Proceedings of the Edinburgh Mathematical Society (2023) **66**, 1085–1109
doi:10.1017/S0013091523000585

ISOMORPHISMS OF QUADRATIC QUASIGROUPS

ALEŠ DRÁPAL[1] AND IAN M. WANLESS[2]

[1] *Department of Mathematics, Charles University, Prague, Czech Republic*
(drapal@karlin.mff.cuni.cz)
[2] *School of Mathematics, Monash University, Clayton Vic, Australia*
(ian.wanless@monash.edu)

(Received 18 February 2023)

Abstract Let $\mathbb{F}$ be a finite field of odd order and $a, b \in \mathbb{F} \setminus \{0, 1\}$ be such that $\chi(a) = \chi(b)$ and $\chi(1-a) = \chi(1-b)$, where χ is the extended quadratic character on $\mathbb{F}$. Let $Q_{a,b}$ be the quasigroup over $\mathbb{F}$ defined by $(x, y) \mapsto x + a(y - x)$ if $\chi(y - x) \geqslant 0$, and $(x, y) \mapsto x + b(y - x)$ if $\chi(y - x) = -1$. We show that $Q_{a,b} \cong Q_{c,d}$ if and only if $\{a, b\} = \{\alpha(c), \alpha(d)\}$ for some $\alpha \in \mathrm{Aut}(\mathbb{F})$. We also characterize $\mathrm{Aut}(Q_{a,b})$ and exhibit further properties, including establishing when $Q_{a,b}$ is a Steiner quasigroup or is commutative, entropic, left or right distributive, flexible or semisymmetric. In proving our results, we also characterize the minimal subquasigroups of $Q_{a,b}$.

Keywords: quasigroup; finite field; quadratic orthomorphism; automorphism group; quadratic nearfield; Steiner triple system; Netto system

2020 Mathematics subject classification: Primary 20N05
Secondary 05B05; 05B15

1. Main results

Throughout, $\mathbb{F}$ will be a finite field of odd order. A *quasigroup* Q is a set with a binary operation, say $\cdot$, such that the equations $x \cdot a = b$ and $a \cdot y = b$ have unique solutions for all $a, b \in Q$. Let $\chi : \mathbb{F} \to \{-1, 0, 1\}$ be the extended quadratic character, which satisfies $\chi(0) = 0$ and sends non-zero squares and non-squares to $+1$ and -1, respectively. For any $a, b \in \mathbb{F}$, there exists an operation $*$ on $\mathbb{F}$ such that

$$x * y = \begin{cases} x + a(y - x) & \text{if } \chi(y - x) \geqslant 0, \\ x + b(y - x) & \text{if } \chi(y - x) = -1. \end{cases} \tag{1.1}$$

This operation yields a quasigroup (see e.g. [8]) if and only if

$$\chi(a) = \chi(b) \neq 0 \quad \text{and} \quad \chi(1-a) = \chi(1-b) \neq 0. \tag{1.2}$$

If Condition (1.2) holds, then the quasigroup given by Condition (1.1) will be denoted by $Q_{a,b}$. A finite quasigroup isomorphic to a quasigroup $Q_{a,b}$ is said to be *quadratic*. Note that quadratic quasigroups are *idempotent*, i.e., they satisfy the law $xx = x$.

Quadratic quasigroups have many applications, including the construction of mutually orthogonal Latin squares [7, 8], atomic Latin squares [14], Falconer varieties [1], perfect 1-factorizations of graphs [1, 9, 14] and maximally non-associative quasigroups [5]. A question raised by [5] was to understand when two quadratic quasigroups are isomorphic. Our first main result answers this question:

Theorem 1.1. *Let $Q_{a,b}$ and $Q_{c,d}$ be quadratic quasigroups over $\mathbb{F}$. Then $Q_{a,b} \cong Q_{c,d}$ if and only if there exists $\alpha \in \mathrm{Aut}(\mathbb{F})$ such that $\{a, b\} = \{\alpha(c), \alpha(d)\}$.*

In [14], it was noted that quadratic quasigroups have rich automorphism groups. Our second major goal is to fully understand these groups. We start by defining the following groups:

- $\mathrm{A\Gamma L}_1(\mathbb{F})$ is the group of all *affine semilinear mappings* $x \mapsto \lambda\alpha(x) + \mu$, where $\lambda \in \mathbb{F}^*$, $\mu \in \mathbb{F}$ and $\alpha \in \mathrm{Aut}(\mathbb{F})$.
- $\mathrm{A\Gamma L}_1(\mathbb{F} \,|\, \mathbb{K})$ is the subgroup of $\mathrm{A\Gamma L}_1(\mathbb{F})$ in which the automorphism $\alpha \in \mathrm{Aut}(\mathbb{F})$ fixes every element of a subfield $\mathbb{K}$ of $\mathbb{F}$ (in other words, $\alpha \in \mathrm{Gal}(\mathbb{F} \,|\, \mathbb{K})$).
- $\mathrm{A\Gamma^2L}_1(\mathbb{F})$ is the subgroup of $\mathrm{A\Gamma L}_1(\mathbb{F})$ consisting of all maps $x \mapsto \lambda\alpha(x) + \mu$ such that $\chi(\lambda) = 1$.
- $\mathrm{A\Gamma^2L}_1(\mathbb{F} \,|\, \mathbb{K}) = \mathrm{A\Gamma^2L}_1(\mathbb{F}) \cap \mathrm{A\Gamma L}_1(\mathbb{F} \,|\, \mathbb{K})$.

The index of $\mathrm{A\Gamma^2L}_1(\mathbb{F} \,|\, \mathbb{K})$ in $\mathrm{A\Gamma L}_1(\mathbb{F} \,|\, \mathbb{K})$ is equal to two. If there exists a subfield $\mathbb{L}$ such that $[\mathbb{K} : \mathbb{L}] = 2$, then it is possible to construct another group of affine semilinear mappings in which $\mathrm{A\Gamma^2L}_1(\mathbb{F} \,|\, \mathbb{K})$ forms a subgroup of index two. This group is said to be a *twist* of $\mathrm{A\Gamma L}_1(\mathbb{F}|\mathbb{K})$. It is denoted by $\mathrm{A\Gamma L}_1^{\mathrm{tw}}(\mathbb{F} \,|\, \mathbb{K})$ and consists of $\mathrm{A\Gamma^2L}_1(\mathbb{F}|\mathbb{K})$ and all mappings

$$x \mapsto \lambda\alpha(x^\gamma) + \mu, \quad \text{where } \chi(\lambda) = -1,\ \alpha \in \mathrm{Gal}(\mathbb{F}|\mathbb{K}),\ \mu \in \mathbb{F} \text{ and } \gamma = |\mathbb{L}|.$$

Theorem 1.2. *Let $Q = Q_{a,b}$ be a quadratic quasigroup over $\mathbb{F}$. Denote by $\mathbb{K}$ the least subfield of $\mathbb{F}$ that contains $\{a, b\}$. The automorphism group of Q is equal to $\mathrm{A\Gamma^2L}_1(\mathbb{F}|\mathbb{K})$ up to these exceptions:*

(i) *If $a = b$, then $\mathrm{Aut}(Q) \cong \mathrm{AGL}_k(\mathbb{K})$, where $k = [\mathbb{F} : \mathbb{K}]$. The automorphisms of Q are all mappings $x \mapsto \sigma(x) + \mu$, where $\mu \in \mathbb{F}$ and $\sigma\colon \mathbb{F} \to \mathbb{F}$ is a $\mathbb{K}$-linear bijection.*
(ii) *If there is an integer γ such that $b = a^\gamma$ and $\gamma^2 = |\mathbb{K}|$, then $\mathrm{Aut}(Q) = \mathrm{A\Gamma L}_1^{\mathrm{tw}}(\mathbb{F}|\mathbb{K})$.*
(iii) *If $|\mathbb{F}| = 7$ and $\{a, b\} = \{3, 5\}$, then $\mathrm{Aut}(Q) \cong \mathrm{PSL}_2(7)$.*

The proof of Theorem 1.2 leads us to examine several varieties of quasigroups, and it becomes important to understand which quadratic quasigroups those varieties contain. This leads to our third main result:

Theorem 1.3. *Let $Q = Q_{a,b}$ be a quadratic quasigroup over $\mathbb{F}$. Then*

(i) *Q is entropic (i.e. fulfils the law $xy \cdot uv = xu \cdot yv$) if and only if $a = b$;*
(ii) *Q is left distributive (i.e. fulfils the law $x \cdot yz = xy \cdot xz$) if and only if $a = b$;*
(iii) *Q is right distributive (i.e. fulfils the law $xy \cdot z = xz \cdot yz$) if and only if $a = b$;*
(iv) *Q is commutative if and only if $a + b = 1$ and either $|\mathbb{F}| \equiv 3 \bmod 4$ or $a = b$.*
(v) *Q is flexible (i.e. fulfils the law $x \cdot yx = xy \cdot x$) if and only if $a = b$ or $\chi(a) = \chi(1-a) = 1$ or both $a + b = 1$ and $|\mathbb{F}| \equiv 3 \bmod 4$;*
(vi) *Q is semisymmetric (i.e. fulfils the law $xy \cdot x = y$) if and only if $a^2 - a + 1 = 0$ and either $a = b$ or $a + b = 1$.*
(vii) *Q is a Steiner quasigroup (i.e. idempotent, commutative and semisymmetric) if and only if either $\mathrm{char}(\mathbb{F}) = 3$ and $a = b = -1$, or $\mathrm{char}(\mathbb{F}) > 3$, $a + b = ab = 1$ and $\chi(a) = \chi(-1) = -1$. In the latter case, $a \neq b$.*
(viii) *Q is isotopic to a group if and only if $a = b$.*

Another outcome from our work is a precise characterization of all minimal subquasigroups of quadratic quasigroups $Q_{a,b}$. See Theorems 5.4 and 5.5.

Regarding Theorem 1.3(i), we note that entropic quasigroups are also sometimes called *medial*.

Regarding Theorem 1.3(vii), we make the following remarks. If $\mathrm{char}(\mathbb{F}) = 3$, then $Q_{a,b}$ is Steiner if and only if $a = b = -1$. Steiner quadratic quasigroups in characteristic 3 thus coincide with affine STSs. If $\mathrm{char}(\mathbb{F}) > 3$, then $Q_{a,b}$ is a Steiner quasigroup if and only if $a + b = 1 = ab$ and $\chi(a) = \chi(b) = \chi(-1) = -1$. An easy number theoretical argument shows that this happens if and only if $|\mathbb{F}| = p^k$ for a prime $p \equiv 7 \bmod 12$ and odd $k \geqslant 1$, and a and b are distinct primitive sixth roots of unity. Blocks of the STS are the sets $\{u, v, av + bu\}$, where $\chi(v - u) = 1$. These STSs are known as *Netto systems*, and we refer to the corresponding quasigroups as *Netto quasigroups*. Robinson [11] proved that their automorphism group is equal to $\mathrm{A\Gamma^2L_1}(\mathbb{F})$, with the exception of order 7, which yields the Fano plane – and thus also Theorem 1.2(iii).

Say that a quadratic quasigroup $Q = Q_{a,b}$ is *twisted* if $b = a^\gamma$, where γ^2 is the order of the least subfield of $\mathbb{F}$ containing the element a. The exceptional cases of Theorem 1.2 may thus be labelled entropic, twisted and Fano. It is immediately clear that these are the only cases in which $\mathrm{Aut}(Q)$ is 2-transitive.

Twisted quadratic quasigroups are closely related to quasigroups constructed from quadratic nearfields. The axioms of a (left) *nearfield* $(N, +, \circ, 0, 1)$ stipulate that $(N, +, 0)$ is an abelian group, $(N \setminus \{0\}, \circ, 1)$ is a group, $0 \circ x = 0 = x \circ 0$ for all $x \in N$ and $x \circ (y + z) = x \circ y + x \circ z$, for all $x, y, z \in N$. A *quadratic nearfield* is defined over a field $\mathbb{F}_{q^2}$, where q is a power of an odd prime, by

$$x \circ y = \begin{cases} xy & \text{if } \chi(x) \geqslant 0; \\ xy^q & \text{if } \chi(x) = -1. \end{cases} \tag{1.3}$$

With each element $c \notin \{0, 1\}$ of a nearfield N, there may be associated a quasigroup $(N, *_c)$ for which

$$x *_c y = x + (y - x) \circ c \quad \text{whenever } x, y \in N. \tag{1.4}$$

https://doi.org/10.1017/S0013091523000585 Published online by Cambridge University Press

Stein [12] showed that each of the mappings $x \mapsto \lambda \circ x + \mu$, where $\lambda \in N \setminus \{0\}$ and $\mu \in N$, is an automorphism of $(N, *_c)$. For background on nearfields, see [13].

The notation $(\mathbb{F}_{q^2}, *_c)$ will always refer to the quasigroup built by means of Condition (1.4) over the quadratic nearfield that is defined on $\mathbb{F}_{q^2}$ by Condition (1.3). These quasigroups may also be obtained by means of Condition (1.1) as quadratic quasigroups:

Proposition 1.4. *Suppose that* $|\mathbb{F}| = q^2$ *and that* $a \in \mathbb{F} \setminus \{0, 1\}$. *Then* $Q_{a,a^q} = (\mathbb{F}_{q^2}, *_a)$ *and* $Q_{a^q,a} = (\mathbb{F}_{q^2}, *_{a^q})$. *The mapping* $x \mapsto x^q$ *yields an isomorphism* $(\mathbb{F}_{q^2}, *_a) \cong (\mathbb{F}_{q^2}, *_{a^q})$.

Proof. We use $*$ to denote the operation of Q_{a,a^q}. If $y - x$ is a square, then $x * y = x + (y - x)a = x + (y - x) \circ a = x *_a y$. If $y - x$ is a non-square, then $x * y = x + (y - x)a^q = x + (y - x) \circ a = x *_a y$, for all $x, y \in \mathbb{F}$. It follows that $Q_{a,a^q} = (\mathbb{F}_{q^2}, *_a)$, and then by substituting a^q for a, we find that $Q_{a^q,a} = (\mathbb{F}_{q^2}, *_{a^q})$. The fact that $x \mapsto x^q$ is an isomorphism $Q_{a,a^q} \cong Q_{a^q,a}$ was shown in [14] (and also follows from Proposition 2.1). □

Let us briefly outline the content of the following sections. Section 2 consists of straightforward arguments that establish Theorem 1.3. To avoid repeating the same condition, let us assume in the rest of this overview that $Q = Q_{a,b}$ is a quadratic quasigroup defined on the field $\mathbb{F} = \mathbb{F}_q$ by means of Condition (1.1) such that $a \neq b$ and such that Q is not a Steiner quasigroup.

The main achievement of Section 3 is Proposition 3.4, which shows that every subquasigroup of Q containing 0 is closed under the addition of $\mathbb{F}$. Section 4 starts by investigating the situation when there exists an additive $\varphi \in \mathrm{Aut}(Q)$ such that $\varphi(1)$ is a non-square in $\mathbb{F}$. Several technical results are needed to obtain Proposition 4.5 by which the latter condition implies that Q is twisted. That suffices to prove Theorem 1.2 for the case of Q being 2-generated. That is done in Theorem 4.7. The structure of $\mathrm{Aut}(Q)$ is then used to establish, in Theorem 4.8, the validity of Theorem 1.1 when Q is 2-generated.

Assume now that Q is not 2-generated. Call a subquasigroup minimal if it consists of more than one element and has no proper subquasigroup with more than one element. Section 5 is devoted to the description of minimal subquasigroups of Q and of 2-generated subquasigroups of Q. This is achieved in Theorems 5.4 and 5.5. It turns out that such subquasigroups may be used to get a structure of affine lines belonging to a subfield of $\mathbb{F}$. Since an automorphism of Q has to respect such a structure, it has to be induced by semilinear mappings (Proposition 5.8). It turns out that such a mapping has to be linear in many cases (Proposition 6.2) and that allows us, by an application of a theorem of Carlitz, to confirm the structure of $\mathrm{Aut}(Q)$ as described in Theorem 1.2. Knowledge of $\mathrm{Aut}(Q)$ is then used to prove Theorem 1.1 in its general form.

2. Varieties of quadratic quasigroups

This section is primarily aimed at proving Theorem 1.3. The proof is split between Lemmas 2.3–2.8 below. Let $Q = Q_{a,b}$ be a quadratic quasigroup over $\mathbb{F}$. We wish to give easily checkable conditions on a, b under which Q is entropic, left or right distributive, commutative, flexible, semisymmetric or totally symmetric. Note that totally symmetric is a term describing the combination of commutative and semisymmetric. Steiner quasigroups are precisely those that are idempotent and totally symmetric.

https://doi.org/10.1017/S0013091523000585 Published online by Cambridge University Press

We start with some basic properties of quadratic quasigroups. If $(Q,*)$ is a quasigroup, then the *opposite* and the *translate* of $(Q,*)$ are, respectively, the quasigroups $(Q,\circ)$ and $(Q,\otimes)$ defined by $x*y=z \Leftrightarrow y\circ x=z \Leftrightarrow z\otimes x=y$. The following statement, with the exception of points (vii) and (viii), is immediate from [14].

Proposition 2.1. *Let $Q_{a,b}$ be a quadratic quasigroup over $\mathbb{F}$.*

(i) *$Q_{a,b}$ is idempotent.*
(ii) *For any $f\in\mathbb{F}$, the map $x\mapsto x+f$ is an automorphism of $Q_{a,b}$.*
(iii) *For any non-zero square $c\in\mathbb{F}$, the map $x\mapsto cx$ is an automorphism of $Q_{a,b}$.*
(iv) *$Q_{a,b}$ is isomorphic to $Q_{b,a}$ by the map $x\mapsto\zeta x$, where ζ is any non-square in $\mathbb{F}$.*
(v) *The opposite quasigroup of $Q_{a,b}$ is $Q_{1-a,1-b}$ if $|\mathbb{F}|\equiv 1 \bmod 4$ and $Q_{1-b,1-a}$ if $|\mathbb{F}|\equiv 3 \bmod 4$.*
(vi) *The translate of $Q_{a,b}$ is $Q_{(a-1)/a,(b-1)/b}$ if $\chi(a)=\chi(-1)$ and $Q_{(b-1)/b,(a-1)/a}$ if $\chi(a)\neq\chi(-1)$.*
(vii) *If $a\neq b$ and ζ is a non-square in $\mathbb{F}$, then $\zeta(x*y)\neq(\zeta x)*(\zeta y)$ for all distinct $x,y\in\mathbb{F}$.*
(viii) *If $\alpha\in\mathrm{Aut}(\mathbb{F})$, then α induces an automorphism between $Q_{a,b}$ and $Q_{\alpha(a),\alpha(b)}$.*

Proof. To prove (vii), consider $x,y\in\mathbb{F}$. If $\chi(y-x)=1$, then $\zeta(x*y)=\zeta x+a\zeta(y-x)$, while $\zeta x*\zeta y=\zeta x+b\zeta(y-x)$. If $\chi(y-x)=-1$, then $\zeta(x*y)=\zeta x+b\zeta(y-x)$, while $\zeta x*\zeta y=\zeta x+a\zeta(y-x)$.

To prove (viii), note that $\chi(y-x)=\chi(\alpha(y-x))=\chi(\alpha(y)-\alpha(x))$ for all $x,y\in Q$. Hence, $x*y=x+a(y-x)$ in $Q_{a,b}$ if and only if

$$\alpha(x)*\alpha(y)=\alpha(x)+\alpha(a)(\alpha(y)-\alpha(x))=\alpha(x*y)$$

in $Q_{\alpha(a),\alpha(b)}$. The argument remains true if a is replaced by b, so $\alpha(x)*\alpha(y)=\alpha(x*y)$ in all cases. □

Lemma 2.2. *Suppose $\mathbb{F}$ is a finite field of odd order $|\mathbb{F}|>9$. Then there exist $u,v\in\mathbb{F}$ such that $\chi(u)=\chi(v)=\chi(u+1)=\chi(v+1)=\chi(u-1)=-1$ and $\chi(v-1)=1$.*

Proof. The statement is concerned with two special cases of a more general problem that asks if for $\varepsilon_i\in\{-1,1\}$, $-1\leqslant i\leqslant 1$, there exists $x\in\mathbb{F}$ such that $\chi(x+i)=\varepsilon_i$. A consequence of Weil's bound (e.g., as stated in [6, Theorem 1.6]) implies that such an x exists if

$$2^{-3}q-(3/2)(\sqrt{q}+1)+\sqrt{q}(1-2^{-3})>0,$$

where $q=|\mathbb{F}|$. This is true for each prime power $q>43$. For prime values $q=11$, 13, 17, 19, 23, 29, 31, 37, 41 and 43, put $u=7$, 6, 6, 13, 20, 11, 12, 14, 12 and 19, respectively. For $q=25$, set $u=2\sqrt{2}$. In all these cases, set $v=u-1$. For $q=27$, set $u=x$ and $v=2x^2$ in $\mathbb{F}_3[x]/(x^3+2x+1)$. □

Lemma 2.3. *Suppose that $Q=Q_{a,b}$ is a quadratic quasigroup over $\mathbb{F}$. Then Q is isotopic to a group if and only if $a=b$.*

Proof. First suppose that $a=b$, so that $(Q,*)$ is defined by $x*y=(1-a)x+ay$ for all $x,y\in\mathbb{F}$. So Q is isotopic to the additive group of $\mathbb{F}$.

For the remainder of this proof, suppose that $a\neq b$. We use the well known quadrangle criterion (see e.g. [8]) to show that Q is not isotopic to any group. This criterion states that if Q is isotopic to a group and $r_1,r_2,c_1,c_2,r_1',r_2',c_1',c_2'$ are any elements of Q such that $r_1*c_1=r_1'*c_1'$, $r_1*c_2=r_1'*c_2'$ and $r_2*c_1=r_2'*c_1'$, then it follows that $r_2*c_2=r_2'*c_2'$. For $|\mathbb{F}|=7$, we apply this criterion to the following quadrangles in $Q_{3,5}$:

$$\begin{array}{c|cc} * & 0 & 1 \\ \hline 0 & 0 & 3 \\ 1 & 3 & 1 \end{array} \qquad \begin{array}{c|cc} * & 6 & 5 \\ \hline 2 & 0 & 3 \\ 4 & 3 & 0 \end{array}$$

It follows that $Q_{3,5}$ (and also, by Proposition 2.1(iv), its isomorph $Q_{5,3}$) is not isotopic to a group.

Similarly, for $|\mathbb{F}|=9$, the following quadrangles

$$\begin{array}{r|cc} * & 1 & 2i \\ \hline 1 & 1 & 2 \\ 1+i & 2 & 1 \end{array} \qquad \begin{array}{r|cc} * & 2+i & 2+2i \\ \hline 1+2i & 1 & 2 \\ i & 2 & 0 \end{array}$$

show that $Q_{1+i,1+2i}$ is not isotopic to any group (where $i=\sqrt{-1}$). This property is necessarily inherited by the opposite quasigroup $Q_{2i,i}$ and translate $Q_{2+i,2+2i}$, as well as by $Q_{1+2i,1+i}$, $Q_{i,2i}$ and $Q_{2+2i,2+i}$. There are no other solutions to Condition (1.2) for $|\mathbb{F}|\leqslant 9$.

If $|\mathbb{F}|>9$, then let $u,v\in\mathbb{F}$ be as given by Lemma 2.2. For such u,v, we have the following violation of the quadrangle criterion:

$$\begin{array}{r|cc} * & u-bu & u-bu+1 \\ \hline -bu & 0 & b \\ 1-bu & 1-b & 1 \end{array} \qquad \begin{array}{r|cc} * & v-bv & v-bv+1 \\ \hline -bv & 0 & b \\ 1-bv & 1-a & 1 \end{array}$$

□

Lemma 2.4. *Let $Q=Q_{a,b}$ be a quadratic quasigroup over $\mathbb{F}$. If -1 is a square, then Q is commutative if and only if $a=b=1/2$. If -1 is a non-square, then Q is commutative if and only if $a+b=1$.*

Proof. We use Proposition 2.1(v). If $|\mathbb{F}|\equiv 1 \bmod 4$, then $Q_{a,b}$ is commutative if and only if $a=1-a$ and $b=1-b$. If $|\mathbb{F}|\equiv 3 \bmod 4$, then $Q_{a,b}$ is commutative if and only if $a=1-b$ and $b=1-a$. The result follows. □

Lemma 2.5. *Let $Q=Q_{a,b}$ be a quadratic quasigroup over $\mathbb{F}$. The quasigroup Q is entropic (or left distributive or right distributive) if and only if $a=b$.*

Proof. If $a=b$, then Q is entropic (this is a well-known fact that may be verified directly). Idempotent entropic quasigroups are left distributive since an idempotent entropic quasigroup fulfils $x\cdot yz=xx\cdot yz=xy\cdot xz$. By Proposition 2.1(v), it thus suffices to assume that Q is left distributive and show that then $a=b$.

https://doi.org/10.1017/S0013091523000585 Published online by Cambridge University Press

Since the number of squares in $\mathbb{F}$ exceeds $|\mathbb{F}|/2$, the squares cannot form a subquasigroup of Q. Hence, there exist squares $x, y \in \mathbb{F}$ such that $x * y$ is a non-square. By Condition (1.1), $0 * (x * y) = b(x * y)$. If a is a square, then $(0 * x) * (0 * y) = ax * ay = a(x * y)$, by Proposition 2.1(iii). Thus, in this case, the left distributivity clearly implies $a = b$. If a is a non-square, then b is a non-square too. If $a \neq b$, then $0 * (x * y) = b(x * y) \neq bx * by = (0 * x) * (0 * y)$ by Proposition 2.1(vii). □

A quasigroup $(M, \circ)$ is said to be *affine* if $x \circ y = x + \varphi(y - x)$ for all $x, y \in M$, where $\varphi \in \mathrm{Aut}(M)$ for some abelian group defined on M. An affine quasigroup is isotopic to the abelian group $(M, +)$ since $x \circ y = (1 - \varphi)(x) + \varphi(y)$. By Lemma 2.3, $Q_{a,b}$ is isotopic to a group if and only if $a = b$. If $a = b$, then $Q_{a,b}$ is affine. We will say that $Q_{a,b}$ is *non-affine* if $a \neq b$.

Lemma 2.6. *Let $Q = Q_{a,b}$ be a quadratic quasigroup over $\mathbb{F}$. The quasigroup Q is semisymmetric if and only if $a^2 - a + 1 = 0$ and either $a = b$ or $a + b = 1$.*

Proof. We use Proposition 2.1(vi) and the fact that $Q_{a,b}$ is semisymmetric if and only if it equals its translate. First suppose that $\chi(a) \neq \chi(-1)$. Then $Q_{a,b}$ equals its translate if and only if $a - 1 = ab = b - 1$, which is equivalent to $a = b = a^2 + 1$. Next suppose that $\chi(a) = \chi(-1)$. Then $Q_{a,b}$ equals its translate if and only if a, b are both solutions to $x = (x - 1)/x$. There are two possibilities. The first is that $a = b = a^2 + 1$. The second is that a, b are the two distinct roots of $x^2 - x + 1 = 0$, in which case $a + b = 1$. The result now follows from the observation that if $a^2 - a + 1 = 0$ and $a + b = 1$, then $\chi(a) = \chi(b) = \chi(-a^2) = \chi(-1)$. □

Lemma 2.7. *Let $Q = Q_{a,b}$ be a quadratic quasigroup over $\mathbb{F}$. If $\mathrm{char}(\mathbb{F}) = 3$, then Q is a Steiner quasigroup if and only if $a = b = -1$. In such a case, Q is induced by an affine STS. If $\mathrm{char}(\mathbb{F}) \neq 3$, then Q is a Steiner quasigroup if and only if $ab = 1 = a + b$ and -1 is a non-square. In such a case, we have $a \neq b$,*

$$\begin{aligned} ab = a + b = a - a^2 = b - b^2 = -a^3 = -b^3 = 1 \ \textit{and} \\ \chi(a) = \chi(b) = \chi(1 - a) = \chi(1 - b) = \chi(-1) = -1. \end{aligned} \tag{2.1}$$

If $Q_{a,b}$ is a non-affine Steiner quasigroup, then $Q_{c,d}$ is another non-affine quadratic Steiner quasigroup over $\mathbb{F}$ if and only if $\{a, b\} = \{c, d\}$. In such a case, $Q_{a,b} \cong Q_{c,d}$.

Proof. Since total symmetry is the combination of semi-symmetry with commutativity, we combine Lemmas 2.6 and 2.4. Together they imply that the necessary and sufficient conditions for total symmetry are that at least one of

$$a^2 - a + 1 = 0 \quad \text{and} \quad a = b = 1/2, \text{ or} \tag{2.2}$$

$$a^2 - a + 1 = 0 \quad \text{and} \quad a + b = 1 \quad \text{and} \quad \chi(-1) = -1 \tag{2.3}$$

holds. Condition (2.2) implies that $3/4 = 0$, so it can only be achieved if $\mathrm{char}(\mathbb{F}) = 3$. Moreover, if $\mathrm{char}(\mathbb{F}) = 3$, then Condition (2.2) is equivalent to $a = b = -1$.

https://doi.org/10.1017/S0013091523000585 Published online by Cambridge University Press

Condition (2.3) implies that $a(1-b)-a=-1$ and hence $ab=1$. Moreover, if $ab=1$ and $a+b=1$, then $a^2=a(1-b)=a-1$. The characterization of quadratic Steiner quasigroups follows.

Assume Condition (2.3) holds. Then $b-b^2=b(1-b)=(1-a)a=1$. So a,b are both roots of $x^2-x+1=0$ and hence also of $x^3+1=(x+1)(x^2-x+1)=0$. From $a^3=b^3=-1$ and $a+b=1$, we get $\chi(a)=\chi(b)=\chi(-1)=\chi(1-b)=\chi(1-a)$.

The polynomial x^2-x+1 has at most two roots (these roots coincide if and only if $\mathrm{char}(\mathbb{F})=3$). That explains why $\{a,b\}=\{c,d\}$ if $Q_{a,b}$ and $Q_{c,d}$ are Steiner quadratic quasigroups on $\mathbb{F}$, with $a\neq b$ and $c\neq d$. If $\{a,b\}=\{c,d\}$, then $Q_{a,b}\cong Q_{c,d}$ by Proposition 2.1(iv). □

For the next proof, we define notation θ_x by $\theta_x=a$ if $\chi(x)=1$ and $\theta_x=b$ if $\chi(x)=-1$. Note that $\theta_a=\theta_b$ and $\theta_{1-a}=\theta_{1-b}$ for any quadratic quasigroup $Q_{a,b}$.

Lemma 2.8. *The quadratic quasigroup $Q=Q_{a,b}$ is flexible if and only if at least one of the following conditions holds:*

(i) $a=b$,
(ii) $\chi(a)=\chi(1-a)=1$, *or*
(iii) $a+b=1$ *and* $|\mathbb{F}|\equiv 3 \bmod 4$.

Proof. First note that $x*(x*x)=x*x=(x*x)*x$ for all $x\in\mathbb{F}$, by idempotence. Thus, consider distinct $x,y\in\mathbb{F}$ and let $z=x-y$. Then

$$x*(y*x)=x*(y+\theta_z z)=x+\theta_{z(a-1)}z(\theta_z-1),$$

and

$$(x*y)*x=(x-\theta_{-z}z)*x=x-\theta_{-z}z+\theta_{az}\theta_{-z}z=x+\theta_{-z}z(\theta_{az}-1).$$

It follows that Q is flexible if and only if

$$\theta_{z(a-1)}(\theta_z-1)=\theta_{-z}(\theta_{az}-1) \tag{2.4}$$

for all z. Both sides of Condition (2.4) are members of $\Phi=\{a(a-1),a(b-1),b(a-1),b(b-1)\}$. If $a=b$, then $|\Phi|=1$, so Condition (2.4) is automatically satisfied. Henceforth, we assume $a\neq b$. In this case, $|\Phi|=4$ unless $a(a-1)=b(b-1)$, which requires $a=1-b$.

Suppose for the moment that $\chi(z)=1$, meaning that Condition (2.4) is equivalent to $\theta_{a-1}(a-1)=\theta_{-1}(\theta_a-1)$. From the above observations, this condition can only be satisfied if

$$\theta_{a-1}=\theta_{-1} \quad \text{and} \quad \theta_a=a, \text{ or} \tag{2.5}$$

$$a=1-b \quad \text{and} \quad \theta_{a-1}=a \quad \text{and} \quad \theta_{-1}=\theta_a=b. \tag{2.6}$$

Now Condition (2.5) is equivalent to condition (ii), whereas Condition (2.6) implies (iii). It follows that for $Q_{a,b}$ to be flexible, it is necessary that (i), (ii) or (iii) holds.

To check sufficiency, we first note that if (iii) is true, then $\chi(a) = \chi(1-a)$, so either (ii) or Condition (2.6) holds. Hence, if (ii) or (iii) holds, then at least one of Conditions (2.5) or (2.6) holds. Moreover, Condition (2.5) implies that $\theta_{z(a-1)} = \theta_{-z}$ and $\theta_z = \theta_{az}$, whereas Condition (2.6) implies that $\theta_{-z} = 1 - \theta_z$ and $\theta_{az} = \theta_{(1-a)z} = 1 - \theta_{z(a-1)}$. In either case, Condition (2.4) holds for all z. □

We note in passing that idempotent entropic quasigroups are always flexible because $x(yx) = (xx)(yx) = (xy)(xx) = (xy)x$. Commutative quasigroups are flexible too because $x(yx) = (yx)x = (xy)x$. These two facts support the observation that the conditions encountered in Lemmas 2.5 and 2.4 are incorporated in Lemma 2.8.

3. Subquasigroups and affine automorphisms

If Q is an idempotent quasigroup, then the term *trivial subquasigroup* refers to a quasigroup consisting of at most one element. A *minimal subquasigroup* is a non-trivial subquasigroup in which all proper subquasigroups are trivial. A 2*-generated subquasigroup* is a subquasigroup S for which there exists $A \subseteq S$ such that $|A| \leqslant 2$ and S is the smallest subquasigroup of Q that contains A. Any 2-element subset of a minimal subquasigroup S generates S. However, there may exist non-trivial 2-generated subquasigroups that are not minimal.

The field $\mathbb{F}$ is a vector space over its prime field. Saying that $U \subseteq \mathbb{F}$ is a *subspace* (of $\mathbb{F}$) means that it is a subspace of that vector space.

The purpose of this section is to show that if $Q_{a,b}$ is not a Steiner quasigroup, then each minimal subquasigroup of $Q_{a,b}$ is formed by a coset of a subspace of $\mathbb{F}$. In particular, if a minimal subquasigroup contains zero, then it is closed under addition.

We start by two auxiliary observations that concern Frobenius groups.

Lemma 3.1. *Let G be a Frobenius group that acts naturally on a finite set Ω. If G_ω contains at most two non-trivial orbits for some $\omega \in \Omega$, then the Frobenius kernel of G is an elementary abelian group.*

Proof. Put $n = |\Omega|$. By the assumptions there exists an orbit Γ of G_ω such that $|\Gamma| + 1 > n/2$. This implies that G is primitive. Now, elements of Ω may be identified with elements of a group N (which is isomorphic to the Frobenius kernel), and G_ω may be identified with a subgroup of $\mathrm{Aut}(N)$. Since there are at most two nontrivial orbits of G_ω, there are at most two integers that occur as an order of a non-trivial element of N. One of these integers has to be a prime, and the other (if it exists) is either a square of this prime or another prime. This means that N is solvable. A finite solvable group is either elementary abelian or it contains a non-trivial proper characteristic subgroup. However, such a subgroup yields a block $B \subseteq \Omega$. That is not possible since G is primitive. □

Lemma 3.2. *Let G be a Frobenius group that acts naturally on a finite set Ω. Suppose that the Frobenius complement of G is abelian. If $\alpha, \beta \in \Omega$, $\alpha \neq \beta$, $\varphi \in G_\alpha$, $\psi \in G_\beta$ and $\mathrm{id}_\Omega \notin \{\varphi, \psi\}$, then $[\varphi, \varphi^\psi]$ is fixed point free.*

Proof. Denote by N the Frobenius kernel of G and recall that non-identity elements of N act without fixed points. Since G/N is abelian, we must have $[g,h] \in N$ for any $g,h \in G$. To prove that $[g,h]$ is fixed point free, it therefore suffices to find any $\omega \in \Omega$ such that $gh(\omega) \neq hg(\omega)$. We take $\omega = \psi^{-1}(\alpha)$ and observe that

$$\varphi\varphi^{\psi}(\omega) = \varphi\omega \quad \text{and} \quad \varphi^{\psi}\varphi(\omega) = \psi^{-1}\varphi\psi(\varphi\omega).$$

Suppose that $\psi(\varphi\omega) = \varphi\psi(\varphi\omega)$. By definition, α is the only fixed point of φ and β is the only fixed point of ψ, so we can deduce in turn that $\psi(\varphi\omega) = \alpha$, $\varphi\omega = \omega$, $\omega = \alpha$, $\psi(\alpha) = \alpha$ and thus $\alpha = \beta$. This contradiction proves that $\varphi\varphi^{\psi}(\omega) \neq \varphi^{\psi}\varphi(\omega)$, from which the result follows. □

A mapping $x \mapsto ux + v$, with $u \in \mathbb{F}^*$ and $v \in \mathbb{F}$, is said to be an *affine permutation* of $\mathbb{F}$. Affine permutations form a sharply 2-transitive group. Those with u a square form a subgroup of $\mathrm{Aut}(Q)$, for any quadratic quasigroup $Q = Q_{a,b}$ over $\mathbb{F}$, by Proposition 2.1(ii),(iii). Hence, we have:

Proposition 3.3. *Suppose that $Q = Q_{a,b}$ is a quadratic quasigroup over $\mathbb{F}$. Let $s,t,u,v \in \mathbb{F}$ be such that $\chi(s-t) = \chi(u-v)$. Then there exists an affine automorphism $\alpha \in \mathrm{Aut}(Q)$ such that $\alpha(s) = u$ and $\alpha(t) = v$.*

Proof. If $s=t$, then $u=v$, so we may use $x \mapsto x + u - s$ for α. So assume $t \neq s$, meaning that $u \neq v$ as well. Put $\lambda = (u-v)/(s-t)$ and $\mu = (vs - ut)/(s-t)$. The mapping $x \mapsto \lambda x + \mu$ is an automorphism of $Q_{a,b}$ that sends s to u and t to v. □

Proposition 3.4. *Suppose that $Q = Q_{a,b}$. If $\mathrm{char}(\mathbb{F}) = 3$, then each minimal subquasigroup of Q is a coset of a subspace of $\mathbb{F}$. If $\mathrm{char}(\mathbb{F}) \neq 3$, then each minimal subquasigroup of Q is either a coset of a subspace of $\mathbb{F}$, or Condition (2.1) holds.*

Proof. Let U be a minimal subquasigroup of Q. Set $m = |U|$. For $\varepsilon \in \{-1,1\}$, denote by $\sigma(\varepsilon)$ the number of $(u,v) \in U \times U$ such that $\chi(v-u) = \varepsilon$. Since $\sigma(1) + \sigma(-1) = m(m-1)$, there exists $\varepsilon \in \{-1,1\}$ such that $\sigma(\varepsilon) \geqslant \binom{m}{2}$. Fix such ε, and fix also $s,t \in U$ such that $\chi(t-s) = \varepsilon$.

Denote by A the permutation group on U that is induced by affine automorphisms acting on U. Since s and t generate U, we see that $\psi(U) = U$ whenever $\psi \in \mathrm{Aut}(Q)$ is such that $\psi(s), \psi(t) \in U$. By Proposition 3.3, for each $(u,v) \in U \times U$ with $\chi(v-u) = \varepsilon$, there exists $\psi \in A$ such that $\psi(s) = u$ and $\psi(t) = v$. Therefore, $|A| \geqslant \binom{m}{2}$.

Denote by f the number of fixed point free elements of A. The aggregate number of fixed points of elements of A is equal to $m + |A| - 1 - f$. By Burnside's lemma, this is equal to $|A|k$, where k is the number of orbits of A. If $k \geqslant 2$, then

$$m - 1 - f = |A|(k-1) \geqslant |A| \geqslant \frac{1}{2}m(m-1).$$

It follows that $2(-1-f) \geqslant m(m-3)$, and hence $m < 3$. However, this is impossible since there is no idempotent quasigroup of order two and $|U| > 1$. Hence, $k=1$; in other words, A is transitive. As each non-trivial element of A fixes at most one element, it follows that

A is either a regular group or a Frobenius group. Since $|A| \geqslant m(m-1)/2$, the former alternative may take place if and only if $m=3$. We distinguish two cases.

First, suppose that $|A| = 3$. This means that A is cyclic, and $|U| = m = 3$ as well. Let A be generated by an affine permutation $x \mapsto \lambda x + \mu$. If $\lambda = 1$, then U is a coset of a subspace and $\mathrm{char}(\mathbb{F}) = 3$. Suppose $\lambda \neq 1$. Then $\lambda^3 = 1$, so $\lambda^2 + \lambda + 1 = 0$. Our intention is to show that $ab = 1 = a + b$. By Proposition 2.1(ii), it may be assumed that $0 \in U$ since automorphisms map minimal subquasigroups to minimal subquasigroups. Suppose that $u \in U \setminus \{0\}$. Then $u = \mu$ and $U = \{0, u, (\lambda+1)u\}$. Since U is idempotent, $u * 0 = 0 * u = (\lambda + 1)u = -\lambda^2 u$. Suppose that -1 is a square. Then $-\lambda^2 u = u * 0 = u - 0 * u = (1 + \lambda^2)u = -\lambda u$, resulting in $\lambda = 1$. Hence, -1 is a non-square. If u is a square, then $0 * u = au$, so $a = -\lambda^2$ and $u = 0 * (-\lambda^2 u) = -\lambda^2 bu = abu$. Alternatively, if u is a non-square, then $0 * u = bu$, so $b = -\lambda^2$ and $u = 0 * (-\lambda^2 u) = -\lambda^2 au = abu$. Therefore, $ab = 1$ in every case. Since at least one of a^3 and b^3 is equal to $(-\lambda^2)^3 = -1$, it must be that $a^3 = -1 = b^3$.

Thus, $\chi(a) = \chi(b) = \chi(-1) = -1$ and $0 = a^3 + 1 = (a+1)(a^2 - a + 1)$. If $a = -1$, then $b = -1$ and $-u = 0 * u = u * 0 = u - (-u) = 2u$. In such a case, $0 = 3$, $U = \{0, u, -u\}$ is a subspace of $\mathbb{F}$, and $a + b = -2 = 1$. Assume $a \neq -1$. Then $b \neq -1$, $a^2 - a = -1 = b^2 - b$ and $a + b = a + a^{-1} = (a^2 + 1)/a = 1$. Hence, Condition (2.1) holds, by Lemma 2.7.

Let us now turn to the case $|A| > 3$. The group A is a Frobenius group on an m-element set U with complements of order $\geqslant (m-1)/2$. The kernel of A is elementary abelian, by Lemma 3.1. To finish it suffices to prove that all elements of the kernel of A are induced by translations $x \mapsto x + \mu$. Assume the contrary. This means that the kernel of A contains a permutation that is a restriction of an affine automorphism $\psi\colon x \mapsto \lambda x + \mu$, where $\lambda \neq 1$. Choose an affine automorphism φ that induces a non-trivial permutation belonging to a complement of A. Both φ and ψ are elements of the Frobenius group formed by affine automorphisms of Q, and they belong to different Frobenius complements of the latter group. Hence, $[\psi, \psi^\varphi]$ is a fixed point free permutation of Q, by Lemma 3.2. Denote by $\tilde{\psi}$ the restriction of ψ to A. Both $\tilde{\psi}$ and $\tilde{\psi}^\varphi$ belong to the kernel of A. This kernel is abelian. Hence, $[\psi, \psi^\varphi]$ fixes each point of U, a contradiction. □

4. Existence and non-existence of isomorphisms

The purpose of this section is to prove Theorems 1.1 and 1.2 for 2-generated quadratic quasigroups and to discuss consequences of the existence of an additive automorphism $\varphi \in \mathrm{Aut}(Q)$ that maps a square to a non-square. One of the tools will be the following obvious fact:

Lemma 4.1. *Let $x \in \mathbb{F}^*$. The least subfield containing x coincides with the set of all sums $x^{i_1} + \cdots + x^{i_k}$, where i_j is a non-negative integer for $1 \leqslant j \leqslant k$ and $k \geqslant 0$.*

The following easy facts may be deduced, e.g., from results of Perron [10]. (To avoid a misunderstanding, let it be mentioned that while Perron's paper is formulated for prime fields only, the proofs of the paper carry without a change to any finite field of odd order.)

Lemma 4.2. *Assume $|\mathbb{F}| \geqslant 5$. Each square may be obtained as a sum of two non-squares, and each non-square may be obtained as a sum of two squares. For each*

https://doi.org/10.1017/S0013091523000585 Published online by Cambridge University Press

$a \in \mathbb{F}$, there exist squares $x, y \in \mathbb{F}$ and non-squares $x', y' \in \mathbb{F}$ such that $a+x$ and $a+x'$ are squares, while $a+y$ and $a+y'$ are non-squares.

Note that if $Q_{a,b}$ is a quadratic quasigroup over $\mathbb{F}_3$, then $a = b = -1$. In particular, if $|\mathbb{F}| < 5$, then $Q_{a,b}$ has to be affine.

A permutation ψ of $\mathbb{F}$ is said to be *additive* if $\psi(x+y) = \psi(x) + \psi(y)$ for all $x, y \in \mathbb{F}$.

Lemma 4.3. *Let $Q = Q_{a,b}$ be a non-affine quadratic quasigroup over $\mathbb{F}$, and let $\varphi \in \mathrm{Aut}(Q)$ be additive. Suppose that there exists $f \in \mathbb{F}$ such that $\varphi(a^i) = b^i f$ for each integer i. Then f is a non-square.*

Furthermore, denote by U the least subfield of $\mathbb{F}$ that contains the subquasigroup generated by 0 and 1. Then U is a subquasigroup of Q containing a and b, and $b = a^\gamma$ for some $\gamma > 1$ such that $\gamma^2 \mid |\mathbb{F}|$ and $\varphi(u) = u^\gamma f$ for each $u \in U$.

If U contains an element that is a non-square in $\mathbb{F}$, then $(U, *) = (\mathbb{F}_{\gamma^2}, *_a)$.

Proof. Since $0 * 1 = a$, we have $0 * f = \varphi(0) * \varphi(1) = \varphi(a) = bf$. Therefore, f is a non-square.

Denote by U_a the subfield of $\mathbb{F}$ generated by a and by U_b the subfield of $\mathbb{F}$ generated by b. The field U_a coincides with the set of all sums $a^{i_1} + \cdots + a^{i_k}$, $k \geqslant 0$, by Lemma 4.1. The assumptions of the statement imply that

$$\varphi(a^{i_1} + \cdots + a^{i_k}) = (b^{i_1} + \cdots + b^{i_k})f. \tag{4.1}$$

This means that the bijection φ maps U_a to $U_b f$. Therefore, there exists a bijection $\alpha\colon U_a \to U_b$ such that φ sends $u \in U_a$ to $\alpha(u)f$. The form of α follows from Condition (4.1), and this form stipulates that α is an isomorphism of fields $U_a \cong U_b$. Both of them are subfields of $\mathbb{F}$. Since they are of the same order, they have to coincide.

Note that any subfield that contains both a and b forms a subquasigroup of Q, by Condition (1.1). Hence, U_a is a subquasigroup that contains both 0 and 1. Therefore, $U_a \supseteq U$. Since $0 * 1 = a \in U$, we have $U \supseteq U_a$ as well, so $U = U_a$.

The field automorphism $\alpha \in \mathrm{Aut}(U)$ extends to an automorphism of $\mathbb{F}$ that sends each $x \in \mathbb{F}$ to x^γ, where γ divides $|U|$, which in turn divides $|\mathbb{F}|$.

Every element of a subfield $\mathbb{K}$ of $\mathbb{F}$ is a square in $\mathbb{F}$ if and only if $|\mathbb{F} : \mathbb{K}|$ is an even number. If $|\mathbb{F} : U|$ is even, then γ^2 divides $|\mathbb{F}|$.

Suppose that $|\mathbb{F} : U|$ is odd. Then there exists $u \in U$ such that u is a non-square in $\mathbb{F}$. Since $0 * u = bu = a^\gamma u$ and φ is an automorphism, $\varphi(a^\gamma u) = \varphi(0) * \varphi(u) = 0 * u^\gamma f = au^\gamma f$. Since $a^\gamma u \in U$, we also have $\varphi(a^\gamma u) = a^{\gamma^2} u^\gamma f$. Therefore, $a^{\gamma^2} = a$. Since $U = U_a$ is the least subfield containing a, we see that $x^{\gamma^2} = x$ for every $x \in U$, by Lemma 4.1. Also $a \neq b = a^\gamma$, so $\gamma \neq 1$ and $U = \mathbb{F}_{\gamma^2}$. The rest follows from Proposition 1.4. $\square$

Lemma 4.4. *Let $Q = Q_{a,b}$, be a quadratic quasigroup over $\mathbb{F}$, with a and b distinct non-squares. Let $\varphi \in \mathrm{Aut}(Q)$ be additive and let $f = \varphi(1)$ be a non-square. Then there exists $\gamma > 1$ such that $b = a^\gamma$, γ^2 divides $|\mathbb{F}|$ and $\mathbb{F}_{\gamma^2}$ carries a subquasigroup of Q that coincides with $(\mathbb{F}_{\gamma^2}, *_a)$.*

Proof. The first step is to prove for each $i \geqslant 0$ that

$$\varphi(a^i b^i) = a^i b^i f, \text{ and} \tag{4.2}$$

https://doi.org/10.1017/S0013091523000585 Published online by Cambridge University Press

$$\varphi(a^{i+1}b^i) = a^i b^{i+1} f. \tag{4.3}$$

Now $\varphi(a) = \varphi(0 * 1) = \varphi(0) * \varphi(1) = 0 * f = bf$, so Condition (4.3) holds for $i = 0$. Also Condition (4.2) holds for $i = 0$ by the definition of f. Note that $a^i b^i$ is a square and $a^i b^{i-1}$ is a non-square. So by induction on i, we find that

$$\varphi(a^i b^i) = \varphi(0 * a^i b^{i-1}) = \varphi(0) * \varphi(a^i b^{i-1}) = 0 * a^{i-1} b^i f = a^i b^i f \text{ and}$$
$$\varphi(a^{i+1} b^i) = \varphi(0 * a^i b^i) = \varphi(0) * \varphi(a^i b^i) = 0 * a^i b^i f = a^i b^{i+1} f,$$

completing the proof of Conditions (4.2) and (4.3).

Denote by C the subfield of $\mathbb{F}$ generated by ab. By Lemma 4.1, each element of C may be expressed as a sum $(ab)^{i_1} + \cdots + (ab)^{i_k}$. Hence, $\varphi(c) = cf$ for each $c \in C$, by Condition (4.2).

Let us now assume that there exists $\zeta \in C$ such that $\chi(\zeta) = -1$. In such a case, the non-squares of C coincide with the non-squares of $\mathbb{F}$ contained in C, and, as we shall prove, whenever $x, y \in \mathbb{F}$ such that $\chi(x) = \chi(y)$ and that $\varphi(x) = yf$, then

$$(\forall c \in C\colon\ \varphi(xc) = ycf) \quad \Rightarrow \quad (\forall c \in C\colon\ \varphi(axc) = bycf). \tag{4.4}$$

Let us assume that the hypothesis of Condition (4.4) is true. Our aim is to show that then $\varphi(axc) = bycf$ for each $c \in C$. The first step is a choice of $x', y' \in \mathbb{F}$. If x is a square, put $(x', y') = (x, y)$. If x is a non-square, put $(x', y') = (x\zeta, y\zeta)$, where ζ is as above. By the hypothesis of Condition (4.4), $\varphi(x's) = y'sf$ for each square $s \in C$. Since $x's$ and $y's$ are squares, $\varphi(ax's) = \varphi(0 * x's) = \varphi(0) * \varphi(x's) = 0 * y'sf = by'sf$ for each square $s \in C$. If $t \in C$ is another square, then $\varphi(ax'(s + t)) = by'(s + t)f$ since φ is additive. Therefore, $\varphi(ax'c) = by'cf$ for each $c \in C$, by Lemma 4.2. That finishes the proof of Condition (4.4) since $\zeta \in C$.

Assuming the existence of ζ, Condition (4.4) implies $\varphi(a^i c) = b^i cf$, for each $i \geqslant 0$ and $c \in C$. Indeed, since we have proved that $\varphi(c) = cf$ for each $c \in C$, the equality holds for $i = 0$. The induction step follows from Condition (4.4), by setting $(x, y) = (a^i, b^i)$.

We have shown that if C carries a non-square in $\mathbb{F}$, then $\varphi(a^i) = b^i f$ for every $i \geqslant 0$. That allows us to draw the needed conclusions from Lemma 4.3. So, for the rest of the proof, we may assume that each element of C is a square in $\mathbb{F}$. In particular, $\chi(-1) = 1$.

Now $\varphi(a) = \varphi(0 * 1) = \varphi(0) * \varphi(1) = 0 * f = bf$ and $\chi(a - 1) = \chi(b - 1)$, by Condition (1.2). Thus, the claim

$$\varphi(a^i) = b^i f \quad \text{and} \quad \chi(a^i - 1) = \chi(b^i - 1) \tag{4.5}$$

holds for $i = 1$. Let us now show that if $\varphi(a^j) = b^j f$ holds for each positive $j \leqslant i$, then $\chi(a^i - 1) = \chi(b^i - 1)$. Since $\chi(a - 1) = \chi(b - 1)$, it suffices to show that $\chi(A) = \chi(B)$, where $A = \sum_{j=0}^{i-1} a^j$ and $B = \sum_{j=0}^{i-1} b^j$. Note that $\varphi(A) = Bf$. It follows that $A = 0$ if and only if $B = 0$, so we may assume that $A \neq 0$ and $B \neq 0$. Suppose that A is a non-zero square, so that $0 * A = aA$. Since φ is an additive automorphism, we must have $0 * fB = \varphi(aA) = fbB$. However, that is possible if and only if B is a square. Conversely, if B is a square, then $\varphi(0 * A) = 0 * fB = fbB = \varphi(aA)$, implying that $0 * A = aA$.

https://doi.org/10.1017/S0013091523000585 Published online by Cambridge University Press

Hence, A is a square in $\mathbb{F}$ if and only if B is a square in $\mathbb{F}$, and the same holds for $a^i - 1$ and $b^i - 1$.

Thus, Condition (4.5) holds for all $i \geqslant 1$ if we can prove that its validity for a given $i \geqslant 1$ implies $\varphi(a^{i+1}) = b^{i+1}f$. For even i, we need only observe that $\varphi(a^{i+1}) = \varphi(0*a^i) = \varphi(0) * \varphi(a^i) = 0 * b^i f = b^{i+1}f$. So we may suppose that i is odd.

Assume first that $a^i - 1$ is a square. Then

$$\varphi(a^{i+1} - a) = \varphi(0 * (a^i - 1)) = \varphi(0) * \varphi(a^i - 1) = 0 * (b^i - 1)f = b^{i+1}f - bf.$$

Since $\varphi(-a) = -bf$ and φ is additive, we have $\varphi(a^{i+1}) = b^{i+1}f$.

Suppose now that $a^i - 1$ is a non-square. Then $b^i - 1$ is a non-square too, and $(b^i - 1)(-a^i) = a^i - (ab)^i$ is a square. By the inductive assumption and Condition (4.2), we see that

$$\varphi(a^i - (ab)^i) = (b^i - (ab)^i)f = (a^i - 1)(-b^i)f$$

is a non-square. Hence, by Condition (4.3),

$$\begin{aligned}\varphi(a^{i+1}) - a^i b^{i+1} f = \varphi(a^{i+1} - a^{i+1}b^i) &= \varphi(0 * (a^i - (ab)^i)) = 0 * (b^i - (ab)^i)f \\ &= b^{i+1}f - a^i b^{i+1} f.\end{aligned}$$

Therefore, $\varphi(a^{i+1}) = b^{i+1}f$, completing the proof of Condition (4.5). We see that Lemma 4.3 may be applied in this case too. □

Proposition 4.5. *Let $Q = Q_{a,b}$ be a non-affine quadratic quasigroup over $\mathbb{F}$. Suppose that there exists $\varphi \in \mathrm{Aut}(Q)$ such that φ is additive and $\varphi(1)$ is a non-square. Then $b = a^\gamma$, where γ^2 divides $|\mathbb{F}|$ and $\gamma > 1$. The subfield U generated by a is equal to $\mathbb{F}_{\gamma^2}$ and forms a subquasigroup of Q such that $(U, *) = (\mathbb{F}_{\gamma^2}, *_a)$.*

Proof. If a and b are non-squares, then the result follows from Lemma 4.4, so we assume that a and b are squares. It is then easy to show by induction that $\varphi(a^i) = b^i f$ for every $i \geqslant 1$, where $f = \varphi(1)$. Indeed $\varphi(a) = bf$ since $0*1 = a$, while $\varphi(a^{i+1}) = \varphi(0*a^i) = 0 * b^i f = b^{i+1}f$ yields the induction step. By Lemma 4.3, U is a subquasigroup, $b = a^\gamma$ for $\gamma > 1$ such that $\gamma^2 \mid |\mathbb{F}|$, and the statement is true if U contains an element that is a non-square in $\mathbb{F}$. Thus, for the rest of the proof, it will be assumed that each element of U is a square in $\mathbb{F}$. Let us also stipulate that $\gamma > 1$ is the least possible.

The next step is to show that if $\chi(\varphi(f)) = 1$, then $\varphi(u^\gamma f) = u\varphi(f)$, while for $\chi(\varphi(f)) = -1$ we have $\varphi(uf) = u\varphi(f)$, for each $u \in U$.

We first assume $\chi(\varphi(f)) = 1$ and employ induction to prove that $\varphi(b^i f) = a^i \varphi(f)$ for each $i \geqslant 0$. The case $i = 0$ is trivial, and $\varphi(b^{i+1}f) = \varphi(0 * b^i f) = 0 * a^i\varphi(f) = a^{i+1}\varphi(f)$ completes the induction. Each $u \in U$ may be expressed as $\sum a^{i_j}$, by Lemma 4.1. In such a case, $u^\gamma = \sum b^{i_j}$ and $\varphi(u^\gamma f) = u\varphi(f)$, by the additivity of φ.

Assume now that $\chi(\varphi(f)) = -1$. Since b is the image of a under the field automorphism $x \mapsto x^\gamma$, we have $a = b^{\gamma'}$, where $x \mapsto x^{\gamma'}$ is the inverse automorphism. Thus, each $u \in U$ may be expressed as $\sum b^{i_j}$, by Lemma 4.1. Also, $\varphi(b^i f) = b^i\varphi(f)$ for each $i \geqslant 0$ by

https://doi.org/10.1017/S0013091523000585 Published online by Cambridge University Press

induction, since $\varphi(b^{i+1}f) = \varphi(0*b^if) = 0*b^i\varphi(f) = b^{i+1}\varphi(f)$. Therefore, $\varphi(uf) = u\varphi(f)$ for each $u \in U$, as claimed.

The automorphism φ may be replaced by its composition with the affine isomorphism $x \mapsto cx$, where c is a square. Hence, f may be equal to any non-square in $\mathbb{F}$. By Lemma 4.2, we may choose f in such a way that $1+f$ is a square. Then

$$\begin{aligned} a^\gamma f + \varphi(af) &= \varphi(a+af) = \varphi(0*(1+f)) \\ &= 0*\varphi(1+f) \in \{af + a\varphi(f),\, a^\gamma f + a^\gamma\varphi(f)\}, \end{aligned} \tag{4.6}$$

by Condition (1.1). If $\varphi(f)$ is a non-square, then $\varphi(af) = a\varphi(f)$, by the results above. This contradicts Condition (4.6) since $a^\gamma \neq a$. Hence, $\varphi(f)$ is a square and $\varphi(af) = a^{1/\gamma}\varphi(f)$. Suppose first that

$$a^\gamma f + a^{1/\gamma}\varphi(f) = af + a\varphi(f)$$

and choose $d \in \mathbb{F}$ such that

$$d^\gamma = \frac{a^\gamma - a}{a - a^{1/\gamma}}.$$

Then $\varphi(f) = d^\gamma f$. Because $d \in U$, we also have $\varphi(d) = d^\gamma f$, by Lemma 4.3. Thus, $d = f$. This is a contradiction since d is a square and f is a non-square. Therefore, $a^{1/\gamma}\varphi(f) = a^\gamma\varphi(f)$, and $a^{\gamma^2} = a$. Hence, $|U|$ divides γ^2 and admits a non-trivial involutory automorphism $x \mapsto x^\gamma$. Since γ has been chosen to be the least possible, γ is a proper divisor of $|U|$. Thus, $|U| = \gamma^2$. □

Lemma 4.6. *Let $Q_{a,b}$ be a 2-generated quadratic quasigroup over $\mathbb{F}$. Then at least one of the quasigroups $Q_{a,b}$ and $Q_{b,a}$ is generated by $\{0,1\}$.*

Proof. Put $Q = Q_{a,b}$. Since $\mathrm{Aut}(Q)$ is transitive, there exists $u \in Q$ such that $\{0,u\}$ generates Q. If u is a square, then Q is generated by $\{0,1\}$ since $x \mapsto ux$ belongs to $\mathrm{Aut}(Q)$. Assume that u is a non-square. Then $x \mapsto u^{-1}x$ is an isomorphism $Q_{a,b} \cong Q_{b,a}$, by Proposition 2.1(iv), and this isomorphism sends $\{0,u\}$ to $\{0,1\}$. □

Theorem 4.7. *Let $Q = Q_{a,b}$ be a 2-generated quadratic quasigroup over $\mathbb{F}$. Then $G = \mathrm{Aut}(Q)$ is 2-transitive if and only if $a = b$ or $Q = (\mathbb{F}_{\gamma^2}, *_a)$.*

In the former case, G consists of all mappings $x \mapsto \lambda x + \mu$, where $\lambda \in \mathbb{F}^*$ and $\mu \in \mathbb{F}$. In the latter case, G consists of mappings $x \mapsto \lambda x + \mu$ and mappings $x \mapsto \lambda' x^\gamma + \mu$, where $\lambda, \lambda', \mu \in \mathbb{F}$, $\chi(\lambda) = 1$ and $\chi(\lambda') = -1$.

If G is not 2-transitive, then it consists of all mappings $x \mapsto \lambda x + \mu$, where $\lambda, \mu \in \mathbb{F}$ and $\chi(\lambda) = 1$.

Proof. By Proposition 2.1, G contains all mappings $x \mapsto \lambda x + \mu$, where $\lambda \in \mathbb{F}^*$ is a square. Suppose first that G is 2-transitive. Then G is sharply 2-transitive since an automorphism that fixes generators pointwise has to be the identity mapping. The mappings $x \mapsto x + \mu$ thus form a normal subgroup of G, and that makes each $\varphi \in G_0$ additive (where G_0 is the stabilizer of 0 in G). Proposition 4.5 hence confirms that G

https://doi.org/10.1017/S0013091523000585 Published online by Cambridge University Press

may be 2-transitive only in the cases described above. All mappings mentioned so far are automorphisms of Q, and they form a 2-transitive group. No other automorphism of Q may thus exist.

Let us now turn to the case when G is not 2-transitive. Let Q be generated by $\{0, u\}$. Then $\chi(u) = \chi(\varphi(u))$ for each $\varphi \in G_0$ since otherwise G is 2-transitive. For each $\varphi \in G_0$, there thus exists a square $\lambda \in \mathbb{F}^*$ such that $\varphi(u) = \lambda u$. Since φ and $x \mapsto \lambda x$ agree on a set of generators, they agree everywhere. Nothing else is needed. □

Theorem 4.8. *Let $Q = Q_{a,b}$ be a 2-generated quadratic quasigroup over $\mathbb{F}$. Then $Q \cong Q_{c,d}$ if and only if there exists $\alpha \in \mathrm{Aut}(\mathbb{F})$ such that $\{c, d\} = \{\alpha(a), \alpha(b)\}$.*

Proof. By Proposition 2.1, only the direct implication needs to be proved. Fix an isomorphism $\psi\colon Q \mapsto Q_{c,d}$ and put $G = \mathrm{Aut}(Q)$. The group G is 2-transitive if and only if $\mathrm{Aut}(Q_{c,d})$ is 2-transitive. If $a = b$, then $c = d$ since this is the only 2-transitive case in which G_0 is abelian, by Theorem 4.7. Hence, Theorem 4.7 implies that G is equal to $\mathrm{Aut}(Q_{c,d})$ in all cases. Therefore, ψ normalizes G, and hence ψ also normalizes the group of translations $x \mapsto x + \mu$. Since G is transitive, $\psi(0) = 0$ may be assumed. The normalizing property means that ψ is additive and normalizes G_0.

By Lemma 4.6, it may be assumed that Q is generated by 0 and 1. Then 0 and $\psi(1)$ generate $Q_{c,d}$. After a possible switch of c and d, we may thus assume that $\psi(1) = 1$ as well, by Proposition 2.1(iii), (iv).

Denote by σ_s the multiplication $x \mapsto sx$, where $s \in \mathbb{F}^*$. If $\sigma_s \in G_0$, then $\psi\sigma_s\psi^{-1} = \sigma_t$ for some $t \in \mathbb{F}^*$ since ψ normalizes G_0. Since $\psi(1) = 1$, we must have $t = \psi(s)$. Hence, $\psi(sy) = \psi\sigma_s(y) = \sigma_t\psi(y) = \psi(s)\psi(y)$ for all $y \in \mathbb{F}$, whenever $\sigma_s \in G_0$. This shows that $\psi \in \mathrm{Aut}(\mathbb{F})$ if $a = b$.

Suppose that $a \neq b$. We shall show that $\psi \in \mathrm{Aut}(\mathbb{F})$ in this case too. Indeed, if $x \in \mathbb{F}$ is a non-square, then x may be expressed as $u + v$, where both u and v are squares, by Lemma 4.2. In such a case, $\psi(xy) = \psi(uy + vy) = (\psi(u) + \psi(v))\psi(y) = \psi(x)\psi(y)$ for all $y \in \mathbb{F}$.

To finish, note that in $Q_{c,d}$ both $c = 0 * 1 = \psi(0) * \psi(1) = \psi(a)$ and $\psi(b)\psi(\zeta) = \psi(b\zeta) = \psi(0 * \zeta) = 0 * \psi(\zeta) = d\psi(\zeta)$ hold, where ζ is any non-square. Hence, $c = \psi(a)$ and $d = \psi(b)$. □

5. Subfields and subquasigroups

In this section, we examine the structure of minimal subquasigroups and 2-generated subquasigroups of quadratic quasigroups. Note that in Steiner quasigroups, every pair of elements generates a (minimal) subquasigroup of order 3, by definition. As this case is trivial, we may for convenience exclude certain Steiner quasigroups from our discussions in this section.

Let us start with an easy general fact:

Lemma 5.1. *Let Q be a finite quasigroup and let α be an automorphism of Q. Suppose that S is a subquasigroup of Q that is generated by a set X. Then $\alpha(S) = S$ if and only if $\alpha(X) \subseteq S$.*

https://doi.org/10.1017/S0013091523000585 Published online by Cambridge University Press

Proof. If $\alpha(S) = S$, then $\alpha(X) \subseteq S$. Conversely, assume $\alpha(X) \subseteq S$, and denote by S' the subquasigroup generated by $\alpha(X)$. We have $\alpha(X) \subseteq S' \cap S$, so $S' \subseteq S$. However, α is an isomorphism from S to S' so $|S'| = |S|$, which means that $\alpha(S) = S' = S$. $\square$

Lemma 5.2. *Let $Q = Q_{a,b}$ be a quadratic quasigroup over $\mathbb{F}$. The set of all $\sum a^{i_k} b^{j_k}$, where $1 \leqslant k \leqslant r$, with $i_k \geqslant 0$, $j_k \geqslant 0$ and $r \geqslant 0$, coincides with the least subfield of $\mathbb{F}$ that contains $\{a, b\}$. This subfield is a subquasigroup of Q.*

Proof. The set is closed under sums and products, and hence a subfield. By Definition (1.1), it is closed under $*$ as well. $\square$

Lemma 5.3. *Let Q be a quadratic quasigroup over $\mathbb{F}$ that is not a Netto quasigroup. Let S be a minimal subquasigroup of Q, with $\{0, 1\} \subseteq S$. Then S is a subfield of $\mathbb{F}$ and $a \in S$. If S contains a non-square, then $b \in S$, and S is equal to the least subfield of $\mathbb{F}$ that contains a and b. If S is composed of squares only, then S coincides with the least subfield of $\mathbb{F}$ that contains a.*

Proof. By Proposition 3.4 and Lemma 2.7, S is a subspace of $\mathbb{F}$. Moreover, if Q is affine Steiner, then S is equal to $\{0, 1, -1\}$ and is a subfield that contains $a = b = -1$. For the rest of the proof, it thus may be assumed that Q is not a Steiner quasigroup.

Put $S_0 = \{\sum x_i : x_i \in S \text{ and } \chi(x_i) \geqslant 0\}$ and note that $S_0 \subseteq S$. If $s \in S$ is a non-zero square, then the automorphism $x \mapsto sx$ sends 0 to 0 and 1 to $s \in S$. Thus, 0 and s generate S, by Lemma 5.1. Hence, $sS = S$ and $sS_0 \subseteq S_0$. Since S_0 is a subspace, $S_0S_0 \subseteq S_0$, and that implies that S_0 is a subfield of $\mathbb{F}$. Furthermore, S is a vector space over S_0, since $x_iS \subseteq S$ yields $(\sum x_i)S \subseteq S$.

If $\{a, b\} \subseteq S_0$, then $S = S_0$, by Lemma 5.2. Note that $a = 0 * 1$ always belongs to S.

Let a be a square. Then $a^i \in S_0$ for each $i \geqslant 0$ since $0 * a^i = a^{i+1}$. Hence, $S_0 \supseteq S_a$ by Lemma 4.1, where S_a is the least subfield of $\mathbb{F}$ that contains a. If S_0 consists only of squares, then S_a is a subquasigroup, and $S_a = S_0 = S$. Suppose that S_0 contains a non-square, say ζ. To show that $b \in S_0$, it suffices to show that $b \in S$, since b is a square. Now, $b\zeta = 0 * \zeta \in S$. Hence, $b = \zeta^{-1}(\zeta b) \in S$, since $\zeta^{-1} \in S_0$ and S_0 acts on S.

For the remainder of the proof, let a and b be non-squares. If S_0 contains a non-square, say ζ, then $b\zeta = 0 * \zeta \in S_0$. Therefore, $b = \zeta^{-1}(\zeta b) \in S_0$. Since $a \in S$, $0 * a = ab \in S_0$, and hence $a = b^{-1}(ab) \in S_0$. Thus, if S_0 contains a non-square, then $\{a, b\} \subseteq S_0 = S$, and S contains the subfield generated by a and b. In such a case, the subfield is equal to S, since the subfield is a subquasigroup containing a and b, by Lemma 5.2.

What remains is the case in which S_0 contains only squares, i.e. the squares of S form a subfield. We shall show that this may be always brought to a contradiction. Consider distinct $s, t \in S_0$. If $s * t = s + a(t - s)$ is a square, i.e. $s * t \in S_0$, then $a(t - s) = s * t - s$ is a square too, a contradiction. Hence, $s * t \in N_1 = S \setminus S_0$. If $s \in S_0 \setminus \{0\}$, then $0 * s = as \in N_1$. If $n \in N_1$, then $0 * n = bn \in S_0$. Therefore, $|S_0| = |N_1| + 1$. Consider now the multiplication table of $(S, *)$. Note that S is a disjoint union of S_0 and N_1. The subtable $S_0 \times S_0$ has elements of S_0 on the diagonal, and the rest is occupied by elements of N_1. Therefore, all entries in subtables $S_0 \times N_1$ and $N_1 \times S_0$ belong to S_0. Therefore, all entries in $N_1 \times N_1$ are from N_1, and that makes N_1 a subquasigroup. Since S is a minimal subquasigroup and $N_1 \neq S$, the only possibility is that $N_1 = \{a\}$ and $S_0 = \{0, 1\}$. Since S is a subspace, $\mathrm{char}(\mathbb{F}) = 3$, $a = -1$ and $ab = 0 * a = 0 * -1 = 1$.

That implies $b = -1$. By Lemma 2.7, this means that Q is a Steiner quasigroup, contrary to our assumptions. □

Theorem 5.4. *Let $Q = Q_{a,b}$ be a quadratic quasigroup over $\mathbb{F}$ that is not a Netto quasigroup. Let $\mathbb{K}$, $\mathbb{K}_0$ and $\mathbb{K}_1$ be the subfields generated by $\{a, b\}$, $\{a\}$ and $\{b\}$, respectively. Suppose that each subquasigroup of Q that is generated by two distinct elements is minimal. There are two possibilities:*

(i) *$\mathbb{K}$ contains an element that is a non-square in $\mathbb{F}$, and $\mathbb{K} = \mathbb{K}_0 = \mathbb{K}_1$. The minimal subquasigroups of Q are exactly the sets $\lambda\mathbb{K} + \mu$, where $\lambda \in \mathbb{F}^*$ and $\mu \in \mathbb{F}$.*

(ii) *All elements of $\mathbb{K}_i$, $i \in \{0, 1\}$, are squares in $\mathbb{F}$. If $\zeta \in \mathbb{F}$ is a non-square, then the minimal subquasigroups of Q are exactly the sets $\lambda\zeta^i\mathbb{K}_i + \mu$, where $\lambda \in \mathbb{F}^*$ is a square, and $\mu \in \mathbb{F}$.*

Proof. Denote by K the minimal subquasigroup generated by 0 and 1. Lemma 5.3 implies that if K contains a non-square, then $K = \mathbb{K} = \mathbb{K}_0 = \mathbb{K}_1$. The other possibility is that K consists of squares only. Then $K = \mathbb{K}_0$.

Suppose that $\lambda \in \mathbb{F}^*$ and $\mu \in \mathbb{F}$. If λ is a square, then $x \mapsto \lambda x + \mu$ is an automorphism of Q, by Proposition 2.1(iii). That makes $\lambda K + \mu$ a minimal subquasigroup of Q. If K contains a non-square ζ, then $\zeta K = K$ and $\lambda K + \mu = \lambda\zeta K + \mu$.

Let S be a minimal subquasigroup of Q that contains 0. By Proposition 2.1(ii), no other subquasigroups need to be considered.

Suppose there exists $s \in S$ and $\xi \in K$ such that $\chi(s) = \chi(\xi) \neq 0$. Let $\lambda = s/\xi$ and note that $x \mapsto \lambda x$ is an automorphism of Q that maps $\{0, \xi\}$ to $\{0, s\}$. By minimality, the former set generates K, while the latter set generates S. Therefore $\lambda K = S$. Such a λ always exists if K contains a non-square.

Suppose that $K = \mathbb{K}_0$ consists of squares only. If S contains a non-zero square, then, as we have proved, $S = \lambda\mathbb{K}_0$, where λ is a square. In such a case, all elements of S are squares. What remains to be characterized are those minimal subquasigroups S where $0 \in S$ and all non-zero elements are non-squares.

The mapping $x \mapsto x\zeta$ yields an isomorphism $Q_{a,b} \cong Q_{b,a}$ and sends S to $S\zeta$. Applying the earlier part of the proof to $Q_{b,a}$ yields $S\zeta = \lambda\mathbb{K}_1$, where λ is a square. □

Theorem 5.5. *Let $Q = Q_{a,b}$ be a quadratic quasigroup over $\mathbb{F}$ that is not a Netto quasigroup. Let $\mathbb{K}$, $\mathbb{K}_0$ and $\mathbb{K}_1$ be the subfields generated by $\{a, b\}$, $\{a\}$ and $\{b\}$, respectively. Suppose that there exists a 2-generated subquasigroup of Q that is neither trivial nor minimal. Then all such subquasigroups are exactly the sets $\lambda\mathbb{K} + \mu$, where $\lambda \in \mathbb{F}^*$ and $\mu \in \mathbb{F}$. Furthermore, each of -1, a, b, $1 - a$ and $1 - b$ is a square in $\mathbb{F}$. There are two possibilities:*

(i) *$\mathbb{K}_1$ consists of squares only and $\mathbb{K}_0$ contains a non-square. In this case $\mathbb{K}$ is generated, as a subquasigroup, by $\{0, s\}$ where $s \in \mathbb{K}$, if and only if $\chi(s) = 1$. In particular, $\mathbb{K}$ is generated by $\{0, 1\}$. The minimal subquasigroups of Q are exactly the sets $\zeta\mathbb{K}_1 + \mu$, where $\mu, \zeta \in \mathbb{F}$ and $\chi(\zeta) = -1$.*

(ii) *$\mathbb{K}_0$ consists of squares only and $\mathbb{K}_1$ contains a non-square. In this case, $\mathbb{K}$ is generated, as a subquasigroup, by $\{0, \zeta\}$, where $\zeta \in \mathbb{K}$, if and only if $\chi(\zeta) = -1$.*

The minimal subquasigroups of Q are exactly the sets $s\mathbb{K}_0 + \mu$, where $\mu, s \in \mathbb{F}$ and $\chi(s) = 1$.

Proof. Let S be a 2-generated subquasigroup that is not minimal. We shall first investigate the situation when S is generated by 0 and 1. The treatment is divided into a sequence of claims. The case of general S is considered at the end of the proof.

Claim 1. *S is generated by any set $\{0, s\}$, where $s \in S$ is a non-zero square.*

Consider the automorphism $x \mapsto sx$, which sends $\{0, 1\}$ to $\{0, s\}$. The claim follows from Lemma 5.1.

Claim 2. *S contains a non-square.*

Assume the contrary. Then there exists a minimal subquasigroup of Q that is contained in S and is generated by $\{0, c\}$, c a square. That cannot happen, by Claim 1.

Claim 3. (a) *$\chi(x) \geqslant 0$ for all $x \in \mathbb{K}_1$; and*
(b) *A set M containing* 0 *is a minimal subquasigroup of Q if and only if there exists $\zeta \in \mathbb{F}$ such that $M = \zeta\mathbb{K}_1$ and $\chi(\zeta) = -1$.*

There must be some minimal subquasigroup M_0 of Q satisfying $0 \in M_0 \subset S$. Every non-zero element of M_0 is a non-square, by Claim 1. Consider a non-zero $\zeta \in M_0$, and note that $\zeta^{-1}M_0$ consists of squares only. The isomorphism $Q_{a,b} \cong Q_{b,a}$, $x \mapsto \zeta^{-1}x$, sends M_0 to the minimal subquasigroup of $Q_{b,a}$ generated by 0 and 1. By Lemma 5.3, $\zeta^{-1}M_0 = \mathbb{K}_1$, and hence $M_0 = \zeta\mathbb{K}_1$ and Claim 3(a) holds. For any square $c \in \mathbb{F}^*$, we know that $c\zeta\mathbb{K}_1$ is a minimal subquasigroup of Q, by Proposition 2.1(iii), which proves the 'if' part of Claim 3(b).

For the converse direction, consider a minimal subquasigroup $M \ni 0$. If M contains a non-square ζ, then $M = \zeta\mathbb{K}_1$, since we already know that $\zeta\mathbb{K}_1$ is a minimal subquasigroup. If M contains a non-zero square c, then $\{0, 1\} \subseteq c^{-1}M$. That would imply that $S \subseteq c^{-1}M$, which is impossible because S is not minimal, but $c^{-1}M$ is minimal.

Claim 4. *All of the elements -1, a, b, $1 - a$ and $1 - b$ are squares.*

Suppose that -1 is a non-square. By Proposition 3.3, then there exists an automorphism of Q that sends 0 to ζ and 1 to 0, for each non-square $\zeta \in S$. That contradicts Claim 3(b), given that S is not minimal. Thus, -1 is a square. We already know from Claim 3(a) that b is a square. Hence, a is a square too. To see that $1 - a$ and $1 - b$ are squares as well, consider the opposite quasigroup, using Proposition 2.1(v).

Set

$$\begin{gathered} N_1 = \{x \in S : \chi(x) = -1\}, \quad S_1 = \{x \in S : \chi(x) = 1\}, \\ N_0 = N_1 \cup \{0\} \quad \text{and} \quad S_0 = S_1 \cup \{0\}. \end{gathered} \tag{5.1}$$

Claim 5. *S is the least subquasigroup containing N_0.*

If $c \in S_1$, then $cS = S$, by Lemma 5.1. This implies that $\zeta S_1 \subseteq S$, for every $\zeta \in N_1$. Since $\zeta S_1 \subseteq N_1$, we have $|S_1| = |\zeta S_1| \leqslant |N_1|$. Therefore, $|N_0| > |S|/2$, which means that N_0 cannot be contained in a proper subquasigroup of S.

https://doi.org/10.1017/S0013091523000585 Published online by Cambridge University Press

Claim 6. *If $c \in \mathbb{K}_1 \setminus \{0\}$, then $cS = S$. In particular, $\mathbb{K}_1 \leqslant S$.*

By Claim 5, N_0 generates S. If $\zeta \in N_1$ and $c \in \mathbb{K}_1 \setminus \{0\}$, then $c\zeta$ is in $\zeta\mathbb{K}_1$, which is minimal by Claim 3(b) and hence generated by 0 and ζ. But $\{0, \zeta\} \subseteq S$, so $c\zeta \in S$, and it then follows from Claim 3(a) that $cN_1 = N_1$. Hence, also $cS = S$, by Lemma 5.1.

Claim 7. *If $s \in S_0$, then $s + S = S$.*

Choosing $c = -1$ yields $-S = S$, by Claim 6. The quasigroup S is thus generated by $\{0, -s\}$, in view of Claim 1 and Claim 4. Denote by ψ the automorphism $x \mapsto x + s$. Since $\psi(0) = s$ and $\psi(-s) = 0$, we have $S = \psi(S) = s + S$, by Lemma 5.1.

Claim 8. $S = \mathbb{K}$.

Both a and b are squares that belong to S. Since $cS = S$ whenever $c \in S$ is a square, $a^i b^j \in S_0$ for all integers $i \geqslant 0$ and $j \geqslant 0$. A sum of such elements belongs to S by Claim 7. By Lemma 5.2, $\mathbb{K}$ is a subquasigroup and $\mathbb{K} \subseteq S$. Since $\{0, 1\} \subseteq \mathbb{K}$, we must have $S \subseteq \mathbb{K}$.

Recall that $\mathbb{K}_0$ denotes the subfield generated by a. If $\mathbb{K}_0$ consists of squares only, then $\mathbb{K}_0$ is a subquasigroup of Q. That cannot be, by Claim 2, since $\{0, 1\} \subseteq \mathbb{K}_0$.

Let S' be any subquasigroup of Q with $0 \in S'$.

Claim 9. *The subquasigroup S' is minimal if and only if $S' = \zeta\mathbb{K}_1$ for a non-square ζ. Also S' is 2-generated non-minimal if and only if $S' = \lambda\mathbb{K}$, where $\lambda \in \mathbb{F}^*$.*

The first equivalence corresponds to Claim 3(b). Now $S = \mathbb{K}$ and S contains some non-square ζ. For any $\lambda \in \mathbb{F}^*$, one of λS or $(\lambda\zeta^{-1})S$ is a subquasigroup isomorphic to S, by Proposition 2.1(iii). However, $(\lambda\zeta^{-1})S = (\lambda\zeta^{-1})\zeta S = \lambda S$ because $S = \mathbb{K}$ is a field. It follows that $\lambda\mathbb{K}$ is a 2-generated non-minimal subquasigroup of Q for all $\lambda \in \mathbb{F}^*$.

Next suppose that $S' \ni 0$ is a non-minimal subquasigroup generated by elements 0 and λ. Let $S'' = \lambda^{-1}S'$. Note that λ must be a square since otherwise 0 and λ would generate the minimal subquasigroup $\lambda\mathbb{K}_1$, by Claim 3(b). So $x \mapsto \lambda^{-1}x$ is an isomorphism $S' \cong S''$, and it maps $0, \lambda$ to $0, 1$. Hence $S'' = S = \mathbb{K}$ and $S' = \lambda\mathbb{K}$.

It remains to consider the case when $S' \ni 0$ is a non-minimal subquasigroup generated by two general elements x and y. By Proposition 2.1(ii), S' is isomorphic to $S''' = S' - x$. Now S''' is a non-minimal subquasigroup generated by 0 and $y - x$, so by the previous case $S''' = (y - x)\mathbb{K}$. But $0 \in S' = (y - x)\mathbb{K} + x$, so $-x(y - x)^{-1} \in \mathbb{K}$. But $\mathbb{K}$ is closed under addition, so $S' = (y - x)(\mathbb{K} - x(y - x)^{-1}) + x = (y - x)\mathbb{K}$, which completes the proof of Claim 9.

Let us now turn to the general case. Recall that S is a subquasigroup generated by two distinct elements that is not minimal, but we no longer assume it is generated by $\{0, 1\}$. Clearly, it may be assumed that there exists $\xi \in \mathbb{F}^*$ such that S is generated by $\{0, \xi\}$. If ξ is a square, then the subquasigroup $S\xi^{-1}$ generated by 0 and 1 is also not minimal, and that allows us to use the characterization developed above. Hence, we may suppose that ξ is a non-square in $\mathbb{F}$. Then $S\xi^{-1}$ is a subquasigroup of $Q_{b,a}$ that is generated by 0 and 1 and is not minimal. Therefore, $S\xi^{-1} = \mathbb{K}$. Since $\mathbb{K}$ contains a non-square, say ζ, we have $S = \mathbb{K}\xi = \mathbb{K}c$, where $c = \zeta\xi$ is a square. Hence, $\mathbb{K}$ is a subquasigroup of Q that is 2-generated but not minimal.

In $Q_{b,a}$, the proper minimal subquasigroups of $\mathbb{K}$ containing 0 are exactly all of the sets $\mathbb{K}_0\xi$, where ξ is a non-square. Furthermore, the field $\mathbb{K}_0$ consists of squares only. The minimal subquasigroups of Q that include 0 are thus equal to $s\mathbb{K}_0$, where $\chi(s) = 1$. □

Theorems 5.4 and 5.5 describe the structure of minimal subquasigroups in all quadratic quasigroups that are not Netto quasigroups. The subfield $\mathbb{K}$ generated by a and b has a clear structural meaning in all these quasigroups except those that are described by Theorem 5.4(ii) and fulfil $\mathbb{K}_0 \neq \mathbb{K}_1$. Note that $\mathbb{K}_0 = \mathbb{K}_1$ for all affine quasigroups $Q_{a,a}$, and hence Theorem 5.5 implies that all 2-generated subquasigroups of $Q_{a,a}$ are minimal.

Affine lines and semilinear mappings

Suppose that $Q = Q_{a,b}$ is a quadratic quasigroup that contains minimal subquasigroups of two different orders. Theorems 5.4 and 5.5 implies that $\mathbb{K}_0 \neq \mathbb{K}_1$, where $\mathbb{K}_0$ is the least subfield containing a, and $\mathbb{K}_1$ the least subfield containing b and that both these subfields consist of squares only. The existence of a subfield consisting only of squares implies that $|\mathbb{F}| = q^2$ and that $\mathbb{K}_0 \cup \mathbb{K}_1 \subseteq \mathbb{F}_q$.

For distinct $x, y \in \mathbb{F}$ denote by $S(x, y)$ the subquasigroup S generated by x and y. Put $\lambda = y - x$. As follows from Theorem 5.4, $S = \lambda\mathbb{K}_0 + x$ if $\chi(\lambda) = 1$ and $S = \lambda\mathbb{K}_1 + x$ if $\chi(\lambda) = -1$.

Call a set $B \subseteq \mathbb{F}$ *saturated* if there exists $i \in \{0, 1\}$ such that for any distinct $x, y \in B$, both $|S(x, y)| = |\mathbb{K}_i|$ and $S(x, y) \subseteq B$ are true.

It follows from the above description of subquasigroups $S(x, y)$ that any set $\lambda\mathbb{F}_q + \mu$ is saturated, provided $\lambda \in \mathbb{F}^*$ and $\mu \in \mathbb{F}$. This may be converted:

Lemma 5.6. *A q-element set $B \subseteq \mathbb{F}$ is saturated if and only if there exist $\lambda \in \mathbb{F}^*$ and $\mu \in \mathbb{F}$ such that $B = \lambda\mathbb{F}_q + \mu$.*

Proof. Let B be saturated. By the definition of a saturated set, there exists $\varepsilon \in \{-1, 1\}$ such that $\chi(y - x) = \varepsilon$ whenever $x, y \in B$ and $x \neq y$. Every q-element set with the latter property is equal to a set of the form $\lambda\mathbb{F}_q + \mu$, where $\lambda \neq 0$, by a theorem of Blokhuis [3]. □

Corollary 5.7. *Let $Q_{a,b}$ be a quasigroup over $\mathbb{F}$ such that $Q_{a,b}$ contains minimal subquasigroups of two different orders. Then there exists $q > 1$ such that $|\mathbb{F}| = q^2$, and* $\mathrm{Aut}(Q)$ *acts on the set of all affine lines $\lambda\mathbb{F}_q + \mu$, where $\lambda \in \mathbb{F}^*$ and $\mu \in \mathbb{F}$.*

Proof. This follows from Lemma 5.6 since each automorphism of Q maps a saturated set to a saturated set. □

Let K be a subfield of $\mathbb{F}$. A permutation σ of $\mathbb{F}$ is said to be *K-semilinear* if σ is additive and there exists $\alpha \in \mathrm{Aut}(K)$ such that $\sigma(\lambda x) = \alpha(\lambda)\sigma(x)$ for all $x \in \mathbb{F}$ and $\lambda \in K$.

Note that if $L \subseteq K \subseteq \mathbb{F}$ are fields, and σ is a K-semilinear permutation of $\mathbb{F}$, then σ is L-semilinear too.

https://doi.org/10.1017/S0013091523000585 Published online by Cambridge University Press

Proposition 5.8. *Let $\psi \in \mathrm{Aut}(Q)$, where $Q = Q_{a,b}$ is a quadratic quasigroup defined on $\mathbb{F}$ that is not a Netto quasigroup. Let $\mathbb{K}$ be the subfield of $\mathbb{F}$ generated by a and b. Then there exists $\mu \in \mathbb{F}$ and a $\mathbb{K}$-semilinear mapping σ such that $\psi(x) = \sigma(x) + \mu$ for all $x \in \mathbb{F}$.*

Proof. If $Q = Q_{a,b}$ is 2-generated, use Theorem 4.7. Suppose that Q is not 2-generated. If all minimal subquasigroups of Q are of the same order, put $K = \mathbb{K}$. If there is no common order, denote by K the subfield of $\mathbb{F}$ that is of order q, where $|\mathbb{F}| = q^2$. Then ψ maps an affine line of K to an affine line of K. This is true for quasigroups in which all 2-generated subquasigroups are minimal by Theorem 5.4 and Corollary 5.7 since ψ preserves the structure of minimal subquasigroups. The other cases follow from Theorem 5.5 since ψ also preserves the structure of 2-generated subquasigroups that are not minimal. By The Fundamental Theorem of Affine Geometry [2], there thus exist $\mu \in \mathbb{F}$ and a K-semilinear permutation σ of $\mathbb{F}$ such that $\psi(x) = \sigma(x) + \mu$ for all $x \in \mathbb{F}$. □

6. Automorphisms and isomorphisms

This section proves Theorems 1.2 and 1.1. The proof of Theorem 1.2 is done separately for the affine case, twisted case, and all other situations. As shown in Lemma 2.7, Steiner quadratic quasigroups that are not affine are induced by Netto systems and fulfil the condition of Theorem 1.1. As mentioned in Section 1, the automorphism group of a Netto system is known [11] and conforms with our statement of Theorem 1.2. Netto quasigroups are thus not discussed in this section.

The proof of Theorem 1.2 has two parts: first we have to verify that certain mappings are automorphisms, and second we have to show that there are no other automorphisms. In view of Proposition 2.1, to achieve the first goal, only the affine and twisted cases need to be considered. For the affine case $x * y = x + a(y - x)$, so it is clear that any $\mathbb{K}$-linear map σ is an automorphism, $\mathbb{K}$ being the least subfield containing a. The second part of the proof of Theorem 1.2 for affine quasigroups follows directly from Proposition 6.2(ii) below.

Recall that $Q = Q_{a,b}$ is called twisted if $\mathbb{K}$, the subfield generated by a, is of order γ^2 and $b = a^\gamma$. The meaning of γ is considered to be fixed throughout this section, whenever Q is twisted.

To see that every permutation described in Theorem 1.2 is an automorphism of $Q_{a,b}$ it thus remains to verify the existence of automorphisms that generalize the automorphisms induced by the structure of a quadratic nearfield:

Lemma 6.1. *Let $Q = Q_{a,b}$ be a twisted quadratic quasigroup over $\mathbb{F}$. Then $x \mapsto \zeta x^\gamma + \mu$ is an automorphism of Q whenever ζ is a non-square in $\mathbb{F}$ and $\mu \in \mathbb{F}$.*

Proof. It may be assumed that $\mu = 0$. Let $x, y \in \mathbb{F}$ be distinct elements. Put $i = 0$ if $\chi(y - x) = 1$, and $i = 1$ if $\chi(y - x) = -1$. Then $x * y = x + a^{\gamma^i}(y - x)$ and

$$\zeta(x * y)^\gamma = \zeta x^\gamma + \zeta b^{\gamma^i}(y - x)^\gamma = \zeta x^\gamma + b^{\gamma^i}(\zeta y^\gamma - \zeta x^\gamma) = \zeta x^\gamma * \zeta y^\gamma,$$

since $\chi(y^\gamma - x^\gamma) = \chi((y - x)^\gamma) = \chi(y - x)$ because γ is odd. □

https://doi.org/10.1017/S0013091523000585 Published online by Cambridge University Press

Proposition 6.2. *Let $Q = Q_{a,b}$ be a quadratic quasigroup over $\mathbb{F}$ that is not a Netto quasigroup. Denote by $\mathbb{K}$ the subfield of $\mathbb{F}$ that is generated by a and b. Let $\psi \in \mathrm{Aut}(Q)$ be such that $\psi(0) = 0$. Then:*

(i) *$\psi(1)$ is a square in $\mathbb{F}$ if Q is neither affine nor twisted; and*
(ii) *ψ is $\mathbb{K}$-linear if $a = b$ or if $\psi(1)$ is a square in $\mathbb{F}$.*

Proof. Point (i) coincides with Proposition 4.5. Put $\lambda = \psi(1)$. Point (ii) will be first proved under the assumption that all minimal subquasigroups of Q are of the same order. In this case, $\psi(\mathbb{K}) = \lambda\mathbb{K}$ by Theorems 5.4 and 5.5 since a minimal subquasigroup is mapped to a minimal subquasigroup and a 2-generated subquasigroup is mapped to a 2-generated subquasigroup. The mapping $x \mapsto \lambda^{-1}\psi(x)$ hence is an automorphism of Q that sends the 2-generated subquasigroup $\mathbb{K}$ to itself. The restriction of the latter mapping to $\mathbb{K}$ is $\mathbb{K}$-linear by Theorem 4.7. Since the mapping is $\mathbb{K}$-semilinear, by Proposition 5.8, it has to be a $\mathbb{K}$-linear automorphism of Q. Hence, ψ is $\mathbb{K}$-linear as well.

Let us now assume that Q contains minimal subquasigroups of two distinct sizes. Let $\alpha \in \mathrm{Aut}(\mathbb{K})$ be the automorphism such that $\psi(cx) = \alpha(c)\psi(x)$ for all $c \in \mathbb{K}$. In this case, $|\mathbb{F}| = q^2$ for some $q > 2$ and $\psi(\mathbb{F}_q) = \lambda\mathbb{F}_q$ by Corollary 5.7. Hence, $x \mapsto \lambda^{-1}\psi(x)$ is a $\mathbb{K}$-semilinear mapping with automorphism α, the restriction of which yields an automorphism of $(\mathbb{F}_q, *)$ such that $x * y = x + a(y - x)$ for all $x, y \in \mathbb{F}_q$. Therefore, $\alpha(a) = a$, by the earlier part of this proof. To finish it suffices to show that $\alpha(b) = b$ too. To that end, choose a non-square $\zeta \in \mathbb{F}$ and note that $\psi(\zeta\mathbb{F}_q) = \lambda'\zeta\mathbb{F}_q$ for a square λ', by Corollary 5.7. The mapping $x \mapsto \zeta^{-1}(\lambda')^{-1}\psi(\zeta x)$ is an automorphism of $Q_{b,a}$ that sends $\mathbb{F}_q$ to $\mathbb{F}_q$ and is associated, as a $\mathbb{K}$-semilinear mapping, with the automorphism $\alpha \in \mathrm{Aut}(\mathbb{K})$. Since b is now in the position of a, we must have $\alpha(b) = b$. □

For non-affine cases, the following fact is of crucial importance.

Lemma 6.3. *Suppose that $\sigma : \mathbb{F} \to \mathbb{F}$ is bijective and additive. If*

$$\chi(v - u) = \chi(\sigma(v) - \sigma(u)) \quad \textit{for all } u, v \in \mathbb{F}, \tag{6.1}$$

then there exist $\alpha \in \mathrm{Aut}(\mathbb{F})$ and $\lambda \in \mathbb{F}$ such that $\sigma(x) = \lambda\alpha(x)$ for each $x \in \mathbb{F}^*$ and $\chi(\lambda) = 1$.

Proof. The set of all additive permutations σ of $\mathbb{F}$ that satisfy Condition (6.1) forms a group. This group contains the mapping $x \mapsto \lambda x$ for each $\lambda \in \mathbb{F}^*$, with $\chi(\lambda) = 1$. Since $\chi(\sigma(1)) = \chi(\sigma(1) - \sigma(0)) = \chi(1) = 1$, it suffices to prove the statement under the assumption that $\sigma(1) = 1$. However, if σ is a permutation of $\mathbb{F}$ such that $\sigma(0) = 0$, $\sigma(1) = 1$ and Condition (6.1) holds, then $\sigma \in \mathrm{Aut}(\mathbb{F})$ as shown by Carlitz [4]. □

Lemma 6.4. *Let $Q = Q_{a,b}$ be a non-affine quadratic quasigroup over $\mathbb{F}$ that is not a Steiner quasigroup. Denote by $\mathbb{K}$ the least subfield of $\mathbb{F}$ containing a and b. If $\sigma \in \mathrm{Aut}(Q)$ is $\mathbb{K}$-linear, then σ satisfies Condition (6.1).*

Proof. If $\chi(v-u) = 1$, then $\sigma(u*v) = \sigma(u + a(v-u)) = \sigma(u) + a(\sigma(v) - \sigma(u))$. Hence, $\sigma(u*v) = \sigma(u)*\sigma(v)$ implies that $\chi(\sigma(v) - \sigma(u)) = 1$. The argument when $\chi(v-u) = -1$ is similar. □

Lemma 6.5. *Let $Q = Q_{a,b}$ be a non-affine quadratic quasigroup over $\mathbb{F}$ that is neither Steiner nor twisted. Let $\mathbb{K}$ be the subfield generated by a and b. Then* $\mathrm{Aut}(Q) = \mathrm{A\Gamma^2L_1}(\mathbb{F}\,|\,\mathbb{K})$.

Proof. Let $\psi \in \mathrm{Aut}(Q)$ be such that $\psi(0) = 0$. Then ψ is $\mathbb{K}$-linear by Proposition 6.2 and is a square scalar multiple of some $\alpha \in \mathrm{Aut}(\mathbb{F})$ by Lemmas 6.4 and 6.3. □

Lemma 6.6. *Let $Q = Q_{a,b}$ be a twisted quasigroup over $\mathbb{F}$. Then* $\mathrm{Aut}(Q) = \mathrm{A\Gamma L}_1^{\mathrm{tw}}(\mathbb{F}\,|\,\mathbb{K})$.

Proof. Let $\psi \in \mathrm{Aut}(Q)$ be such that $\psi(0) = 0$. If $\psi(1)$ is a square, then $\psi \in \mathrm{A\Gamma^2L_1}(\mathbb{F}\,|\,\mathbb{K})$, by the same argument as in the proof of Lemma 6.5. Suppose that $\zeta = \psi(1)$ is a non-square and compose ψ with the mapping $\sigma\colon x \mapsto (\zeta^{-1})^\gamma x^\gamma$. Then $\sigma\psi \in \mathrm{Aut}(Q)$ by Lemma 6.1 and $\sigma \in \mathrm{A\Gamma L}_1^{\mathrm{tw}}(\mathbb{F}\,|\,\mathbb{K})$. Since $\sigma\psi(1) = 1$ is a square, $\sigma\psi \in \mathrm{A\Gamma^2L_1}(\mathbb{F}\,|\,\mathbb{K})$. These facts imply that ψ belongs to $\mathrm{A\Gamma L}_1^{\mathrm{tw}}(\mathbb{F}\,|\,\mathbb{K})$. □

This finishes the proof of Theorem 1.2. What follows is a proof of Theorem 1.1.

Proof. As mentioned at the beginning of this section, it may be assumed that $a = b$ if $Q = Q_{a,b}$ is a Steiner quasigroup. The subfield generated by a and b is denoted by $\mathbb{K}$.

Let $\zeta \in \mathbb{F}$ be a non-square. Since $x \mapsto \zeta x$ maps isomorphically $Q_{a,b}$ to $Q_{b,a}$ and $Q_{c,d}$ to $Q_{d,c}$, certain assumptions may be made. By Theorem 5.5, it may be assumed that if Q possesses a 2-generated subquasigroup that is not minimal, then $\mathbb{K}$ carries one such subquasigroup. It may also be assumed that there exists an isomorphism $\sigma\colon Q_{a,b} \cong Q_{c,d}$ that sends 0 to 0 and 1 to a square in $\mathbb{F}$. Since scalar multiplication by a non-zero square is an automorphism of $Q_{c,d}$, it may be assumed, in fact, that $\sigma(0) = 0$ and $\sigma(1) = 1$.

Suppose that Q does not contain minimal subquasigroups of distinct orders. Then $\mathbb{K}$ coincides with the subquasigroup generated by 0 and 1, by Theorems 5.4 and 5.5. By these theorems, $\sigma(\mathbb{K}) = \mathbb{K}$ since $\sigma(\mathbb{K})$ is a subquasigroup of $Q_{c,d}$ that is generated by 0 and 1. Applying Theorem 4.8 to the restriction of σ to $\mathbb{K}$ yields $\alpha \in \mathrm{Aut}(\mathbb{K})$ such that $c = \alpha(a)$ and $d = \alpha(b)$. This suffices, since α may be extended to an automorphism of $\mathbb{F}$.

Suppose now that Q contains minimal subquasigroups of two different orders. Then $|\mathbb{F}| = q^2$ for some $q > 2$, and in Q, there exists a unique saturated set of order q that contains both 0 and 1. This set is equal to $\mathbb{F}_q$. Since σ maps a saturated set to a saturated set, it must be that $\sigma(\mathbb{F}_q) = \mathbb{F}_q$. The orders of minimal subquasigroups contained in $\mathbb{F}_q$ are thus the same in both $Q_{a,b}$ and $Q_{c,d}$. By interpreting an affine line $\lambda\mathbb{F}_q + \mu$ as a saturated set, we therefore obtain that for all $\lambda \in \mathbb{F}^*$ and $\mu \in \mathbb{F}$ there exist $\lambda' \in \mathbb{F}^*$ and $\mu' \in \mathbb{F}$ such that $\chi(\lambda) = \chi(\lambda')$ and $\sigma(\lambda\mathbb{F}_q + \mu) = \lambda'\mathbb{F}_q + \mu'$. This means that σ fulfils Condition (6.1). Since $\sigma(0) = 0$ and $\sigma(1) = 1$, the theorem of Carlitz [4] implies that $\sigma \in \mathrm{Aut}(\mathbb{F})$. To get $\sigma(a) = c$ consider the quasigroup product of 0 and 1. To obtain $\sigma(b) = d$, multiply 0 and ζ. □

7. Concluding comments

The theory developed in this paper should prove to be useful in the many applications of quadratic quasigroups [1, 5, 7–9, 14]. In [14], methods were developed for distinguishing isomorphism classes of quasigroups generated from cyclotomic orthomorphisms.

In the quadratic case, this is now a very simple task, given Theorem 1.1. It would be of interest to develop similar methods for quasigroups generated from other cyclotomic orthomorphisms. Another feature of [14] is that commutative, semisymmetric and totally symmetric quasigroups played a prominent role, as they did in the current work. It thus should prove useful to have the characterizations in Theorem 1.3.

It was mentioned in the introduction that this paper grew out of a need in [5] to understand when quadratic quasigroups are isomorphic to each other. In that paper, we showed that, asymptotically, a non-zero constant fraction of the choices for the pair (a, b), result in $Q_{a,b}$ having a special property called maximal non-associativity. We conjectured that removing isomorphs would not reduce the demonstrated number of examples by more than a factor proportional to $\log|\mathbb{F}|$. Thanks to Theorem 1.1, we now know this conjecture to be true, since the automorphism group of $\mathbb{F}$ has order $O(\log|\mathbb{F}|)$.

Funding Statement. A. Drápal supported by INTER-EXCELLENCE project LTAUSA19070 MŠMT Czech Republic.

References

(1) J. Allsop and I. M. Wanless, Row-Hamiltonian Latin squares and Falconer varieties, *Proc. London Math. Soc.,* https://arxiv.org/abs/2211.13826.
(2) E. Artin, *Geometric Algebra* (Interscience Publishers, New York, 1957).
(3) A. Blokhuis, On subsets of $GF(q^2)$ with square differences, *Indag. Math.* **87**(4) (1984), 369–372.
(4) L. Carlitz, A theorem on permutations in a finite field, *Proc. Amer. Math. Soc.* **11** (1960), 456–459.
(5) A. Drápal and I. M. Wanless, Maximally nonassociative quasigroups via quadratic orthomorphisms, *Algebr. Comb.* **4**(3) (2021), 501–515.
(6) A. Drápal and I. M. Wanless, On the number of quadratic orthomorphisms that produce maximally nonassociative quasigroups, *J. Aust. Math. Soc.* **115** (2023), 311–336. doi:10.1017/S1446788722000386
(7) A. B. Evans, *Orthomorphism graphs of groups.* Lecture Notes in Mathematics, Volume 1535, (Springer, Berlin, 1992).
(8) A. B. Evans, *Orthogonal Latin squares based on groups.* Developments in Mathematics, Volume 57 (Springer, Cham, 2018).
(9) M. J. Gill and I. M. Wanless, Perfect 1-factorisations of K_{16}, *Bull. Aust. Math. Soc.* **101**(2) (2020), 177–185.
(10) O. Perron, Bemerkungen über die Verteilung der quadratischen Reste, *Math. Z.* **56** (1952), 122–180.
(11) R. M. Robinson, The structure of certain triple systems, *Math. Comp.* **29** (1975), 223–241.
(12) S. K. Stein, Homogeneous quasigroups, *Pacific J. Math.* **14** (1964), 1091–1102.
(13) H. Wähling, *Theorie der Fastkörper* (THALES Verlag GmbH, Essen, 1987).
(14) I. M. Wanless, Atomic Latin squares based on cyclotomic orthomorphisms, *Electron. J. Combin.* **12** (2005), R22.