)$. We will show that u and v have the same parity. Suppose for a while that $u \in V^+$ and $v \in V^-$. Then $\psi(z) = -\varphi(v) + \psi(w) - 2\varphi(u)$. If $z \in V^+$ we deduce $\varphi(z) = -\varphi(v) \pm \varphi(w) - 2\varphi(u) = \varphi(-v \pm w - 2u)$, so that $z = -v \pm w - 2u$. This is a contradiction, since the coefficient of e_0 is 1 on the left hand side and -1 on the right hand side. If $z \in V^-$ then $w \in V^+$ leads to $-z = -v + w - 2u$, a contradiction (compare $e_{0'}$), while $w \in V^-$ leads to $-z = -v - w - 2u = -z - 4u$, $0 = 4u$, a contradiction. A similar argument shows that $u \in V^-$ and $v \in V^+$ is impossible.
Hence u and $e_0 + u$ have the same parity. Similarly, for every $i \in \{0, 0', 1, 1', 2, 2'\}$, u and $e_i + u$ have the same parity. Finally, with $v' = e_\infty + z$, $w' = e_{\infty'} + z \in SQ(A(F))$ we have $u = v' + w' - 2z$ and it can once again be shown that z, $e_\infty + z$ and $e_{\infty'} + z$ have the same parity.
Suppose now that $u = e_\infty + e_{\infty'} \in V^\varepsilon$. Then for every $i \in \{0, 0', 1, 1', 2, 2'\}$, $e_i + u \in V^\varepsilon$ and therefore $e_i = e_i + u - u \in V^\varepsilon$. Then $z \in V^\varepsilon$ and thus e_∞, $e_{\infty'} \in V^\varepsilon$. Altogether, $\mathsf{Zorn}(F) = V^\varepsilon$. If $\varepsilon = 1$, we are done. If $\varepsilon = -1$ then the linear automorphism $\tau = \varphi^{-1}\psi$ satisfies $\tau(u) = -u$ for all $u \in \mathsf{Zorn}(F)$. But then $-I = \tau(I) = \tau(I \bullet I) = \tau(I) \bullet \tau(I) = (-I) \bullet (-I) = I \bullet I = I$ by linearity, a contradiction. □

Proposition 7.8. *Suppose that F is a field, $\bullet \in \{\cdot, \circ, *\}$, and $A(F) = (\mathsf{Zorn}(F), +, \bullet)$. For $\varphi \in \mathrm{Aut}(A(F))$, a map*

$$\varphi' : \mathsf{PSL}_{1+3}(F) \to \mathsf{PSL}_{1+3}(F)$$

is well-defined by $\varphi'(\pm u) = \pm\varphi(u)$. Then $\varphi' \in \mathrm{Aut}(\mathsf{PSL}_{1+3}(F), \bullet)$. Moreover, the assignment $\varphi \mapsto \varphi'$ is injective.

Proof. Let $\varphi \in \mathrm{Aut}(A(F))$. For $u \in \mathsf{Zorn}(F)$ we have $\varphi(-u) = -\varphi(u)$, so φ' is well-defined. Then

$$\begin{aligned}\varphi'((\pm u) \bullet (\pm v)) &= \varphi'(\pm(u \bullet v)) = \pm\varphi(u \bullet v) = \pm(\varphi(u) \bullet \varphi(v)) \\ &= (\pm\varphi(u)) \bullet (\pm\varphi(v)) = \varphi'(\pm u) \bullet \varphi'(\pm v)\end{aligned}$$

by linearity. Clearly, φ' is surjective. If $\varphi'(\pm u) = \varphi'(\pm v)$, then $\pm\varphi(u) = \pm\varphi(v)$ and thus $\pm u = \pm v$, proving that φ' is injective. If $\varphi, \psi \in \mathrm{Aut}(A(F))$ and $\varphi' = \psi'$ then for every $u \in SQ(A(F))$ we have $\varphi(u) \in \{\psi(u), -\psi(u)\}$. By Lemma 7.7, $\varphi = \psi$. □

COROLLARY 7.9. *Suppose that F is a field, $\bullet \in \{\cdot, \circ, *\}$ and $A(F) = (\mathsf{Zorn}(F), +, \bullet)$. Then the group $\mathrm{Aut}(A(F))$ of linear automorphisms of the algebra $A(F)$ embeds into the group $\mathrm{Aut}(\mathsf{PSL}_{1+3}(F), \bullet)$ of multiplicative automorphisms of the quasigroup $SQ(A(F))$ of unit norm elements of $\mathsf{Zorn}(F)$ modulo the normal subgroup $\{\pm I\}$.*

7.3 THE AUTOMORPHISM GROUPS OF $\mathsf{OQ}(2)$ AND $\mathsf{Okubo}(2)$

In this subsection we will computationally determine the groups $\mathrm{Aut}(\mathsf{OQ}(2))$ and $\mathrm{Aut}(\mathsf{Okubo}(2))$.

PROPOSITION 7.10. *The group $\mathrm{Aut}(\mathsf{OQ}(2))$ is of order 216 and has structure $(C_3 \times C_3) : \mathsf{SL}_2(3)$.*

Proof. We constructed the quasigroup $\mathsf{OQ}(2)$ in `GAP` [11] and calculated $\mathrm{Aut}(\mathsf{OQ}(2))$ using the `LOOPS` package [20]. The structure description of $\mathrm{Aut}(\mathsf{OQ}(2))$ was also obtained in `GAP`. □

REMARK 7.11. The group $\mathrm{Aut}(\mathsf{PSL}_{1+3}(2))$ is isomorphic to $\mathsf{G}_2(2)$ and has order $12096 = 56 \cdot 216$. We checked that $\mathrm{Aut}(\mathsf{OQ}(2))$ is *not* isomorphic to a subgroup of index 56 in $\mathrm{Aut}(\mathsf{PSL}_{1+3}(2))$.

By Corollary 7.6, if φ is a linear automorphism of $(\mathsf{Zorn}(F), +, \bullet)$ then the restriction φ' of φ onto $(SQ(\mathsf{Zorn}(F)), \bullet)$ is a multiplicative automorphism and the mapping $\varphi \to \varphi'$ is one-to-one. We now consider the converse problem.

LEMMA 7.12. *Suppose that F is a field, $\bullet \in \{\cdot, \circ, *\}$, and let $f \in \mathrm{Aut}(SQ(\mathsf{Zorn}(F)), \bullet)$. Define $\widehat{f} : \mathsf{Zorn}(F) \to \mathsf{Zorn}(F)$ by setting*

$$\widehat{f}(e_i) = \begin{cases} f(e_i + e_\infty + e_{\infty'}) - f(e_\infty + e_{\infty'}), & \text{if } i \in \{0, 0', 1, 1', 2, 2'\}, \\ f(e_i + e_0 + e_{0'}) - f(e_0 + e_{0'}), & \text{if } i \in \{\infty, \infty'\} \end{cases}$$

on the canonical basis of $\mathsf{Zorn}(F)$ and extending it linearly. Then $\widehat{f}$ is an additive homomorphism of $(\mathsf{Zorn}(F), +)$. Moreover:

(a) *$\widehat{f}$ is the unique candidate for an extension of f into a linear automorphism of $(\mathsf{Zorn}(F), +, \bullet)$,*

(b) *$\widehat{f}$ extends f into a linear automorphism of $(\mathsf{Zorn}(F), +, \bullet)$ if and only if $\widehat{f}$ is a bijection of $\mathsf{Zorn}(F)$, $\widehat{f}(u \bullet v) = \widehat{f}(u) \bullet \widehat{f}(v)$ for every u, $v \in \mathsf{Zorn}(F)$, and the restriction of $\widehat{f}$ to $SQ(\mathsf{Zorn}(F))$ coincides with f.*

Proof. All the vectors used in the definition of $\widehat{f}$ on the canonical basis of $\mathsf{Zorn}(F)$ are of norm 1. The rest is clear. □

PROPOSITION 7.13. *Every multiplicative automorphism of $\mathsf{OQ}(2) = SQ(\mathsf{Okubo}(2))$ extends into a linear automorphism of $\mathsf{Okubo}(2)$. In particular,* $\mathrm{Aut}(\mathsf{Okubo}(2))$ *is isomorphic to* $\mathrm{Aut}(\mathsf{OQ}(2))$.

Proof. Given $f \in \mathrm{Aut}(\mathsf{OQ}(2))$, we have constructed

$$\widehat{f} : \mathsf{Zorn}(2) \to \mathsf{Zorn}(2)$$

as in Lemma 7.12 and checked that the conditions of Lemma 7.12(b) are satisfied. □

We have $\mathrm{Aut}(\mathsf{Okubo}(2)) = \langle g_1, g_2, g_3, g_4 \rangle$, where the values of the linear automorphisms g_i on the canonical basis are given by

$$\begin{aligned}
g_1 :\ & (e_\infty, e_{\infty'})(e_0, e_{0'})(e_1, e_{1'})(e_2, e_{2'}),\\
g_2 :\ & (e_0, e_1, e_2)(e_{0'}, e_{1'}, e_{2'}),\\
g_3 :\ & (e_\infty, e_{0'}, e_{\infty'}, e_0)(e_1, e_{2'}, e_{1'}, e_2),\\
g_4 :\ & e_\infty \mapsto e_{\infty'} + e_{0'} + e_{1'} + e_{2'}\\
& e_{\infty'} \mapsto e_\infty + e_{0'} + e_{1'} + e_{2'}\\
& e_0 \mapsto e_{0'} + e_1 + e_2\\
& e_{0'} \mapsto e_\infty + e_{\infty'} + e_0 + e_{0'} + e_{1'} + e_{2'}\\
& e_1 \mapsto e_0 + e_{1'} + e_2\\
& e_{1'} \mapsto e_\infty + e_{\infty'} + e_{0'} + e_1 + e_{1'} + e_{2'}\\
& e_2 \mapsto e_0 + e_1 + e_{2'}\\
& e_{2'} \mapsto e_\infty + e_{\infty'} + e_{0'} + e_{1'} + e_2 + e_{2'}.
\end{aligned}$$

The subgroup generated by $\{g_1, g_2, g_3\}$ is isomorphic to $\mathsf{SL}_2(3)$, and it consists of all 24 linear automorphisms that permute the canonical basis.

8 MULTIPLICATION GROUPS

Let F be a field. In this section we describe the multiplication groups of Paige loops, para-Paige quasigroups and Okubo quasigroups. Again, the result for Paige loops is known:

THEOREM 8.1 ([22, Corollary 4.7]). *Suppose that F is a field. Then the multiplication group of the Paige loop $\mathsf{PSL}_{1+3}(F)$ is $\mathsf{D}_4(F)$.*

We proceed to describe the multiplication group of $\mathsf{PP}(F)$. For a diassociative loop Q, let

$$J\colon Q \to Q; x \mapsto x^{-1} \tag{8.1}$$

denote the inversion mapping. Recall that a permutation φ of a loop Q is a *right pseudo-automorphism* if there exists an element c_φ of Q, the *companion* of φ, such that

$$(xy)\varphi \cdot c_\varphi = x\varphi \cdot (y\varphi \cdot c_\varphi)$$

for all elements x and y of Q.

PROPOSITION 8.2. *Let Q be a nontrivial Moufang loop with trivial commutant. Let φ be an anti-automorphism of Q. Then $\varphi \notin \mathrm{Mlt}(Q)$.*

Proof. Since $1\varphi = (1\cdot 1)\varphi = 1\varphi\cdot 1\varphi$, we have $1\varphi = 1$. It therefore suffices to show that $\varphi \notin \mathrm{Inn}(Q)$. Suppose that φ does lie in $\mathrm{Inn}(Q)$. By [3, Lemma VII.3.2], each inner mapping of a Moufang loop is a right pseudo-automorphism. We therefore have $(y\varphi \cdot x\varphi)\cdot c_\varphi = (xy)\varphi \cdot c_\varphi = x\varphi \cdot (y\varphi \cdot c_\varphi)$ for x, y in Q. Since φ is a bijection of Q, we conclude $(yx)c_\varphi = x(yc_\varphi)$ for x, y in Q. With $y = c_\varphi^{-1}$, we get $c_\varphi^{-1}xc_\varphi = x$, so c_φ lies in the trivial commutant. Then $yx = xy$ and $Q = C(Q)$, a contradiction. □

COROLLARY 8.3. *For any field F, the inversion mapping J is not an element of* $\mathrm{Mlt}\big(\mathsf{PSL}_{1+3}(F)\big)$.

Proof. Since Moufang loops are diassociative, the inversion mapping is an anti-automorphism of $\mathsf{PSL}_{1+3}(F)$. The result follows from Lemma 5.2 and Proposition 8.2. □

THEOREM 8.4. *Let F be a field. The multiplication group of the para-Paige quasigroup $\mathsf{PP}(F)$ is $\mathsf{D}_4(F).2$.*

Proof. Since $u \circ v = uJ \cdot vJ$, one has

$$\mathrm{Mlt}(\mathsf{PP}(F)) = \langle \mathrm{Mlt}(\mathsf{PSL}_{1+3}(F)), J\rangle = \langle \mathsf{D}_4(F), J\rangle = \mathsf{D}_4(F).2$$

by Lemma 2.2, Theorem 8.1 and Corollary 8.3. □

We conclude by describing the multiplication groups of Okubo quasigroups.

LEMMA 8.5. *For a field F, consider the map ρ or $\rho_{\mathsf{Zorn}(F)}$ given by the element* (4.7) *of $\mathsf{SL}_3(F)$.*

(a) *The map $\rho_{\mathsf{Zorn}(F)}$ is orthogonal.*

(b) *The map $\rho_{\mathsf{Zorn}(F)}$ acts as the permutation $(e_0\ e_1\ e_2)(e_{0'}\ e_{1'}\ e_{2'})$ on the canonical basis of §4.3.*

(c) *The map $\rho_{\mathsf{Zorn}(F)}$ has determinant* 1.

(d) *The map* $\rho_{\mathsf{Zorn}(F)}$ *induces an element of* $\mathrm{Mlt}(\mathsf{PSL}_{1+3}(F)))$*, a group isomorphic to* $\mathsf{D}_4(F)$*.*

Theorem 8.6. *Let* F *be a field. The multiplication group of the Okubo quasigroup* $\mathsf{OQ}(F)$ *is* $\mathsf{D}_4(F).2$*.*

Proof. Since $u * v = uJ\rho \cdot vJ\rho^2$, one has

$$\begin{aligned}\mathrm{Mlt}(\mathsf{OQ}(F)) &= \langle \mathrm{Mlt}(\mathsf{PSL}_{1+3}(F)), J\rho, J\rho^2\rangle = \langle \mathrm{Mlt}(\mathsf{PSL}_{1+3}(F)), J, \rho\rangle \\ &= \langle \mathsf{D}_4(F).2, \rho\rangle = \mathsf{D}_4(F).2\end{aligned}$$

by Lemma 2.2, Theorem 8.4 and Lemma 8.5. □

9 Character tables

In this section, the character tables of the para-Paige and Okubo quasigroups over a finite field $\mathsf{GF}(q)$ will be identified as coinciding with those of the Paige loop over $\mathsf{GF}(q)$ [2, 31]. The character table of a quasigroup determines its congruence lattice [15, Theorem 3.6] [27, Theorem 7.1], and therefore its simplicity. Thus the following theorem offers an alternative proof of the simplicity of the finite para-Paige and Okubo quasigroups.

Theorem 9.1. *For a prime power* q*, the character tables of the Paige loop* $\mathsf{PSL}_{1+3}(q)$*, the para-Paige quasigroup* $\mathsf{PP}(q)$*, and the Okubo quasigroup* $\mathsf{OQ}(q)$ *coincide.*

Proof. Recall that the (quasigroup) conjugacy classes of a quasigroup are the orbits of the diagonal action of its multiplication group on the Cartesian square of the quasigroup [27, §6.1]. By Theorems 8.4 and 8.6, the multiplication groups of the para-Paige and Okubo quasigroups are extended from the multiplication group of the Paige loop by the inversion mapping (8.1).
Let C be a conjugacy class of the quasigroup $\mathsf{PSL}_{1+3}(q)$. Since the association scheme consisting of all such classes is symmetric [2] [31, p.6], the class C coincides with its converse C^{-1}. Consider an element $(1, x)$ of C whose first component is the identity element of the loop $\mathsf{PSL}_{1+3}(q)$. Note that each element (y, z) of C may be written in the form $(y, z) = (1, x)g$ for some element g of $\mathrm{Mlt}(\mathsf{PSL}_{1+3}(F))$. One then has

$$(y, z)J = (1, x)gJ = (1, x^{-1})g^J = (x, 1)R(x^{-1})g^J \in C^{-1} = C\,,$$

so that $CJ = C$. The Fusion Theorem [16, §3] [27, §7.3] then shows that the conjugacy class schemes, and in particular the character tables, of $\mathsf{PSL}_{1+3}(q)$, $\mathsf{PP}(q)$, and $\mathsf{OQ}(q)$ coincide. □

Corollary 9.2. *The number of quasigroup conjugacy classes in* $\mathsf{PP}(q)$ *and* $\mathsf{OQ}(q)$ *is* $1 + q$ *if* q *is even, and* $(3 + q)/2$ *if* q *is odd.*

Proof. These numbers, which count the rows and columns in the respective character tables, were computed for $\mathsf{PSL}_{1+3}(q)$ in [2]. □

10 MINIMAL GENERATING SETS

Given a subset S of a quasigroup Q, let $\langle S\rangle = \langle S\rangle_Q$ denote the subquasigroup of Q generated by S, where we use the subscript when Q is not clear from the context. Recall that a nonempty subset of a finite quasigroup is a subquasigroup if and only if it is closed under multiplication.

For a quasigroup Q, let the *rank* $r(Q)$ the smallest cardinality of a generating set of Q.

In this section we determine the rank of all the finite Paige loops and finite para-Paige quasigroups, by showing that $r(\mathsf{PSL}_{1+3}(q)) = r(\mathsf{PP}(q)) = 3$. Moreover, $r(\mathsf{OQ}(q)) = 2$ if $q \not\equiv 1 \pmod 3$, and $2 \le r(\mathsf{OQ}(q)) \le 3$ if $q \equiv 1 \pmod 3$.

We start with the Paige loops. Note that $r(\mathsf{PSL}_{1+3}(F)) \ge 3$, since Moufang loops are diassociative and Paige loops are not groups. It was shown in [34] that $r(\mathsf{PSL}_{1+3}(q)) = 3$ for every q. We establish this result anew (cf. Theorem 10.4), with a different choice of generators that will simultaneously generate the corresponding para-Paige quasigroup.

Call an element of $\mathsf{SL}_2(F)$ *diagonal* if it is diagonal as a matrix. Then an element of $\mathsf{PSL}_2(F) = \mathsf{SL}_2(F)/\{\pm I\}$ is *diagonal* if any of its $\mathsf{SL}_2(F)$-representatives is diagonal.

For $i \in \{0,1,2\}$ define $\varphi_i : \mathsf{PSL}_2(F) \to \mathsf{PSL}_{1+3}(F)$ by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \varphi_i = \begin{bmatrix} a & b\mathbf{e}_i \\ c\mathbf{e}_i & d \end{bmatrix}.$$

Then φ_i is a monomorphism, and we set $G_i(F) = \mathsf{PSL}_2(F)\varphi_i$.

LEMMA 10.1. *Let F be a field, and i, j distinct elements of $\{0,1,2\}$. Then the Paige loop $\mathsf{PSL}_{1+3}(F)$ is generated by $G_i(F) \cup G_j(F)$. In particular, if $\mathsf{PSL}_2(F) = \langle D, E\rangle$ with D diagonal, then $\mathsf{PSL}_{1+3}(F) = \langle D\varphi_i,\, E\varphi_i,\, E\varphi_j\rangle$.*

Proof. The second statement follows immediately from the first, since $D\varphi_i = D\varphi_j$ when D is diagonal. To prove the first statement, we mimic the proof of [34, Proposition 3.3]. For x in F or F^3 let

$$U_x = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}.$$

Paige showed that $Q = \mathsf{PSL}_{1+3}(F) = \langle U_{\mathbf{a}},\, U_{\mathbf{a}}^T \mid \mathbf{a} \in F^3\rangle$, cf. [25, Lemmas 4.2, 4.3].

For the rest of the proof, let i, j be distinct elements of $\{0,1,2\}$. With α, β, $\gamma \in F$, we have

$$U_{\alpha\mathbf{e}_i} U_{\beta\mathbf{e}_j} \cdot U^T_{-\alpha\beta(\mathbf{e}_i\times\mathbf{e}_j)} = U_{\alpha\mathbf{e}_i+\beta\mathbf{e}_j},$$
$$U_{\alpha\mathbf{e}_i+\beta\mathbf{e}_j} U_{\gamma(\mathbf{e}_i\times\mathbf{e}_j)} \cdot U^T_{-\beta\gamma\mathbf{e}_i+\alpha\gamma\mathbf{e}_j} = U_{\alpha\mathbf{e}_i+\beta\mathbf{e}_j+\gamma(\mathbf{e}_i\times\mathbf{e}_j)},$$

where we have used $\mathbf{e}_i \times (\mathbf{e}_j \times \mathbf{e}_i) = \mathbf{e}_j$ and other familiar cross-product identities. Dual identities are obtained for $U^T_{\mathbf{a}}$ by applying the anti-automorphic

transpose operation. Thus

$$Q = \langle U_{\alpha\mathbf{e}_i}, U^T_{\alpha\mathbf{e}_i} \mid \alpha \in F,\, i \in \{0,1,2\}\rangle\,.$$

Finally, with $0 \neq \alpha \in F$, we calculate

$$\begin{bmatrix} 0 & \mathbf{e}_i \\ -\mathbf{e}_i & 0 \end{bmatrix} \begin{bmatrix} 1 & -\alpha\mathbf{e}_j \\ \alpha^{-1}\mathbf{e}_j & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & \mathbf{e}_i \\ -\mathbf{e}_i & 0 \end{bmatrix} \begin{bmatrix} 1 & -\alpha\mathbf{e}_j \\ \alpha^{-1}\mathbf{e}_j & 0 \end{bmatrix} = -U^T_{\alpha(\mathbf{e}_i\times\mathbf{e}_j)},$$

and dually for $U_{\mathbf{a}}$. This implies that $Q = \langle G_i(F) \cup G_j(F)\rangle$. □

As will become clear from Lemma 10.5, we are particularly interested in generating sets of $\mathsf{PSL}_2(q)$ where one of the generators is diagonal and at least one generator has order relatively prime to 3. In Lemma 10.3, we rely heavily on results of Albert and Thompson [1], where it was proved that each $\mathsf{PSL}_n(q)$ has a 2-generating set containing an involution.

PROPOSITION 10.2 ([1, Lemmas 8, 9, 10]). *Let $G = \mathsf{PSL}_2(q)$, let α be a primitive element of $\mathsf{GF}(q)$, and let*

$$A = \begin{bmatrix} a & b \\ -(1+a^2)b^{-1} & -a \end{bmatrix}, \quad B = \begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{bmatrix}, \quad C = \begin{bmatrix} 0 & 1 \\ -1 & \alpha \end{bmatrix},$$

where a, $b \in \mathsf{GF}(q)$ will be specified below.

(a) *If $q > 2$ then G is generated by B and C.*

(b) *If $q > 2$ is even then G is generated by A and B, where $a \neq 0$, 1 and $b = \alpha a^3(1+a^{-1})^2$. Moreover, A is an involution.*

(c) *If q is odd, $q \neq 3$, 5, 9, then G is generated by A and B, where $a = (\alpha-\alpha^{-1})/2$, $\delta = (\alpha+\alpha^{-1})/(\alpha-\alpha^{-1})$ and $b = a^{-3}\delta^2\alpha((1-\delta^2)(\delta^4-1))^{-1}$. Moreover, A is an involution.* □

LEMMA 10.3. *Let $q > 2$. Then $\mathsf{PSL}_2(q) = \langle D, E\rangle$, where D is diagonal and one of D, E has order relatively prime to 3.*

Proof. If $q > 2$ is even, let $D = B$ and $E = A$ as in Proposition 10.2(b). If q is odd and $q \neq 3$, 5, 9, let $D = B$ and $E = A$ as in Proposition 10.2(c). Finally, supposing that $q \in \{3, 5, 9\}$, use $D = B$ and $E = C$ as in Proposition 10.2(a), and note that $|D| = (q-1)/2$ is relatively prime to 3 in this situation. □

Note that no nonidentity element of $\mathsf{PSL}_2(2) \cong S_3$ is diagonal, so Lemma 10.3 does not extend to the case $q = 2$.

THEOREM 10.4. *Every finite Paige loop has rank 3. Moreover, it is always possible to choose a 3-generating subset of $\mathsf{PSL}_{1+3}(q)$ in which at least one element has order relatively prime to 3.*

Proof. When $q > 2$, we are done by Lemmas 10.1 and 10.3. We have

$$\mathsf{PSL}_{1+3}(2) = \left\langle \pm \begin{bmatrix} 1 & \mathbf{e}_1 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} 1 & \mathbf{e}_2 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} 0 & \mathbf{e}_3 \\ \mathbf{e}_3 & 1 \end{bmatrix} \right\rangle$$

by [34, Proposition 4.1], and the first generator has order 2. □

We proceed to obtain a minimal generating set for finite para-Paige quasigroups.

LEMMA 10.5. *Let q be a prime power. Identify the underlying sets of $\mathsf{PSL}_{1+3}(q)$ and $\mathsf{PP}(q)$, and let S be a nonempty subset of $\mathsf{PSL}_{1+3}(q)$. Then:*

(a) $\langle S\rangle_{\mathsf{PP}(q)} \subseteq \langle S \cup \overline{S}\rangle_{\mathsf{PP}(q)} = \langle S \cup \overline{S}\rangle_{\mathsf{PSL}_{1+3}(q)} = \langle S\rangle_{\mathsf{PSL}_{1+3}(q)}$.

(b) $\overline{x} \in \langle x\rangle_{\mathsf{PP}(q)}$ *if and only if the order of x in $\mathsf{PSL}_{1+3}(q)$ is not divisible by* 3.

(c) *If S contains an element whose order in $\mathsf{PSL}_{1+3}(q)$ is not divisible by* 3, *then $\langle S\rangle_{\mathsf{PP}(q)} = \langle S\rangle_{\mathsf{PSL}_{1+3}(q)}$.*

Proof. (a) Note that $\overline{x} = x^{-1}$ and $x \circ y = x^{-1}y^{-1}$, where the inverses are taken in $\mathsf{PSL}_{1+3}(q)$. Part (a) follows.

(b) By Proposition 6.2, $\langle x\rangle_{\mathsf{PP}(q)} = \{x^{3k+1} \mid k \in \mathbb{Z}\}$. It follows that $\overline{x} = x^{-1} \in \langle x\rangle_{\mathsf{PP}(q)}$ if and only if $x^{-1} = x^{3k+1}$ for some k, which happens if and only if 3 does not divide $\left|\langle x\rangle_{\mathsf{PP}(q)}\right|$.

(c) Let $x \in S$ be such that 3 does not divide $\left|\langle x\rangle_{\mathsf{PSL}_{1+3}(q)}\right|$. Since $\overline{x} \in \langle S\rangle_{\mathsf{PP}(q)}$ by (b), we have $1 = \overline{x} \cdot x = x \circ \overline{x} \in \langle S\rangle_{\mathsf{PP}(q)}$ and $\overline{y} = 1 \cdot \overline{y} = 1 \circ y \in \langle S\rangle_{\mathsf{PP}(q)}$ for every $y \in S$. Hence $\langle S\rangle_{\mathsf{PP}(q)} = \langle S \cup \overline{S}\rangle_{\mathsf{PP}(q)}$ and we are done by part (a). □

THEOREM 10.6. *Each finite para-Paige quasigroup has rank equal to* 3. *Moreover, it is possible to choose a* 3*-element subset of $\mathsf{PP}(q)$ that simultaneously generates $\mathsf{PP}(q)$ and $\mathsf{PSL}_{1+3}(q)$.*

Proof. By Lemma 10.5(a) we have $r(\mathsf{PP}(q)) \geq r(\mathsf{PSL}_{1+3})(q)$. We are done by Theorem 10.4 and Lemma 10.5. □

The situation appears to be more complicated in finite Okubo quasigroups and we offer only a partial result. We start with an observation that appears to be obvious, but for which we do not have a one-line argument:

LEMMA 10.7. *No finite Okubo quasigroup is generated by a single element. That is, $r(\mathsf{OQ}(q)) > 1$ for every q.*

We offer two complete proofs, and yet another proof for the case $q \not\equiv 0 \pmod 3$. In all three proofs, suppose for a contradiction that $\langle a\rangle_{\mathsf{OQ}(q)} = \mathsf{OQ}(q)$ for some $a \in \mathsf{OQ}(q)$.

Proof 1 (based on the fine structure of $\langle a\rangle_{\mathsf{OQ}(q)}$): By Proposition 6.10, the order of $\langle a\rangle_{\mathsf{OQ}(q)}$ is at most $2\big|\langle a^{\rho^2}a^{\rho}\cdot a\rangle_{\mathsf{PSL}_{1+3}(q)}\big|$. Hence there is $b\in\mathsf{PSL}_{1+3}(q)$ such that $\big|\langle b\rangle_{\mathsf{PSL}_{1+3}(q)}\big|\geq|\mathsf{PSL}_{1+3}(q)|/2$. In any finite Moufang loop, the order of an element divides the order of the loop [10, 12]. Thus either $\big|\langle b\rangle_{\mathsf{PSL}_{1+3}(q)}\big|=|\mathsf{PSL}_{1+3}(q)|$ or $\big|\langle b\rangle_{\mathsf{PSL}_{1+3}(q)}\big|=|\mathsf{PSL}_{1+3}(q)|/2$. The former case is impossible, since $\mathsf{PSL}_{1+3}(q)$ is power-associative but not a group. In the latter case, b generates a subloop of index 2 in $\mathsf{PSL}_{1+3}(q)$, necessarily a normal subloop, in contradiction to the simplicity of $\mathsf{PSL}_{1+3}(q)$.

Proof 2 (based on a linearization of semisymmetry): Let $S=SQ(\mathsf{Okubo}(q))$. Then $\langle a,-a\rangle_S=S$. We will show that $\langle a,-a\rangle_S$ is contained in the linear span of a and $a*a$. This contradicts the fact that the linear span of S contains a basis of $\mathsf{Okubo}(q)$ (see proof of Lemma 7.5). By semisymmetry, $(a*a)*a=aN(a)=a*(a*a)$. Linearizing the identity $(x*y)*x=yN(x)$ with $x+z$ in place of x, we get

$$\begin{aligned}yN(x+z)&=((x+z)*y)*(x+z)\\&=(x*y)*x+(x*y)*z+(z*y)*x+(z*y)*z\\&=(x*y)*z+(z*y)*x+y(N(x)+N(z)),\end{aligned}$$

so $(x*y)*z+(z*y)*x=y(N(x+z)-N(x)-N(z))$. Substituting $x=a$, $y=a$ and $z=a*a$ yields $(a*a)*(a*a)+((a*a)*a)*a=a(N(a+a*a)-N(a)-N(a*a))$, so $(a*a)*(a*a)=a(N(a+a*a)-N(a)-N(a*a))-(a*a)N(a)$. We have shown that $(a*a)*a$, $a*(a*a)$ and $(a*a)*(a*a)$ are elements of the linear span of a and $a*a$. More complicated iterated products of a then lie in the same span by distributivity.

Partial proof 3 (based on automorphisms of $\mathsf{OQ}(q)$): Suppose that $q\not\equiv 0 \pmod 3$. By Corollary 7.9, $|\mathrm{Aut}(\mathsf{OQ}(q))|\geq|\mathrm{Aut}(\mathsf{Okubo}(q))|$. Theorem 7.4 yields $\mathrm{Aut}(\mathsf{Okubo}(F))=\mathsf{PGL}_3(q)$. Now,

$$\mathsf{PGL}_3(q)=(q^3-1)(q^3-q)(q^3-q^2)/(q-1).$$

An automorphism of $\mathsf{OQ}(q)=\langle a\rangle_{\mathsf{OQ}(q)}$ is determined by its value on a and therefore $|\mathrm{Aut}(\mathsf{OQ}(q))|\leq|\mathsf{OQ}(q)|$. By Theorem 5.8, $|\mathsf{OQ}(q)|=(q^7-q^3)/2$ if q is odd and $|\mathsf{OQ}(q)|=q^7-q^3$ if q is even. In any case, $|\mathsf{OQ}(q)|\leq q^7-q^3$. But $q^7-q^3<(q^3-1)(q^3-q)(q^3-q^2)/(q-1)$ for every q, a contradiction. □

LEMMA 10.8. *Let $S\subseteq\mathsf{PSL}_{1+3}(F)$, and let I be the identity element of $\mathsf{PSL}_{1+3}(F)$. Then:*

(a) $\langle S\cup\{I\}\rangle_{\mathsf{OQ}(F)}\geq\langle S\rangle_{\mathsf{PSL}_{1+3}(F)}$.

(b) *If D, $E\in\mathsf{PSL}_2(F)$ are such that $\langle D,E\rangle_{\mathsf{PSL}_2(F)}=\mathsf{PSL}_2(F)$ and D is diagonal, then $\langle I,D,E\varphi_1\rangle_{\mathsf{OQ}(F)}=\mathsf{OQ}(F)$.*

Proof. Part (a) follows immediately from the identity (4.11). For (b), let $H=\langle I,D,E\varphi_1\rangle_{\mathsf{OQ}(F)}$. By (4.13), we have

$$E\varphi_2=(E\varphi_1)^{\rho}=I*(I*E\varphi_1)$$

in H. By (a), $H = \langle I, D, E\varphi_1, E\varphi_2\rangle_{\mathsf{OQ}(F)} \geq \langle D, E\varphi_1, E\varphi_2\rangle_{\mathsf{PSL}_{1+3}(F)}$. Finally, by Lemma 10.1, $\langle D, E\varphi_1, E\varphi_2\rangle_{\mathsf{PSL}_{1+3}(F)} = \mathsf{PSL}_{1+3}(F)$. □

THEOREM 10.9. *If $q \equiv 1 \pmod 3$, then $2 \leq r(\mathsf{OQ}(q)) \leq 3$. If $q \not\equiv 1 \pmod 3$, then $r(\mathsf{OQ}(q)) = 2$.*
In more detail, let B, $C \in \mathsf{PSL}_2(q)$ be as in Proposition 10.2. Then $\mathsf{OQ}(q) = \langle I, B, C\varphi_1\rangle_{\mathsf{OQ}(q)}$ for every q. If $q \not\equiv 1 \pmod 3$, then $\mathsf{OQ}(q) = \langle B, C\varphi_1\rangle_{\mathsf{OQ}(q)}$.

Proof. By Lemma 10.7, $r(\mathsf{OQ}(q)) > 1$. If $q = 2$ then $I = B$, and it can be verified computationally that $\langle I, C\varphi_1\rangle_{\mathsf{OQ}(2)} = \mathsf{OQ}(2)$. For the rest of the proof suppose that $q > 2$.
Let α be a primitive element of $\mathsf{GF}(q)$ and set $D = B$ and $E = C$. Then the condition (b) of Lemma 10.8 holds by Proposition 10.2(a), and we therefore have $\langle I, D, E\varphi_1\rangle_{\mathsf{OQ}(q)} = \mathsf{OQ}(q)$.
For any diagonal element $D_0 \in \mathsf{PSL}_2(q)$, we have

$$\langle D_0\rangle_{\mathsf{OQ}(q)} = \{D_0^{3k+1} \mid k \in \mathbb{Z}\}$$

by Lemma 6.1, since $D_0^k * D_0^\ell = D_0^{-k} \cdot D_0^{-\ell} = D_0^{-(k+\ell)}$ (with powers taken in $\mathsf{PSL}_2(q)$).
Suppose that $q \not\equiv 1 \pmod 3$. If $q \equiv 2 \pmod 3$, then $q - 1 \equiv 1 \pmod 3$, and hence $I \in \langle D\rangle_{\mathsf{OQ}(q)}$. If $q \equiv 0 \pmod 3$, then $q-1 \equiv 2 \pmod 3$ and $2(q-1) \equiv 1 \pmod 3$, so $I \in \langle D\rangle_{\mathsf{OQ}(q)}$ again. Thus $\langle D, E\varphi_1\rangle_{\mathsf{OQ}(q)} = \langle I, D, E\varphi_1\rangle_{\mathsf{OQ}(q)} = \mathsf{OQ}(q)$. □

Note that, up to the choice of a primitive element, Theorems 10.4, 10.6 and 10.9 are constructive.
We have also verified computationally that $\mathsf{OQ}(q) = \langle I, C\varphi_1\rangle$ for $q = 4$, 7 and 13.

11 REDUCED HASSE DIAGRAMS

This section is motivated by concepts developed in [32, 33]. Given an algebra Q, the *Hasse diagram* $\mathrm{Sub}(Q)$ is a drawing of the set of subalgebras of Q, partially ordered with respect to inclusion, where a subalgebra A is placed below B if and only if $A < B$.
Hasse diagrams become unwieldy when Q has a large number of subalgebras. To overcome this problem, we describe a reduced version of the labeled Hasse diagrams for finite algebras, in which the subalgebras are presented only up to the action of the automorphism group $\mathrm{Aut}(Q)$. The resulting diagram, denoted by $\mathrm{Sub}(Q)/\mathrm{Aut}(Q)$ (see Definition 11.4), is typically much smaller than $\mathrm{Sub}(Q)$, and although it does not capture all the details of $\mathrm{Sub}(Q)$, it gives useful global and local information about inclusions among subalgebras.

11.1 AUTOMORPHISMS OF BINARY RELATIONS

We start with a general notion.

DEFINITION 11.1. Let X be a set and $\sim_1$, $\sim_2$ binary relations on X. For x_1, $x_2 \in X$ define

$$\begin{aligned} H_{\sim_1,\sim_2}(x_1,x_2) &= \{y \in X \mid x_1 \sim_1 y \sim_2 x_2\}, \\ h_{\sim_1,\sim_2}(x_1,x_2) &= |H_{\sim_1,\sim_2}(x_1,x_2)|. \end{aligned}$$

Note that if $\equiv$ is an equivalence relation on X and $x_1 \equiv x_1'$, $x_2 \equiv x_2'$ then

$$\begin{aligned} H_{\equiv,\sim_2}(x_1,x_2) &= H_{\equiv,\sim_2}(x_1',x_2), \\ H_{\sim_1,\equiv}(x_1,x_2) &= H_{\sim_1,\equiv}(x_1,x_2'). \end{aligned} \tag{11.1}$$

We say that f is an *automorphism* of a binary relation $\sim$ on X if f is a bijection on X, and for every x_1, $x_2 \in X$ we have $x_1 \sim x_2$ if and only if $f(x_1) \sim f(x_2)$. Suppose that f is an automorphism of both $\sim_1$ and $\sim_2$. Then

$$\begin{aligned} f(H_{\sim_1,\sim_2}(x_1,x_2)) &= \{f(y) \mid x_1 \sim_1 y \sim_2 x_2\} \\ &= \{f(y) \mid f(x_1) \sim_1 f(y) \sim_2 f(x_2)\} = H_{\sim_1,\sim_2}(f(x_1),f(x_2)) \end{aligned}$$

implies

$$h_{\sim_1,\sim_2}(x_1,x_2) = h_{\sim_1,\sim_2}(f(x_1),f(x_2)). \tag{11.2}$$

11.2 SUBALGEBRAS MODULO AUTOMORPHISMS

We now specialize the above concepts to subalgebras modulo automorphisms. Throughout this section, let Q be an algebra, and let X be the set of all subalgebras of Q. Let $\leq$ be the partial order on X induced by inclusion, and let $\equiv$ be the equivalence relation on X whose equivalence classes are the orbits of the action of $G = \mathrm{Aut}(Q)$ on X.

DEFINITION 11.2. For A, $B \in X$, the constant $h_{\leq,\equiv}(A,B)$ counts the number of subalgebras C such that $A \leq C \equiv B$, and $h_{\equiv,\leq}(A,B)$ counts the number of subalgebras C such that $A \equiv C \leq B$. The constants $h_{\leq,\equiv}(A,B)$ and $h_{\equiv,\leq}(A,B)$ are called the (*reduced*) *Hasse constants* for Q.

PROPOSITION 11.3. *Under the assumptions of this section:*

(a) *The reduced Hasse constants $h_{\leq,\equiv}(A,B)$, $h_{\equiv,\leq}(A,B)$ are well-defined modulo $\equiv$ in both coordinates.*

(b) *For A, $B \in X$, define $A^G \preceq B^G$ if and only if $h_{\leq,\equiv}(A,B) > 0$, where A^G and B^G are the respective orbits of A and B under the action of G on X. Then $\preceq$ is a reflexive and transitive relation on $X^{\equiv}$.*

Furthermore, if Q is finite, then:

(c) *$\preceq$ is a partial order on $X^{\equiv}$.*

(d) *For A, $B \in X$ we have*

$$|A^G| \cdot h_{\leq,\equiv}(A,B) = |B^G| \cdot h_{\equiv,\leq}(A,B). \tag{11.3}$$

(v) Let A, $B \in X$ be such that $A < B$.

(a) If $|B^G| = 1$ then $h_{\leq,\equiv}(A,B) = 1$ and $h_{\equiv,\leq}(A,B) = |A^G|$.
(b) If $|A^G| = 1$ then $h_{\leq,\equiv}(A,B) = |B^G|$ and $h_{\equiv,\leq}(A,B) = 1$.

Proof. By (11.1), $h_{\leq,\equiv}$ is well-defined modulo $\equiv$ in the second coordinate. Suppose that A, $A' \in X$ satisfy $A \equiv A'$, and let $f \in G$ be such that $f(A) = A'$. By (11.2), we have $h_{\leq,\equiv}(A,B) = h_{\leq,\equiv}(f(A),f(B)) = h_{\leq,\equiv}(A',f(B)) = h_{\leq,\equiv}(A',B)$, where the last equality follows because $B \equiv f(B)$ by definition. The proof for $h_{\equiv,\leq}$ is similar.
For (b), suppose that A, $B \in X$. Since $A \leq A$, we have $h_{\leq,\equiv}(A,A) > 0$, and $\preceq$ is reflexive on $X^{\equiv}$. Suppose that $A^G \preceq B^G \preceq C^G$. Then there are $A' \in A^G$, $B' \in B^G$ such that $A' \leq B'$. Using (a) and $h_{\leq,\equiv}(B,C) > 0$, there is $C' \in C^G$ such that $B' \leq C'$. Hence $A' \leq C'$, and $\preceq$ is transitive on X.
For the remainder of the proof, suppose that Q is finite.
If $A^G \preceq B^G$ then $|A| \leq |B|$. Hence, if $A^G \preceq B^G \preceq A^G$, then $|A| \leq |B| \leq |A|$ implies $|A| = |B|$. Thus $A = B$, by finiteness, proving (c).
To establish (11.3), we will count in two ways the number m of pairs $(A_0,B_0) \in X \times X$ such that $A_0 \equiv A$, $B_0 \equiv B$ and $A_0 \leq B_0$. On the one hand,

$$m = \sum_{A_0 \equiv A} h_{\leq,\equiv}(A_0,B) = |A^G| \cdot h_{\leq,\equiv}(A_0,B) = |A^G| \cdot h_{\leq,\equiv}(A,B),$$

where we have used (a) in the last step. On the other hand,

$$m = \sum_{B_0 \equiv B} h_{\equiv,\leq}(A,B_0) = |B^G| \cdot h_{\equiv,\leq}(A,B_0) = |B^G| \cdot h_{\equiv,\leq}(A,B).$$

Part (v) follows immediately from (11.3). □

11.3 The reduced Hasse diagram

Definition 11.4. Using the notational conventions of §11.2, the *reduced Hasse diagram* $\mathrm{Sub}(Q)/\mathrm{Aut}(Q)$ of Q is a labeled drawing of the partially ordered set $(X^{\equiv}, \preceq)$, with vertices A^G labeled by $|A^G|$, and with edges $A^G \prec B^G$ labeled by the Hasse constants $h_{\leq,\equiv}(A,B)$.

Remark 11.5. (a) Proposition 11.3 guarantees that the Hasse constants are well-defined modulo the action of $G = \mathrm{Aut}(Q)$, and that $\preceq$ is a partial order on $X^{\equiv}$. The reduced Hasse diagram $\mathrm{Sub}(Q)/\mathrm{Aut}(Q)$ is therefore well-defined. Only the constants $h_{\leq,\equiv}(A,B)$ are displayed in the reduced Hasse diagram. However, the dual constants $h_{\equiv,\leq}(A,B)$ may be derived from (11.3).

(b) In the reduced Hasse diagram $\mathrm{Sub}(Q)/\mathrm{Aut}(Q)$, we will suppress all edge labels $h_{\leq,\equiv}(A, B)$ with $|A^G| = 1$ or $|B^G| = 1$, since their values may be calculated by Proposition 11.3(v).

(c) Call an edge $A < B$ in a reduced Hasse diagram *maximal* if A is a maximal subalgebra of B. In an ordinary Hasse diagram of a finite algebra, it is customary to plot only maximal edges, the remaining edges being implied by the transitivity of inclusion. We will also plot only the maximal edges in the reduced Hasse diagram $\mathrm{Sub}(Q)/\mathrm{Aut}(Q)$. However, in general, the Hasse constants on non-maximal edges cannot be deduced from the Hasse constants on maximal edges and the vertex labels.

11.4 A SYMMETRIC GROUP EXAMPLE

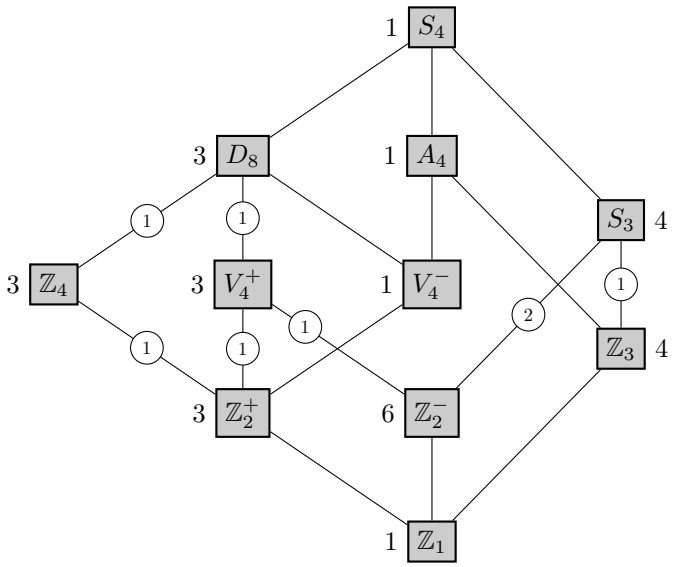

Figure 1: The Hasse diagram $\mathrm{Sub}(S_4)/\mathrm{Aut}(S_4)$ with $\mathbb{Z}_2^+ = \langle (1,2)(3,4) \rangle$, $\mathbb{Z}_2^- = \langle (1,2) \rangle$, $V_4^+ = \langle (1,2), (3,4) \rangle$ and $V_4^- = \langle (1,2)(3,4), (1,3)(2,4) \rangle$.

To illustrate Definition 11.4 and the above conventions, Figure 1 depicts the reduced Hasse diagram $\mathrm{Sub}(Q)/\mathrm{Aut}(Q)$ for the symmetric group $Q = S_4$. The orbits of subalgebras (subgroups) are labeled with the isomorphism type of a representative, where we use standard notational conventions of group theory, and employ superscripts to distinguish orbits whose representatives have the same isomorphism type. The nontrivial edge labels not displayed in Figure 1 are $h_{\leq,\equiv}(\mathbb{Z}_2^+, D_8) = 3$ and $h_{\leq,\equiv}(\mathbb{Z}_2^-, D_8) = 1$.

12 CLASSIFYING SUBQUASIGROUPS OVER THE FIELD OF ORDER 2

We now present analyses of the subquasigroup structure for the Paige, para-Paige, and Okubo quasigroups over the field $\mathsf{GF}(2)$.

12.1 SUBLOOPS OF $\mathsf{PSL}_{1+3}(2)$

The lattice of subloops of the Paige loop $Q = \mathsf{PSL}_{1+3}(2)$ and the actions of $\mathrm{Aut}(Q) \cong \mathsf{G}_2(2)$ on the subloops of Q are described in [33].

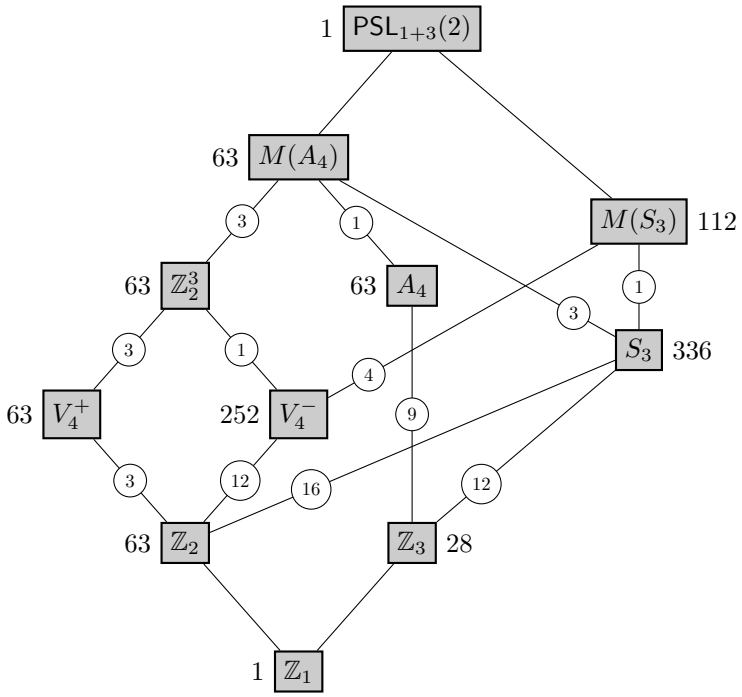

Figure 2: The Hasse diagram $\mathrm{Sub}(Q)/\mathrm{Aut}(Q)$ for $Q = \mathsf{PSL}_{1+3}(2)$.

Figure 2 gives the reduced Hasse diagram $\mathrm{Sub}(Q)/\mathrm{Aut}(Q)$. In the diagram, $M(H)$ denotes the Chein double of a group H, cf. [4]. The nontrivial edge labels not displayed in Figure 2 are listed as follows:

$$h_{\leq,\equiv}(\mathbb{Z}_2, \mathbb{Z}_2^3) = 7\,; \qquad h_{\leq,\equiv}(\mathbb{Z}_2, M(S_3)) = 16\,;$$
$$h_{\leq,\equiv}(\mathbb{Z}_2, A_4) = 3\,; \qquad h_{\leq,\equiv}(\mathbb{Z}_2, M(A_4)) = 15\,;$$
$$h_{\leq,\equiv}(\mathbb{Z}_3, M(S_3)) = 4\,; \qquad h_{\leq,\equiv}(\mathbb{Z}_3, M(A_4)) = 9\,;$$
$$h_{\leq,\equiv}(V_4^+, M(A_4)) = 7\,; \qquad h_{\leq,\equiv}(V_4^-, M(A_4)) = 3\,.$$

12.2 Subquasigroups of $\mathsf{PP}(2)$

According to Proposition 7.3, the automorphism group of $\mathsf{PP}(2)$ is isomorphic to $\mathsf{G}_2(2)$. By Lemma 5.5, every subloop of $\mathsf{PSL}_{1+3}(2)$ is also a subquasigroup of $\mathsf{PP}(2)$. The converse is close to being true.

Lemma 12.1. *A subquasigroup of* $\mathsf{PP}(2)$ *which is not a subloop of* $\mathsf{PSL}_{1+3}(2)$ *is a union of some idempotents of* $\mathsf{PP}(2)$ *different from* I*.*
There are 57 *idempotents in* $\mathsf{PP}(2)$*, corresponding to* I *and the* 56 *elements of order* 3 *in* $\mathsf{PSL}_{1+3}(2)$*.*

Proof. By Lemma 10.5, a subquasigroup of $\mathsf{PP}(q)$ that is not a subloop of $\mathsf{PSL}_{1+3}(q)$ consists of elements whose order in $\mathsf{PSL}_{1+3}(q)$ is divisible by 3. Any element of $\mathsf{PSL}_{1+3}(2)$ is of order 1, 2 or 3, and there are 56 elements of order 3. Hence a subquasigroup of $\mathsf{PP}(2)$ which is not a subloop of $\mathsf{PSL}_{1+3}(2)$ must consist of elements whose order is precisely 3 in $\mathsf{PSL}_{1+3}(2)$. Finally, we have $x \circ x = x$ if and only if $x^{-2} = x$, that is, $x^3 = 1$. □

Computer calculations with the `LOOPS` package for `GAP` show:

Proposition 12.2. *The proper subquasigroups of the para-Paige quasigroup* $\mathsf{PP}(2)$ *over the two-element field consist of:*

- *the empty quasigroup;*
- *the* 1045 *subloops of* $\mathsf{PSL}_{1+3}(2)$ *(see Figure 2 and Lemma 5.5);*
- *the* 56 *idempotents of Lemma 12.1, on which* $\mathrm{Aut}(\mathsf{PP}(2))$ *acts transitively;*
- 126 *additional quasigroups isomorphic to* $O_4 = (\mathbb{Z}_2 \times \mathbb{Z}_2, *)$ *with multiplication*
$$(a, b) * (c, d) = (b + c + d, a + b + c),$$
which are precisely the subquasigroups of $\mathsf{PP}(2)$ *of order* 4 *generated by* 2 *idempotents, and on which* $\mathrm{Aut}(\mathsf{PP}(2))$ *acts transitively. These quasigroups are identified structurally in Corollary 12.5.*

The reduced Hasse diagram $\mathrm{Sub}(Q)/\mathrm{Aut}(Q)$ for $Q = \mathsf{PP}(2)$ is depicted in Figure 3. We keep the labels of subloops of $\mathsf{PSL}_{1+3}(2)$ for subquasigroups of $\mathsf{PP}(2)$ for convenience, but the subquasigroups are in fact isotopes of the subloops as described in Lemma 5.5. The trivial subloop of $\mathsf{PSL}_{1+3}(2)$ is denoted by $\mathbb{Z}_1^+$ to distinguish it from the remaining 56 idempotents of $\mathsf{PP}(2)$, denoted by $\mathbb{Z}_1^-$. Finally, O_4 stands for any of the 126 quasigroups of order 4 that do not correspond to any subloop of $\mathsf{PSL}_{1+3}(2)$. The nontrivial Hasse constants not depicted in Figure 3 are listed as follows:

$$h_{\leq,\equiv}(\mathbb{Z}_1^-, S_3) = 12\,; \qquad h_{\leq,\equiv}(\mathbb{Z}_1^-, M(S_3)) = 4\,;$$
$$h_{\leq,\equiv}(\mathbb{Z}_1^-, A_4) = 9\,; \qquad h_{\leq,\equiv}(\mathbb{Z}_1^-, M(A_4)) = 9\,;$$
$$h_{\leq,\equiv}(Q_4, M(A_4)) = 1\,.$$

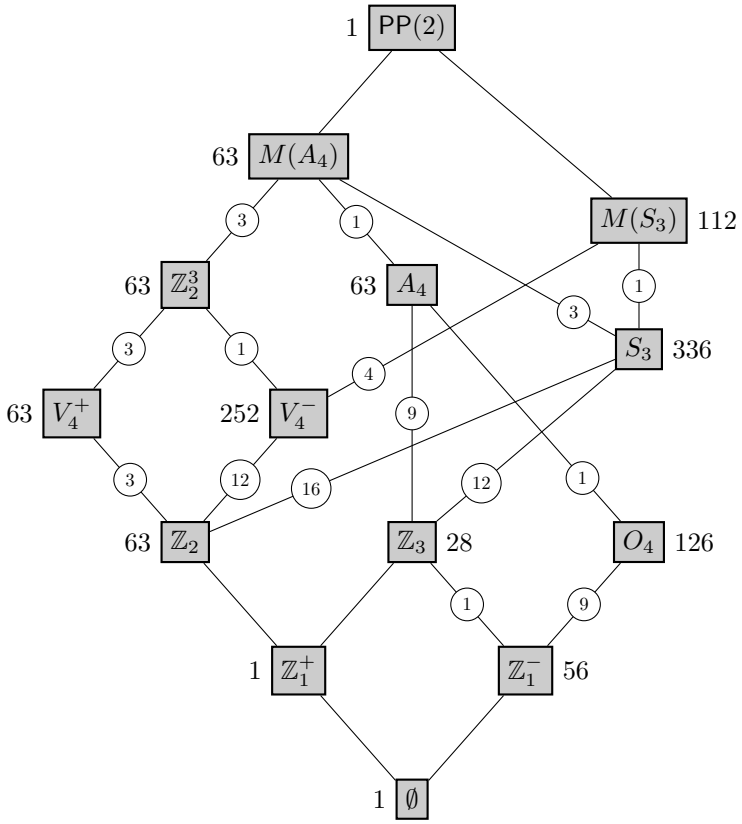

Figure 3: The Hasse diagram $\mathrm{Sub}(Q)/\mathrm{Aut}(Q)$ for $Q = \mathsf{PP}(2)$.

12.3 Subquasigroups of $\mathsf{OQ}(2)$

Let $Q = \mathsf{OQ}(2)$ be the Okubo quasigroup over the two-element field $\mathsf{GF}(2)$. In this section we will describe the lattice of subquasigroups of Q to within the action of the automorphism group of Q. With the exception of Proposition 12.4 and its corollary, all the results were obtained computationally with the `LOOPS` package.

For the purposes of Proposition 12.3, let us fix a canonical copy of the Chein

double $M(S_3)$ of the symmetric group S_3 as follows:

1	2	3	4	5	6	7	8	9	10	11	12
2	1	4	3	6	5	8	7	12	11	10	9
3	6	5	2	1	4	9	10	11	12	7	8
4	5	6	1	2	3	10	9	8	7	12	11
5	4	1	6	3	2	11	12	7	8	9	10
6	3	2	5	4	1	12	11	10	9	8	7
7	8	11	10	9	12	1	2	5	4	3	6
8	7	12	9	10	11	2	1	4	5	6	3
9	12	7	8	11	10	3	4	1	6	5	2
10	11	8	7	12	9	4	3	6	1	2	5
11	10	9	12	7	8	5	6	3	2	1	4
12	9	10	11	8	7	6	5	2	3	4	1

.

Proposition 12.3. *The subquasigroups of the Okubo quasigroup* $\mathsf{OQ}(2)$ *over the two-element field consist of:*

- *the empty subquasigroup;*
- 12 *subquasigroups of order* 1*, denoted* $\mathbb{Z}_1$*;*
- 36 *subquasigroups of order* 2 *without identity element, denoted by* O_2*;*
- 4 *subquasigroups of order* 3 *isomorphic to* $(\mathbb{Z}_3, -x-y)$*, denoted* $O_{3,1}$*;*
- 24 *subquasigroups of order* 3 *isomorphic to* $(\mathbb{Z}_3, 2-x-y)$*, denoted* $O_{3,2}$*;*
- 9 *subquasigroups of order* 4 *that are isomorphic to the quasigroup* $O_4 = (\mathbb{Z}_2 \times \mathbb{Z}_2, *)$ *of §12.2 that is described structurally in Corollary 12.5;*
- 12 *subquasigroups of order* 6 *isomorphic to* $(S_3, *)$ *with multiplication*

$$x * y = (1,2,3)x^{-1}(1,2,3)y^{-1}(1,2,3),$$

  denoted O_6*;*
- 9 *subquasigroups of order* 8 *isomorphic to the direct product* $\mathbb{Z}_2 \times O_4$*, described structurally in Proposition 12.4;*
- 8 *subquasigroups of order* 12 *isomorphic to* $(M(S_3), *)$ *with multiplication* $x * y = xf \cdot yf^{-1}$*, where*

$$f = (2,12,7)(3,5)(4,10,11)(6,8,9),$$

  denoted $O_{12,1}$*;*

- 1 *subquasigroup of order* 12 *isomorphic to* $(M(S_3), *)$ *with multiplication* $x * y = xf \cdot yf^{-1}$, *where*

$$f = (2, 8, 7)(3, 5)(4, 12, 11)(6, 10, 9),$$

  denoted $O_{12,2}$, *the union of the* 12 *idempotents of* $\mathsf{OQ}(2)$;

- 4 *subquasigroups of order* 12 *isomorphic to* $(M(S_3), *)$ *with multiplication* $x * y = xf \cdot yf^{-1}$, *where*

$$f = (3, 5)(7, 9, 11)(8, 12, 10),$$

  denoted $O_{12,3}$;

- *the improper subquasigroup* $\mathsf{OQ}(2)$.

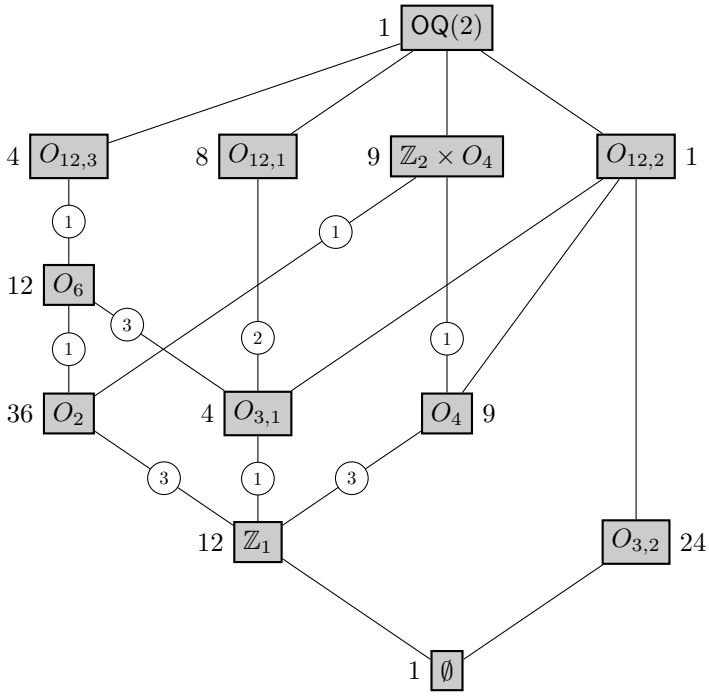

Figure 4: The Hasse diagram $\mathrm{Sub}(Q)/\mathrm{Aut}(Q)$ for $Q = \mathsf{OQ}(2)$.

The reduced Hasse diagram $\mathrm{Sub}(Q)/\mathrm{Aut}(Q)$ is depicted in Figure 4. The non-trivial edge labels not displayed in the figure are as follows:

$$h_{\leq,\equiv}(\mathbb{Z}_1, O_6) = 3\,; \qquad h_{\leq,\equiv}(\mathbb{Z}_1, \mathbb{Z}_2 \times O_4) = 3\,;$$
$$h_{\leq,\equiv}(\mathbb{Z}_1, O_{12,1}) = 2\,; \qquad h_{\leq,\equiv}(\mathbb{Z}_1, O_{12,3}) = 1\,;$$
$$h_{\leq,\equiv}(\mathbb{Z}_2, O_{12,3}) = 1\,; \qquad h_{\leq,\equiv}(O_{3,1}, O_{12,3}) = 1\,.$$

PROPOSITION 12.4. *The 8-element subquasigroups $\mathbb{Z}_2 \times O_4$ of $\mathsf{OQ}(2)$ are isomorphic to the semisymmetrization $\mathbb{Z}/_2^\Delta$ of the additive group $\mathbb{Z}/_2$.*

Proof. Consider row vectors $\mathbf{x}, \mathbf{y} \in \left(\mathbb{Z}/_2\right)^3$, i.e., bit strings of length 3. By [13, (2,2)], the multiplication in the semisymmetrization $\mathbb{Z}/_2^\Delta$ of the additive group $\mathbb{Z}/_2$ is given by $\mathbf{x}\mathrm{P} + \mathbf{y}\mathrm{P}^{-1}$ with

$$\mathrm{P} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

On the other hand, the multiplication in the quasigroup $\mathbb{Z}_2 \times O_4$ is given by $\mathbf{x}\mathrm{Q} + \mathbf{y}\mathrm{Q}^{-1}$ with

$$\mathrm{Q} = [1] \oplus \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

The matrix similarity $\mathrm{Q} = \mathrm{U}^{-1}\mathrm{P}\mathrm{U}$ with

$$\mathrm{U} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}.$$

then provides the required isomorphism. □

The *characteristic congruences* on semisymmetrizations of abelian groups are described in [13, §3]. Within $\mathbb{Z}/_2^\Delta$, two distinct bit strings of length 3 are related by the characteristic congruence if and only if they are complementary.

COROLLARY 12.5. *The 4-element subquasigroups O_4 of $\mathsf{PP}(2)$ and $\mathsf{OQ}(2)$ are isomorphic to the quotient of the semisymmetrization $\mathbb{Z}/_2^\Delta$ of the additive group $\mathbb{Z}/_2$ by its characteristic congruence.*

13 OPEN PROBLEMS

PROBLEM 13.1. Determine $\mathrm{Aut}(\mathsf{PSL}_{1+3}(F)) = \mathrm{Aut}(\mathsf{PP}(F))$ for fields F that are not perfect.

PROBLEM 13.2. Determine $\mathrm{Aut}(\mathsf{OQ}(F))$ for all fields F.

PROBLEM 13.3. Within the semisymmetric quasigroups $(\mathsf{PP}(F), \bullet)$ and $(\mathsf{OQ}(F), \bullet)$, which subquasigroups P carry a *semisymmetrized algebra* structure $(P, \bullet, \alpha)$ in the sense of [28, Definition 34], so that they form the semisymmetrization Q^Δ of a quasigroup Q?

- A necessary condition is that $|P|$ be a perfect cube.
- By Proposition 12.4, the 8-element subquasigroups of $\mathsf{OQ}(2)$ are isomorphic to $(\mathbb{Z}/_2, +)^\Delta$.

PROBLEM 13.4. Is every finite Okubo quasigroup $\mathsf{OQ}(q)$ generated by 2 elements?

- For a positive answer, it would remain to be shown that for $q \equiv 1 \pmod 3$, there are x, $y \in \mathsf{OQ}(q)$ such that $\langle x, y \rangle = \mathsf{OQ}(q)$.

ACKNOWLEDGMENT

The authors thank an anonymous referee for several useful comments that significantly improved the manuscript, especially for the second proof of Lemma 10.7. Petr Vojtěchovský was supported by the Simons Foundation Mathematics and Physical Sciences Collaboration Grant for Mathematicians no. 855097 and by the PROF grant of the University of Denver.

REFERENCES

[1] A.A. Albert and J. Thompson, "Two-element generation of the projective unimodular group," *Illinois J. Math.* 3 (1959), 421–439.

[2] E. Bannai and S.-Y. Song, "The character tables of Paige's simple Moufang loops and their relationship to the character tables of $\mathrm{PSL}(2,q)$," *Proc. London Math. Soc.* 58 (1989), 209–236.

[3] R.H. Bruck, *A Survey of Binary Systems*, Springer, Berlin, 1971.

[4] O. Chein, "Moufang loops of small order," *Mem. Amer. Math. Soc.* 13 (1978), no. 197.

[5] V. Chernousov, A. Elduque, M.-A. Knus and J.-P. Tignol, "Algebraic groups of type D_4, triality, and composition algebras," *Documenta Math.* 18 (2013), 413–468.

[6] J.A. Cuenca, A. Elduque and J.M. Pérez-Izquierdo, "Power associative composition algebras," *Manuscripta Math.* 103 (2000), no. 1, 77–90.

[7] J.D. Dixon and B. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics 163, Springer-Verlag, New York, 1996.

[8] A. Elduque, "Symmetric composition algebras," *J. Algebra.* 196 (1997), no. 1, 282–300.

[9] A. Elduque, "Okubo algebras: automorphisms, derivations and idempotents," pp. 61–73 in *Lie Algebras and Related Topics*, Contemp. Math. 652, Amer. Math. Soc., Providence, RI, 2015.

[10] S.M. Gagola, III and J.I. Hall, "Lagrange's theorem for Moufang loops," *Acta Sci. Math. (Szeged)* 71 (2005), 45–64.

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

[12] A.N. Grishkov and A.V. Zavarnitsine, "Lagrange's theorem for Moufang loops," *Math. Proc. Cambridge Philos. Soc.* 139 (2005), 41–57.

[13] B. Im, H.-J. Ko and J.D.H. Smith, "Semisymmetrizations of abelian group isotopes," *Taiwan J. Math.* 11 (2007), 1529–1534.

[14] N. Jacobson, *Lie Algebras*, Wiley, New York, NY, 1962.

[15] K.W. Johnson and J.D.H. Smith, "Characters of finite quasigroups," *Eur. J. Comb.* 5 (1984), 43–50.

[16] K.W. Johnson and J.D.H. Smith, "Characters of finite quasigroups III: quotients and fusion," *Eur. J. Comb.* 10 (1989), 47–56.

[17] K. Kunen, "Moufang quasigroups," *J. Algebra* 183 (1996), no. 1, 231–234.

[18] W. McCune, Mace4, `http://www.cs.unm.edu/~mccune/prover9`

[19] Ruth Moufang, "Zur Struktur von Alternativkörpern," *Math. Ann.* 110 (1935), no. 1, 416–430.

[20] G.P. Nagy and P. Vojtěchovský, LOOPS, version 3.4.1, package for GAP, `https://github.com/gap-packages/loops`

[21] G.P. Nagy and P. Vojtěchovský, "Automorphism groups of simple Moufang loops over perfect fields," *Math. Proc. Cambridge Philos. Soc.* 135 (2003), 193–197.

[22] G.P. Nagy and P. Vojtěchovský, "Octonions, simple Moufang loops and triality," *Quasigroups & Related Systems* 10 (2003), 65–93.

[23] S. Okubo, *Introduction to Octonion and Other Non-Associative Algebras in Physics*, Montroll Memorial Lecture Series in Mathematical Physics 2, Cambridge University Press, Cambridge, 1995.

[24] S. Okubo and J.M. Osborn, "Algebras with nondegenerate associative symmetric bilinear forms permitting composition," *Comm. Algebra* 9 (1981), 1233–1261.

[25] L.J. Paige, "A class of simple Moufang loops," *Proc. Amer. Math. Soc.* 7 (1956), 471–482.

[26] H.P. Petersson, "Eine Identität fünften Grades, der gewisse Isotope von Kompositions-Algebren genügen," *Math. Z.* 109 (1969), 217–238.

[27] J.D.H. Smith, *An Introduction to Quasigroups and Their Representations*, Chapman and Hall/CRC, Boca Raton, FL, 2007.

[28] J.D.H. Smith, "Quasigroup homotopies, semisymmetrization, and reversible automata," *Internat. J. Algebra Comput.* 18 (2008), 1203–1221.

[29] J.D.H. Smith, "Sylow theory for quasigroups," *J. Comb. Designs* 23 (2015), 115–133.

[30] J.D.H. Smith and A.B. Romanowska, *Post-Modern Algebra*, Wiley, New York, NY, 1999.

[31] S.-Y. Song, *The Character Tables of Certain Association Schemes*, Ph.D. thesis, The Ohio State University, 1987.

[32] P. Vojtěchovský, *Finite Simple Moufang Loops*, Ph.D. thesis, Iowa State University, 2001.

[33] P. Vojtěchovský, "Investigation of subalgebra lattices by means of Hasse constants," *Algebra Universalis* 50 (2003), 7–26.

[34] P. Vojtěchovský, "Generators for finite simple Moufang loops," *J. Group Theory* 6 (2003), 169–174.

[35] M. Zorn, "Alternativkörper und quadratische Systeme," *Abh. Math. Sem. Univ. Hamburg* 9 (1933), 395–402.

Department of Mathematics
Iowa State University
Ames, Iowa 50011
U.S.A.
jdhsmith@iastate.edu
jdhsmith.math.iastate.edu

Department of Mathematics
University of Denver
Denver, Colorado 80208
U.S.A.
petr@math.du.edu
www.math.du.edu/~petr