Comment.Math.Univ.Carolin. 61,4 (2020) 459–479

Nonassociative triples in involutory loops and in loops of small order

Aleš Drápal, Jan Hora

Abstract. A loop of order n possesses at least $3n^2 - 3n + 1$ associative triples. However, no loop of order $n > 1$ that achieves this bound seems to be known. If the loop is involutory, then it possesses at least $3n^2 - 2n$ associative triples. Involutory loops with $3n^2-2n$ associative triples can be obtained by prolongation of certain maximally nonassociative quasigroups whenever $n-1$ is a prime greater than or equal to 13 or $n-1 = p^{2k}$, p an odd prime. For orders $n \leq 9$ the minimum number of associative triples is reported for both general and involutory loops, and the structure of the corresponding loops is described.

Keywords: quasigroup; loop; prolongation; involutory loop; associative triple; maximally nonassociative

Classification: 20N05, 05B15

1. Results

Let Q be a quasigroup. A triple $(x, y, z) \in Q^3$ is said to be *associative* if $x(yz) = (xy)z$. The number of associative triples in a quasigroup Q will be denoted by $\mathbf{a}(Q)$.

If Q is a loop of finite order n, and $1 \in \{x, y, z\}$, then (x, y, z) is an associative triple. Hence $\mathbf{a}(Q) \geq 3n^2 - 3n + 1$. Does there exist a loop of order $n > 1$ such that $\mathbf{a}(Q) = 3n^2 - 3n + 1$? We do not know. And we hope that this paper will stimulate interest in this question.

If x is an element of a loop Q, then the left inverse $1/x$ may differ from the right inverse $x\backslash 1$. Note that $(1/x, x, x\backslash 1)$ is an associative triple if and only if $1/x = x\backslash 1$.

Therefore $\mathbf{a}(Q) \geq 3n^2-2n$ whenever Q is a loop of order n such that $1/x = x\backslash 1$ for all $x \in Q$. A loop is said to be *involutory* if $x^2 = 1$ for all $x \in Q$. In an involutory loop $1/x = x = x\backslash 1$ for every $x \in Q$. We shall show that for infinitely many orders n there exists an involutory loop Q such that $\mathbf{a}(Q) = 3n^2 - 2n$.

DOI 10.14712/1213-7243.2020.037

Computational resources were supplied by the project "e-Infrastruktura CZ" (e-INFRA LM2018140) provided within the program Projects of Large Research, Development and Innovations Infrastructures.

Each involutory loop can be obtained by a prolongation of an idempotent quasigroup. A quasigroup is *idempotent* if $xx = x$ for all $x \in Q$. Idempotent quasigroups discussed in this paper will usually be derived from an abelian group $(G, +)$. In many cases this group will be the additive group of a field or a (left) nearfield. To avoid confusion with standard multiplication and addition the binary operation of an idempotent quasigroup will be denoted by "$*$". If $(Q, *)$ is an idempotent quasigroup, then the prolongation $\widehat{Q}$ is a loop upon $Q \cup \{1\}$ such that $1 \cdot x = x \cdot 1 = x$ and $xx = 1 = 1 \cdot 1$ for all $x \in Q$, and $xy = x * y$ for all $x, y \in Q$, $x \neq y$. This definition assumes that $1 \notin Q$. If the latter is not true, then the unit element of $\widehat{Q}$ is chosen in another way.

The relationship of $\mathbf{a}(Q)$ and $\mathbf{a}(\widehat{Q})$ follows from the ensuing theorem. The proof is not difficult and appears in Section 2.

Theorem 1.1. *Let $(Q, *)$ be an idempotent quasigroup of order $n-1 \geq 1$. Then*

$$\begin{aligned} \mathbf{a}(\widehat{Q}) &= 3n^2 - 3n + 1 + \mathbf{a}(Q) + \sum_{y \in Q} (l_y + r_y + s_y), \ \textit{where} \\ l_y &= |\{x \in Q \colon y \neq x \textit{ and } y = (y * x) * x\}|, \\ r_y &= |\{x \in Q \colon y \neq x \textit{ and } y = x * (x * y)\}|, \ \textit{and} \\ s_y &= |\{x \in Q \colon y \neq x \textit{ and } y = x * (y * x)\}|. \end{aligned}$$

Let $(G, +)$ be an abelian group. A mapping $\psi \colon G \to G$ is said to be an orthomorphism [5], [7] if G is permuted by both $x \mapsto \psi(x)$ and $x \mapsto \psi(x) - x$.

If ψ is an orthomorphism, then

$$x * y = x + \psi(y - x)$$

defines upon G a quasigroup. Each translation $x \mapsto a + x$ is an automorphism of this quasigroup, and the quasigroup is idempotent if and only if $\psi(0) = 0$. Orthomorphisms with $\psi(0) = 0$ are said to be *canonical*.

For a permutation μ of a set X put $\mathrm{Fix}(\mu) = \{x \in X \colon \mu(x) = x\}$. Note that an automorphism ψ of abelian group G is an orthomorphism if and only if $\mathrm{Fix}(\psi) = \{0\}$. Such automorphisms are called *fixed point free*.

Let $(Q, *)$ be a quasigroup. Then $x *^{\mathrm{op}} y = y * x$ defines the *opposite quasigroup* $(Q, *^{\mathrm{op}})$. If $x * y = x + \psi(y - x)$, where ψ is an orthomorphism of $(G, +)$, then $x *^{\mathrm{op}} y = x + \varphi(y - x)$, where $\varphi(x) = x + \psi(-x)$. The mapping φ is also an orthomorphism of $(G, +)$, and $\psi(x) = x + \varphi(-x)$. These facts allow to subject orthomorphisms to mirror arguments.

Theorem 1.2. *Let ψ be a canonical orthomorphism of a group $(G,+)$. Let $x*y = x+\psi(y-x)$. Put $\varphi(x) = x+\psi(-x)$ for all $x, y \in G$. If $y \in G$, then*

$$l_y + 1 = |\operatorname{Fix}(\varphi^2)|, \quad r_y + 1 = |\operatorname{Fix}(\psi^2)| \text{ and } s_y + 1 = |\operatorname{Fix}(\psi\varphi)| = |\operatorname{Fix}(\varphi\psi)|.$$

The latter statement is a direct consequence of Proposition 2.3.

Combining Theorems 1.1 and 1.2 with recently described constructions, see [2], [4], of maximally nonassociative quasigroups leads to the following result, the proof of which fills the bigger part of Section 2.

Theorem 1.3. *Let n be an integer such that $n-1$ is a prime greater than or equal to* 13 *or $n-1 = p^{2k}$, p an odd prime, $k \geq 1$. Then there exists an involutory loop of order n with exactly $3n^2 - 2n$ associative triples.*

Many orders not covered by Theorem 1.3 can be obtained by prolongation of a known maximally nonassociative quasigroup too. However, to get a more comprehensive result seems to require proofs that would make the paper more technical than has been our desire.

In the future there might be discovered other constructions, perhaps even simpler. Our guess is that there exists $N < 20$ such that an involutory loop of order n with exactly $3n^2 - 2n$ associative triples exists for all $n \geq N$.

A quasigroup Q is said to be *maximally nonassociative* if every associative triple (x, y, z) satisfies $x = y = z$. If Q is a quasigroup of order n, then $\mathbf{a}(Q) \geq n$. The equality holds if and only if Q is maximally nonassociative. Each maximally nonassociative quasigroup is idempotent (this is easy to prove, see [6], [3]).

The existence of maximally nonassociative quasigroups was an open question since 1980, see [6], till 2018, see [3]. The generic constructions of papers [2] and [4] are described in Section 2.

Computations reported in this paper include a description of loops of order $n \leq 9$ with the lowest possible number of associative triples. This is summarized in Table 1.1. Details appear in Section 4.

n	1	2	3	4	5	6	7	8	9
general	1	8	27	64	74	104	146	186	233
involutory	1	–	–	64	89	116	153	201	253

Table 1.1. The minimal number of associative triples for general and involutory loops of order $n \leq 9$.

Call $\mathbf{a}(Q) - (3n^2 - 3n + 1)$ the *surplus* of associative triples whenever Q is a loop of order n. For Q involutory define the *(involutory) surplus* as $\mathbf{a}(Q) - (3n^2 - 2n)$. The surpluses appear in Table 1.2.

n	1	2	3	4	5	6	7	8	9	10
general	0	1	8	27	13	13	20	17	16	$\leq$11
involutory	0	–	–	24	24	20	21	25	28	0

Table 1.2. The minimal surpluses of associative triples for loops of order $n \leq 9$, and for involutory loops of order $n \leq 10$.

Section 3 is concerned with a construction dubbed *double prolongation*. This construction also starts from a quasigroup defined upon an abelian group G by $x * y = x + \psi(y - x)$. The first prolongation deals with a transversal $\{(x, x + d)\colon x \in G\}$, where $d \neq 0$ is fixed. This yields another idempotent quasigroup, and that quasigroup is then standardly prolonged to a loop.

It turns out that extremal involutory loops of orders 7 and 9 can be produced by double prolongation. Otherwise the construction of double prolongation does not seem to be of much importance. However, there is an open question worth attention whether a similar construction using another type of transversal might yield a prolongation of a maximally nonassociative quasigroup into another maximally nonassociative quasigroup.

2. Prolongations by an element

The following easy fact is often handy:

Lemma 2.1. *Let $(Q, *)$ be an idempotent quasigroup. If $x, y \in Q$ and $x \neq y$, then none of the triples (x, x, y), (y, x, x), $(x, y, x*y)$ and $(y*x, y, x)$ is associative.*

Proof: Indeed, $x * (x * y) = (x * x) * y$ implies $x * (x * y) = x * y = (x * y) * (x * y)$, and that yields $x * y = x = x * x$ and $x = y$, by cancellation. Similarly, $x * y = (x * y) * (x * y) = x * (y * (x * y))$ implies $y = y * y = y * (x * y)$, $y = y * y = x * y$ and $x = y$. □

Let y be an element of an idempotent quasigroup Q. Define l_y, r_y and s_y as in Theorem 1.1, and put

$$t_y = |\{x \in Q\colon\ x \neq y \ \text{ and } \ y = (x * y) * x\}|.$$

Lemma 2.2. *Let $(Q, *)$ be an idempotent quasigroup. Then $\sum_y s_y = \sum_y t_y$.*

Proof: Denote by S the set of all $(x, y) \in Q \times Q$ such that $x \neq y$ and $y = x * (y * x)$. Define $T \subset Q \times Q$ by changing the latter condition to $y = (x * y) * x$. Since $|S| = \sum s_y$ and $|T| = \sum t_y$, it suffices to find a bijection $S \to T$. Note that $y = x * (y * x)$ if and only if $(x * (y * x)) * x = y * x$. The sought bijection can be obtained by restricting the permutation $(x,y)\mapsto(x,y*x)$ of $Q\times Q$ to S. Indeed, the mapping sends each (x,x) upon itself, and each element of $Q\times Q$ can be uniquely expressed in the form $(x,y*x)$. $\square$

We are now ready to prove Theorem 1.1.

Proof of Theorem 1.1: If $1\in\{x,y,z\}$, then $x\cdot yz = xy\cdot z$. This yields $3n^2-3n+1$ associative triples. Let $x,y\in Q$ be such that $x\neq y$. Then $(x*x)*y\neq x*(x*y)$ and $y*(x*x)\neq(y*x)*x$, by Lemma 2.1, while $xx\cdot y = x\cdot xy$ if and only if $y=x*(x*y)$, and $y\cdot xx = yx\cdot x$ if and only if $y=(y*x)*x$. The prolongation thus brings $\sum_y(l_y+r_y)$ additional associative triples of the form (x,x,y) or (y,x,x), where $x,y\in Q$ and $x\neq y$.

Consider now a triple $(x,y,z)\in Q^3$ such that $x\neq y$ and $y\neq z$. If $x=y*z$, then (x,y,z) is not associative in Q by Lemma 2.1. Similarly, (x,y,z) is not associative in Q if $z=x*y$. If none of $x=y*z$ and $z=x*y$ is true, then (x,y,z) is associative in Q if and only if it is associative in $\widehat{Q}$, yielding thus $\mathbf{a}(Q)-(n-1)$ associative triples. If exactly one of the equations holds, then the triple is not associative in any of the two quasigroups. If both equations hold, then the triple is associative in $\widehat{Q}$, but not in Q. This results in an increase of $\sum s_y$ triples since the number of such triples is the same as the number of (x,y), $x\neq y$, with $x=y*(x*y)$.

This accounts for all associative triples (x,y,z) such that $x\neq y$ or $y\neq z$ or $1\in\{x,y,z\}$. What remains are $n-1$ triples (x,x,x), $x\neq 1$. $\square$

Proposition 2.3. *Let φ be an orthomorphism of an abelian group $(G,+)$. Set $\psi(x)=x+\varphi(-x)$ and $x*y=x+\psi(y-x)$ for all $x,y\in Q$. Then*

$$\begin{aligned}
y=x*(x*y) &\iff y-x\in \mathrm{Fix}(\psi^2);\\
y=(y*x)*x &\iff y-x\in \mathrm{Fix}(\varphi^2);\\
y=x*(y*x) &\iff y-x\in \mathrm{Fix}(\psi\varphi);\ \textit{and}\\
y=(x*y)*x &\iff y-x\in \mathrm{Fix}(\varphi\psi).
\end{aligned}$$

If φ is canonical, then $|\operatorname{Fix}(\psi\varphi)|=|\operatorname{Fix}(\varphi\psi)|$.

Proof: Fix $x,y\in G$. The equation $x*(x*y)=y$ translates into

$$x+\psi(x+\psi(y-x)-x)=y,$$

which is the same as $y-x\in\operatorname{Fix}(\psi^2)$. The case of $y=(y*x)*x$ follows by a mirror argument, and $y=x*(y*x)=x*(x*^{\mathrm{op}}y)$ if and only if $y=x+\psi(\varphi(y-x))$.

It remains to prove that if φ is canonical, then $|\operatorname{Fix}(\psi\varphi)|=|\operatorname{Fix}(\varphi\psi)|$. Put $n=|G|$. By the earlier part of the proof is $\sum(s_y+1)=n|\operatorname{Fix}(\psi\varphi)|$, while $\sum(t_y+1)=n|\operatorname{Fix}(\varphi\psi)|$. The rest follows from Lemma 2.2. $\square$

Theorem 1.2 is a direct consequence of Proposition 2.3.

Proposition 2.4. *Let $(G,+)$ be an abelian group and ψ an orthomorphism of G. Put $x * y = x + \psi(y-x)$ for all $x, y \in G$. A triple $(u,v,w) \in G^3$ is associative in $(G,*)$ if and only if*

$$\psi(\psi(x)+y) - \psi(y) = \psi(x+y-\psi(y)), \tag{2.1}$$

where $y = v - u$ and $x = w - v$. If $\psi \in \mathrm{Aut}(G)$, then (u,v,w) is associative if and only if $u = w$.

Proof: If $(u,v,w) \in G^3$, then $u*(v*w) = u + \psi((v*w)-u) = u + \psi((v-u) + \psi(w-v))$ and $(u*v)*w = (u+\psi(v-u))*w = u+\psi(v-u)+\psi((w-u)-\psi(v-u))$. Thus $(u*v)*w = u*(v*w)$ if and only if $\psi(\psi(x)+y)-\psi(y) = \psi(x+y-\psi(y))$, where $y = v-u$ and $x = w-v$. If $\psi \in \mathrm{Aut}(G)$, then this is true if and only if $\psi^2(x) = \psi(y) + \psi(x - \psi(y))$, which is the same as $\psi^2(x+y) = \psi(x+y)$, and that is true if and only if $\psi(x+y) = x+y$. Now, ψ is assumed to be a fixed point free automorphism of the abelian group G. The latter condition thus means that $x+y=0$, i.e., $u = w$. □

Equation (2.1) will be called the *associativity equation*.

Corollary 2.5. *If κ is the number of solutions to the associativity equation, then $\mathbf{a}(G,*) = \kappa \cdot |G|$.*

The following statement gives an example defined on seven elements. It may be verified by direct computation.

Proposition 2.6. *Let ψ and φ be permutations of $\mathbb{Z}_7$ such that*

$$\psi = (1\,5\,6\,2\,4\,3) \quad \textit{and} \quad \varphi = (1\,3\,6\,4\,5\,2). \tag{2.2}$$

Both φ and ψ are canonical orthomorphisms of $\mathbb{Z}_7$, $\mathrm{Fix}(\varphi^2) = \{0\} = \mathrm{Fix}(\psi^2)$ and $\mathrm{Fix}(\psi\varphi) = \{0,1\}$. Put $x*y = x + \psi(y-x) = y + \varphi(x-y)$ for all $x,y \in \mathbb{Z}_7$. Solutions (x,y) to the associativity equation form the set

$$\{(0,0),(2,5),(3,4),(5,2),(5,6),(6,3)\}.$$

Corollary 2.7. *Let Q be the idempotent quasigroup upon $\mathbb{Z}_7$ with operation $x + \psi(y-x)$, where ψ is as in (2.2). Then $\mathbf{a}(Q) = 42$ and $\mathbf{a}(\widehat{Q}) = 218$.*

Proof: Indeed, $\mathbf{a}(Q) = 6 \cdot 7$ by Corollary 2.5, and $\mathbf{a}(\widehat{Q}) = 169 + 42 + 7$ by Theorems 1.1 and 1.2. □

Denote by Q the quasigroup obtained from (2.2). The quasigroup yields an optimal solution neither for idempotent quasigroups of order 7, nor for involutory quasigroups of order 8. Nevertheless, there exists a double prolongation of Q that yields an optimal solution for involutory quasigroups of order 9. This is shown in Section 3.

We now turn to the two generic constructions of maximal nonassociative quasigroups. The first of them, see [2], is based upon a (left) nearfield, say N. (Axioms of a nearfield are nearly the same as of a field. The only difference is that the distributivity is assumed only from the left. If "$\circ$" denotes the multiplication of N, then $x \circ (y + z) = x \circ y + x \circ z$ for all $x, y, z \in N$, while there may exist $x, y, z \in N$ such that $(y + z) \circ x \neq y \circ x + z \circ x$. A nearfield N is called *proper* if such a triple (x, y, z) exists.)

Here we shall consider only the *quadratic nearfields*, see [1]. They are defined upon $\mathbb{F}_{q^2}$, the finite field of order q^2, $q > 1$, an odd prime power, by

$$x \circ y = \begin{cases} xy & \text{if } x \text{ is a square;} \\ xy^q & \text{if } x \text{ is a nonsquare.} \end{cases}$$

Define an operation "$*_c$" by

$$x *_c y = x + (y - x) \circ c \quad \text{for all } x, y \in N, \text{ where } c \in N \setminus \{0, 1\}. \tag{2.3}$$

The operation of the opposite quasigroup is given by $x *_c^{\mathrm{op}} y = x + (y - x) \circ (1 - c)$. Thus $(N, *_c^{\mathrm{op}}) = (N, *_{1-c})$. To apply results above denote by ψ the mapping $x \mapsto x \circ c$ and by φ the mapping $x \mapsto x \circ (1 - c)$.

Theorem 2.8. *Let $Q = (N, *_c)$, where N is a quadratic nearfield of order q^2. Put $n = q^2 + 1$. If $c \in N$ is such that the quasigroup $(N, *_c)$ is maximally nonassociative, then $\mathbf{a}(\widehat{Q}) = 3n^2 - 2n$.*

Proof: Let $(N, *_c)$ be maximally nonassociative. Then at least one of c and $1-c$ has to be a nonsquare in $\mathbb{F}_{q^2}$, by [2, Proposition 3.2]. By Theorems 1.1 and 1.2 we have to prove that 0 is the only point fixed by any of ψ^2, φ^2 and $\varphi\,\psi$. This means to show that there is no $x \in \mathbb{F}_{q^2}^*$ such that $x = (x \circ c) \circ c$ or $x = (x \circ (1 - c)) \circ (1 - c)$ or $x = (x \circ c) \circ (1 - c)$.

If c is a nonsquare, then $(x \circ c) \circ c = xc^{q+1}$ for all $x \in \mathbb{F}_{q^2}$. This is never equal to x if $x \neq 0$, since c is a square if $c^{q+1} = 1$. Suppose thus that c is a square. If x is square, then $(x \circ c) \circ c = xc^2$. If x is a nonsquare, then $(x \circ c) \circ c = x(c^2)^q$. Now $c^2 = 1 \Leftrightarrow (c^2)^q = 1 \Leftrightarrow c \in \{-1, 1\}$. Indeed, in every nearfield -1 and 1 are the only solutions to $x^2 = 1$ (cf. [3, Lemma 3.2] for a short proof). However, if $c \in \mathbb{F}_q$, then $1 - c$ cannot be nonsquare since all elements of $\mathbb{F}_q$ are squares in $\mathbb{F}_{q^2}$. Hence $\mathrm{Fix}(\psi^2) = \{0\}$. By mirror argument, $\mathrm{Fix}(\varphi^2) = \{0\}$ as well.

It remains to consider the equality $x = (x \circ c) \circ (1 - c)$, $x \neq 0$. At least one of c and $1 - c$ has to be a nonsquare. Values of c and $1 - c$ are interchangeable because of mirror arguments. Hence it may be assumed that c is a nonsquare. This will be brought to contradiction by proving that $c \in \mathbb{F}_q$. Now, $(x \circ c) \circ (1-c)$ equals $xc(1-c)^q$ if x is a square, and $xc^q(1-c)$ if x is a nonsquare. To conclude we thus need to show that $c^q(1-c) = 1$ implies $c \in \mathbb{F}_q$. Represent elements of $\mathbb{F}_{q^2}$ as sums $a + b\vartheta$, where $\vartheta^2 = d$ is a nonsquare in $\mathbb{F}_q$ and $a, b \in \mathbb{F}_q$. Assume that $c = a + b\vartheta$. Then $c^q(1-c) = (a - b\vartheta)(1 - a - b\vartheta) = (a - a^2 + b^2 d) - b\vartheta$. If this is equal to 1, then $b = 0$. □

Corollary 2.9. *If $q > 1$ is an odd prime power and $n = q^2 + 1$, then there exists an involutory loop of order n with exactly $3n^2 - 2n$ associative triples.*

Proof: This follows from Proposition 2.8 since for each quadratic nearfield N there exists $c \in N$ such that $(N, *_c)$ is maximally nonassociative, by [2, Theorem 5.6]. □

The other generic construction in [4] of maximally nonassociative quasigroups is that of $\psi = \psi_{a,b} \colon \mathbb{F}_q \to \mathbb{F}_q$, where $q > 1$ is an odd prime power and $a, b \in \mathbb{F}_q$ are such that both ab and $(1-a)(1-b)$ are nonzero squares:

$$\psi(x) = \begin{cases} ax & \text{if } x \text{ is a square,} \\ bx & \text{if } x \text{ is a nonsquare.} \end{cases} \tag{2.4}$$

These orthomorphisms are often called *quadratic*, cf. [5], [8].

Lemma 2.10. *Let $\psi = \psi_{a,b}$ be a quadratic orthomorphism over a finite field $\mathbb{F}_q$, $q > 1$ an odd prime power. Put $n = q+1$ and $Q = (\mathbb{F}_q, *)$, where $x*y = x+\psi(y-x)$ for all $x, y \in Q$. If none of a^2, b^2, $(1-a)^2$, $(1-b)^2$, ab, $(1-a)(1-b)$, $a(1-b)$, $b(1-a)$, $a(1-a)$ and $b(1-b)$ is equal to 1, then $\mathbf{a}(\widehat{Q}) = 3n^2 - 3n + 1 + \mathbf{a}(Q)$.*

Proof: Denote by φ the permutation $x \mapsto x + \psi(-x)$. It is well known (and easy to verify) that $\varphi = \psi_{1-a,1-b}$ if $q \equiv 1 \bmod 4$, and $\varphi = \psi_{1-b,1-a}$ if $q \equiv 3 \bmod 4$. Hence if $x \in \mathbb{F}_q$ and y is equal to $\psi^2(x)$ or $\varphi^2(x)$ or $\psi\varphi(x)$, then y is equal to cx, where c is one of the elements in the list. The rest follows from Theorems 1.1 and 1.2. □

Proposition 2.11. *Let $q \equiv 1 \bmod 4$ be such a prime power that $q \neq 17$, and q is not divisible by 5. Put $n = q + 1$. There exists $a \in \mathbb{F}_q$ such that $\psi_{a,1-a}$ is a quadratic orthomorphism that determines a quasigroup the prolongation of which is an involutory loop with exactly $3n^2 - 2n$ associative triples.*

Proof: By Lemma 2.10 we are concerned with pairs (a, b) determining a maximally nonassociative quasigroup such that $a + b = 1$, $a^2 \neq 1$, $b^2 \neq 1$ and $ab \neq 1$. We shall check whether the latter inequalities are compatible with known examples of maximally nonassociative quasigroup. If $ab = 1$, then $a^2 = -b$ and

$b^2 = -a$. However, if both a and b are squares, then the quasigroup is not maximally nonassociative, by point (2) of [4, Theorem 3.5]. This means that $ab \neq 1$ is always true. If $a^2 = 1$ or $b^2 = 1$, then $a \in \{-1, 2\}$. Theorem 4.3 of [4] describes a procedure that was used to find $a \in \mathbb{F}_q$ such that $(a, 1-a)$ determines a maximally nonassociative quasigroup. We have observed that such an a may be used here if it differs from both -1 and 2. The procedure used in the proof [4, Theorem 4.3] finds a such that both a and $a-1$ are nonsquares unless $q \notin \{37, 49\}$. Such an a differs from both -1 and 2 since -1 is a square. For $q \in \{37, 49\}$ the value of a established in [4, Theorem 4.3] may be used as well. For $q = 37$ choose $a = 18$, and for $q = 49$ choose $a = 3t$, assuming that $\mathbb{F}_{49}$ is represented by $\mathbb{Z}_7[t]/(t^2+t+3)$. □

Proposition 2.12. *Let $q \equiv 3 \bmod 4$ be a prime greater than or equal to 23. Put $n = q+1$. There exist $a, b \in \mathbb{F}_q$ such that $\psi_{a,b}$ is a quadratic orthomorphism that determines a quasigroup the prolongation of which is an involutory loop with exactly $3n^2 - 2n$ associative triples.*

Proof: Let us first assume that $b = 4a$. By [4, Lemma 4.4] it suffices to find a such that

$$\begin{aligned} &a,\ a-1,\ a+2,\ 4a-1 \ \text{ and } \ 16a-7 \text{ are squares,} \\ &\qquad\qquad \text{while } \ a-4,\ 4a-3,\ 4a+3 \ \text{ and } \ 16a-1 \ \text{ are nonsquares.} \end{aligned} \tag{2.5}$$

Suppose that $a \in \mathbb{F}_q$ fulfils these conditions. The question is which of the values mentioned in Lemma 2.10 may be, under these assumptions, equal to 1. If $a^2 = 1$, then $a = -1$. That cannot be since -1 is a nonsquare. If $b^2 = 16a^2 = 1$, then $a = \pm 1/4$. That cannot be since $-1/4$ is a nonsquare and $4(1/4)+3$ is a square. If $(1-a)^2 = 1$, then $a = 2$. This implies that 2 and 7 are squares, and 5, 11 and 31 are nonsquares. If that is true, then $a = 2$ fulfils (2.6). If $(1-4a)^2 = 1$, then $a = 1/2$. This cannot occur since if $1/2$ is a square, then $1/2 - 1$ is a nonsquare. If $4a^2 = 1$, then $a = \pm 1/2$. If $a = -1/2$, then $-(a-1) = 3/2 = a+2$. Hence both $a-1$ and $-(a-1)$ should be squares. That is not possible. The case $(ab)^2 = 1$ thus never arises. The conditions we work with exclude $a(1-4a) = 1$, $4a(1-a) = 1$ and $4a(1-4a) = 1$ since in each of these cases the term upon the left is a product of a square with a nonsquare. The only remaining case is that of $(1-a)(1-4a) = 1$. This gives $4a^2 - 5a = 0$. Hence $a = 5/4$. This is an admissible case that requires 5, 11 and 13 to be squares, while 2 and 19 have to be nonsquares.

We shall now show that the case $a = 2$ may be refuted. If $a = 2$, then $(1-a)^2 x = x$ for all $x \neq 0$. However this equation does not automatically imply that $\varphi^2(x) = x$ for some $x \neq 0$. Indeed, the permutation φ is defined so that $\varphi(x) = (1-b)x$ if x is a square, and $\varphi(x) = (1-a)x$ if x is a nonsquare. In our case $b = 4a$, and both $1-a$ and $1-b$ are assumed to be nonsquares. This means that $\varphi^2(x) = (1-a)(1-b)x$ for each $x \neq 0$. Therefore $\varphi^2(x) = x$ never occurs if $a = 2$ and $x \neq 0$.

The only value which may cause a difficulty thus is $a = 5/4$. By the proof of [4, Theorem 4.6] for $q > 1663$ there always exists $a \in \mathbb{F}_q$ that fulfils (2.6). This is achieved by using an argument based on Weil bound for large q, and using computer for the other values. For the purposes here the Weil bound argument has to be used with slightly different parameters than in [4] since we need to ascertain the existence of at least two different a fulfilling (2.6). The argument confirms the existence of two such values for $q > 3220479$. For $1663 < q < 3220479$ the existence of $a \neq 5/4$ was verified by computer.

For primes $19 \leq q \leq 1663$ a computer search was also performed. The goal was to find elements a and b such that both [4, Theorem 3.5] and Lemma 2.10 hold. When setting $b = 4a$ the search succeeded for all values except for 19, 47, 67 and 79. By allowing b general suitable values of a and b were found for 47, 67 and 79. They are $a_{47} = 3$, $b_{47} = 8$, $a_{67} = 5$, $b_{67} = 7$ and $a_{79} = 3$, $b_{79} = 43$, respectively. □

Corollary 2.13. *Let $q \geq 13$ be a prime number. Assume that $q \neq 19$ and put $n = q+1$. Then there exists a maximally nonassociative quasigroup Q determined by a quadratic orthomorphism, $|Q| = q$, such that $\mathbf{a}(\widehat{Q}) = 3n^2 - 2n$.*

PROOF: For $q = 17$ parameters $(a, b) = (4, 8)$ yield a maximally nonassociative quasigroup, by [4]. They also fulfil conditions of Lemma 2.10. For other values $q \equiv 1 \bmod 4$ use Proposition 2.11. The case $q \equiv 3 \bmod 4$ is treated by Proposition 2.12. □

The proof of Theorem 1.3 is nearly complete. By Corollaries 2.9 and 2.13 the only missing step is the proof that there exists an involutory loop of order 20 with 1160 associative triples. Such a loop is constructed below, again by a prolongation of an idempotent quasigroup. Quadratic orthomorphisms as defined by (2.4) cannot be used here since while there exist parameters (a, b) that yield a maximally nonassociative quasigroup, none of such quasigroups meets the conditions of Theorems 1.1 and 1.2. Another construction is needed.

Such a construction is given by formula (2.6). This formula defines a mapping $\psi\colon \mathbb{F}_q \to \mathbb{F}_q$, q an odd prime power $\equiv 1 \bmod 6$, based on parameters $a, b, c \in \mathbb{F}_q$. If ψ is an orthomorphism, then this orthomorphism is said to be *cubic*. (We do not claim that (2.6) provides an exhaustive definition of cubic orthomorphisms.)

Lemma 2.14 gives a list of conditions under which the mapping ψ of (2.6) is an orthomorphism. These conditions allow to construct a set of cubic orthomorphisms of order $q = 19$. The section ends by a report on computer search that ran through all cubic orthomorphisms of order 19 fulfilling conditions of Lemma 2.14. This search has revealed the existence of a cubic orthomorphism that can be prolonged to an involutory loop with 1160 associative triples, providing thus the missing piece in the proof of Theorem 1.3.

Suppose that a, b and c are elements of a finite field $\mathbb{F}_q$ in which 2 is not a cube (this implies that $q \equiv 1 \bmod 6$). Define a mapping $\psi = \psi_{a,b,c}\colon \mathbb{F}_q \to \mathbb{F}_q$ by

$$\psi(x) = \begin{cases} ax & \text{if } x \text{ is a cube,} \\ bx & \text{if } 2x \text{ is a cube,} \\ cx & \text{if } 4x \text{ is a cube.} \end{cases} \tag{2.6}$$

Lemma 2.14. *Let $q > 1$ be an odd prime power such that 2 is not a cube in $\mathbb{F}_q$. If a, b and c are elements of $\mathbb{F}_q \setminus \{0, 1\}$, then there exists exactly one mapping $\psi = \psi_{a,b,c}\colon \mathbb{F}_q \to \mathbb{F}_q$ for which (2.6) is true. This mapping is an orthomorphism if and only if none of*

$$2ab^{-1},\ \ 4ac^{-1},\ \ 2bc^{-1},\ \ 2(1-a)(1-b)^{-1},\ \ 4(1-a)(1-c)^{-1}\ \ \textit{and}\ \ 2(1-b)(1-c)^{-1}$$

is a cube.

Proof: Denote by C the set of nonzero cubes of $\mathbb{F}_q^*$. Note that C is a subgroup of index 3. We assume that $2 \notin C$. Thus $4 \notin C$ too. Indeed, if $4 = x^3$ for some $x \in \mathbb{F}_q^*$, then $(2/x)^3 = 2$. This means that cosets C, $2C$ and $4C$ are pairwise distinct. Hence C, $(1/2)C$ and $(1/4)C$ also are pairwise distinct cosets of C. That makes ψ well defined.

Let us now consider when ψ is a bijection. If x_1 and x_2 are elements of $\mathbb{F}_q^*$ such that $\psi(x_1) = \psi(x_2)$ and $x_1 \neq x_2$, then for some $u, v \in \mathbb{F}_q^*$ one of the following situations arises:

(1) $au^3 = bv^3/2 \ \Rightarrow\ 2ab^{-1} \in C$;
(2) $au^3 = cv^3/4 \ \Rightarrow\ 4ac^{-1} \in C$; and
(3) $bu^3/2 = cv^3/4 \ \Rightarrow\ 2bc^{-1} \in C$.

It follows that ψ permutes $\mathbb{F}_q$ if and only if none of $2ab^{-1}$, $4ac^{-1}$ and $2bc^{-1}$ is a cube. For ψ to be an orthomorphism we need that $\varphi(x) = x - \psi(x)$ also permutes $\mathbb{F}_q$. To complete the proof note that $\varphi = \psi_{a',b',c'}$, where $a' = 1-a$, $b' = 1-b$ and $c' = 1-c$. $\square$

By checking all cubic orthomorphisms of order 19 that can be constructed via Lemma 2.14, we found that 24 of them provide a maximally nonassociative quasigroup. The prolongation of 18 of them yields a loop with 1160 associative triples. These 18 loops form six isomorphism classes, which may be partitioned into three pairs of classes formed by mutually opposite loops.

One of the orthomorphisms yielding an extremal loop was obtained by means of parameters $a = 4$, $b = 9$ and $c = 10$. It is equal to

$$(1\ 4\ 17\ 18\ 15\ 2)(3\ 11\ 6\ 16\ 8\ 13)(5\ 12\ 10\ 14\ 7\ 9).$$

3. Prolongations by two elements

Let G be an abelian group and let ψ be a canonical orthomorphism of G. Define φ by $x \mapsto x + \psi(-x)$. Set $x * y = x + \psi(y - x)$ for all $x, y \in G$, and recall that $x * y = y *^{\mathrm{op}} x$ may be expressed as $y + \varphi(x - y)$.

Suppose that $e \notin G$, $d \in G$, $d \neq 0$, and define upon $G_e = G \cup \{e\}$ a binary operation "$\circledast$" by

$$\begin{aligned} e \circledast e &= e,\\ e \circledast x &= x + \varphi(-d),\\ x \circledast e &= x + \psi(d),\\ x \circledast (x + d) &= e, \quad \text{and}\\ x \circledast y &= x * y \ \text{ if } \ y - x \neq d, \end{aligned}$$

where $x, y \in G$.

The operation "$\circledast$" is idempotent since "$*$" is idempotent. Note that $(x - d) * x = x - d + \psi(d) = x + \varphi(-d) = e \circledast x$, $(x - d) \circledast x = e = x \circledast (x + d)$ and $x * (x + d) = x + \psi(d) = x \circledast e$. The operation table of "$\circledast$" thus arises from that of "$*$" by moving the content of each of the cells $(x, x + d)$ along the vertical and horizontal lines to the newly formed row and column of e, and replacing the content of the cell by e. Each of the rows and columns of the newly formed table thus permutes G_e. In fact, the construction of "$\circledast$" is nothing else but a prolongation along a transversal that is different from the main diagonal. Since we start from an idempotent quasigroup and the transversal is disjoint with the main diagonal, the resulting quasigroup is idempotent as well.

Note that replacing the triple (φ, ψ, d) with $(\psi, \varphi, -d)$ yields a quasigroup that is opposite to $(G, \circledast)$. This makes possible arguments based on mirroring.

Lemma 3.1. *Assume $2\varphi(-d) \neq 0$ and $2\psi(d) \neq 0$. A triple (e, y, e) is associative for every $y \in G_e$. If $d = 2\psi(d)$, then the triple $(x, e, x + d + \psi(d))$ is associative for each $x \in G$. All other triples of the form (x, e, z), where $x, z \in G$, can be expressed as $(x, e, x + u + \psi(d))$, where $u \in G$ fulfils $\psi(d) + \psi(u) = \psi(d + u + 2\varphi(-d))$. If u satisfies the latter equation, then $u \neq d$. In $(G_e, \circledast)$ there exists no other associative triple (x, y, z) such that $e \in \{x, y, z\}$.*

Proof: Let $(x, y, z) \in G_e^3$ be an associative triple such that $e \in \{x, y, z\}$. Suppose first that $e = y$. By Lemma 2.1 it may be assumed that $x, z \in G$. Then $x \circledast$

$(e \circledast z) = x \circledast (z+\varphi(-d))$ is equal to $x+\psi(z-x+\varphi(-d))$ if $x+d \neq z+\varphi(-d)$, and to e otherwise. On the other hand, $(x \circledast e) \circledast z = x+\psi(d)+\psi(z-x-\psi(d))$ unless $z = x+d+\psi(d)$. Both sides of the associativity equation thus yield e if and only if $z = x+d-\varphi(-d) = x+d+\psi(d)$. This is the same as $-\varphi(-d) = \psi(d)$ and as $d = 2\psi(d)$. If both sides of the associativity equation differ from e, then they are equal if $\psi(d)+\psi(z-x-\psi(d)) = \psi(z-x+\varphi(-d))$. To see that each such equation yields an associative triple it suffices to observe that this equation is compatible neither with $x+d = z+\varphi(-d)$, nor with $z = x+d+\psi(d)$. Indeed, the former case implies $2\varphi(-d) = 0$ and the latter case yields $2\psi(d) = 0$.

Let us now assume that $y \in G$. Then $(e \circledast y) \circledast e = y+\varphi(-d)+\psi(d) = e \circledast (y \circledast e)$. The case of $x \in G$ and $z = e$ is mirror symmetric to the case $x = e$ and $z \in G$. Hence only the latter will be considered. We have $(e \circledast y) \circledast z = (y+\varphi(-d)) \circledast z$. If $z = y+d$, then $e \circledast (y \circledast z) = e \neq (e \circledast y) \circledast z$.

Let us have $z \neq y+d$. Then $e \circledast (y \circledast z) = y+\psi(z-y)+\varphi(-d)$. This is never equal to $y+\varphi(-d)+\psi(z-y-\varphi(-d))$. □

Lemma 3.2. *Suppose that $t = 0$ is the only solution to each of the equations*

$$t+\psi(d) = \psi(d+\psi(t)) \quad \text{and} \quad t+\varphi(-d) = \varphi(-d+\varphi(t)). \tag{3.1}$$

Then there is no triple $(x,y,z) \in G^3$ associative in $(G_e, \circledast)$ for which $y = x+d$ or $z = y+d$.

Proof: Because of mirror symmetry, only the case $y = x+d$ will be considered. In this case $(x \circledast y) \circledast z = z+\varphi(-d)$. If $z = y+d$, then $x \circledast (y \circledast z) = x \circledast e = x+\psi(d) = z-2d+\psi(d) = z-d+\varphi(-d) \neq (x \circledast y) \circledast z$ since $d \neq 0$. Hence $z \neq y+d$ may be assumed.

Note that $y \circledast z = x+d$ if and only if $y = z$ since $y = x+d$. Thus $y \circledast z \neq x+d$ and $y \neq z$ also may be assumed, by Lemma 2.1. Therefore $x \circledast (y \circledast z) = x \circledast (x+d+\psi(z-x-d)) = x+\psi(d+\psi(z-x-d))$. On the other hand $(x \circledast y) \circledast z = e \circledast z = z+\varphi(-d) = x+(z-x-d)+\psi(d)$. The associativity thus implies $v+\psi(d) = \psi(d+\psi(v))$, where $v = z-x-d$. If $v = 0$, then $z = x+d = y$. However, we are assuming that $y \neq z$. □

Lemma 3.3. *If $(x,y,z) \in G^3$, then the following is equivalent:*

(i) $x \circledast (y \circledast z) = e = (x \circledast y) \circledast z$;
(ii) $z = (x * y)+d$ *and* $y * z = x+d$; *and*
(iii) $x = y+u$ *and* $z = y+d+\varphi(u)$, *where* $u \in G$ *is such that* $\psi(\varphi(u)+d) = u+d$.

If $(x,y,z) \in G^3$ satisfies these conditions, then $x*(y*z) \neq (x*y)*z$.

Proof: The first step is to show that if $y = x+d$ or $z = y+d$, then none of (i) and (ii) may be true. Indeed, if $y = x+d$, then $(x \circledast y) \circledast z = e \circledast z \neq e$, while $y * z = x + d$ implies $y = z$, and $z - d = x$ is not equal to $x * y$. Similarly, $z - d = y = x * y$ implies $x = y$, and then $x + d = z \neq y * z$.

The equivalence of (i) and (ii) may be thus proved under the assumption that $x \circledast y = x * y$ and $y \circledast z = y * z$. Then $x \circledast (y \circledast z) = e$ if and only if $x + d = y * z$, and $e = (x \circledast y) \circledast z$ if and only if $z - d = x * y$. Hence (i) $\Leftrightarrow$ (ii).

Now $y * z = x + d$ for $z = (x * y) + d = x + d + \psi(y - x)$ if and only if $y + \psi(x + d + \psi(y - x) - y) = x + d$. This is the same as $\psi(\varphi(x - y) + d) = (x - y) + d$.

Suppose now that (x, y, z) fulfils (i)–(iii) and is associative in $(G, *)$. Then there exists $u \in G$ such that $\psi(\varphi(u) + d) = u + d$, $x * (y * z) = x * (y * (y + d + \varphi(u)) = x * (y + \psi(\varphi(u) + d)) = x * (y + u + d) = x * (x + d) = x + \psi(d)$, $(x * y) * z = (z - d) * z = z - d + \psi(d)$, and thus $y + \varphi(u) = z - d = x = y + u$. This implies $u = 0$. However $\psi(\varphi(0) + d) = \psi(d) \neq d = 0 + d$ since $d \neq 0$. $\square$

Proposition 3.4. *Let $(G_e, \circledast)$ be the idempotent quasigroup given by an orthomorphism ψ of $(G, +)$ and an element $d \in G$, $d \neq 0$. For each $u \in G$ there exists an automorphism of $(G_e, \circledast)$, $e \mapsto e$ and $x \mapsto u + x$ for every $x \in G$.*

Let $(u, v, w) \in G^3$ be such that $(u \circledast v) \circledast w \neq e$ and suppose that none of equations (3.1) *possesses a nontrivial solution. Then (u, v, w) is associative in $(G_e, \circledast)$ if and only if $(u, v, w) = (v - y, v, v + x)$, where $(x, y) \in G^2$ is a solution to the associativity equation* (2.1) *such that $d \notin \{x, y, x - \varphi(-y), \psi(x) + y\}$.*

Proof: The fact that each $u \in G$ induces an automorphism of $(G_e, \circledast)$ may be derived from the definition of "$\circledast$" in a straightforward manner. Suppose that $(u, v, w) \in G^3$ is an associative triple in $(G_e, \circledast)$. By Lemma 3.2, $u \circledast v = u * v$ and $v \circledast w = v * w$. If $(u \circledast v) \circledast w \neq e$, then $u * (v * w) = u \circledast (v \circledast w) = (u \circledast v) \circledast w = (u * v) * w$.

The question thus is which triples (u, v, w) that are associative in $(G, *)$ are also associative in $(G_e, \circledast)$. If $d = v - u$ or $d = w - v$, then the triple is not associative, by Lemma 3.2. With these triples excluded, we have also to exclude the triples in which $(u * v) \circledast w = e$, or $u \circledast (v * w) = e$. By Proposition 2.4, each associative triple of $(G, *)$ can be uniquely expressed as $(v - y, v, v + x)$ where (x, y) is a solution to the associativity equation. Because translations of G yield automorphisms of $(G_e, \circledast)$ only the triples $(-y, 0, x)$ have to be tested. Hence $d \neq y$, $d \neq x$, $d \neq x - (-y * 0) = x + y - \psi(y) = x - \varphi(-y)$ and $d \neq (0 * x) + y = \psi(x) + y$. $\square$

Proposition 3.5. *Let "$\circledast$" be given by $G = \mathbb{Z}_7$, by the orthomorphism ψ described in* (2.2), *and by $d = 3$. Then $\mathbf{a}(\mathbb{Z}_7 \cup \{e\}, \circledast) = 36$. The set of associative triples consists of (e, e, e), (e, v, e) (v, v, v), $(v + 1, v, v - 2)$, $(v + 2, v, v + 2)$ and $(v, e, v + 3)$, where v runs through $\mathbb{Z}_7$.*

Proof: Triples (e, e, e) and (e, v, e) come from Lemma 3.1 directly. To locate the other triples described by Lemma 3.1 note that $2\psi(d) = 5 \neq 3 = d$, and that

$\psi(d) + \psi(u) = \psi(u) + 1$ is equal to $\psi(d + u + 2\varphi(-d)) = \psi(u - 1)$ if and only if $u = 2$. This gives triples $(v, e, v + 3)$. Since there is only a trivial solution to equations (3.1), the solution pairs $(6, 3)$ and $(3, 4)$ do not induce associative triples of "$\circledast$". The pair $(5, 2)$ may be removed too, by Proposition 3.4, since $5-\varphi(-2) = 3$. This leaves us with pairs $(0, 0)$, $(5, 6)$ and $(2, 5)$, by Proposition 2.6. There are no associative triples $(x, y, z) \in G^3$ with $x \circledast (y \circledast z) = e$ since there is no $u \in G$ fulfilling $\psi(\varphi(u)+3) = u+3$, as demanded by point (iii) of Lemma 3.3. $\square$

Lemma 3.6. *Assume that $\psi \in \mathrm{Aut}(G)$, $2d \neq 0$ and $\mathrm{Fix}(\varphi^2) = \mathrm{Fix}(\psi^2) = \{0\}$. The four elements $u - d$, $u + d$, $u + \varphi^{-1}(d)$ and $u - \psi^{-1}(d)$ are pairwise distinct for each $u \in G$. A triple $(u, v, u) \in G^3$ is associative in $(G_e, \circledast)$ if and only if v avoids any of these four elements. All other triples $(u, v, w) \in G^3$ associative in $(G_e, \circledast)$ satisfy $e = (u \circledast v) \circledast w$ and $u \neq w$.*

Proof: Firstly note that each of the equations in (3.1) possesses a trivial solution only since $\mathrm{Fix}(\varphi^2) = \mathrm{Fix}(\psi^2) = \{0\}$. Secondly note that conditions in point (iii) of Lemma 3.3 cannot be satisfied if $x = z$. Indeed, if they had been satisfied, we would have $d + \varphi(u) = u$ and $\psi(u) = u + d$ for some $u \in G$. By summing these two equations we obtain $d + u = 2u + d$. That gives $u = 0$ and $d = 0$, a contradiction.

Points d, $-d$, $\varphi^{-1}(d)$ and $-\psi^{-1}(d)$ are pairwise distinct since $2d \neq 0$ and $d = \varphi(d)+\psi(d) \neq 0$, and since $\psi \in \mathrm{Aut}(G)$ and $\psi(d) = -d$ imply that $\psi^2(d) = d$, while $\varphi(d) = -d$ implies $\varphi^2(d) = d$.

By Propositions 2.4 and 3.4 it remains to describe triples (u, v, u) such that $x = u - v$ fulfils $d \notin \{x, -x, x - \varphi(x), \psi(x) - x\}$. Conditions of the statement are that $x \notin \{d, -d, -\varphi^{-1}(d), \psi^{-1}(d)\}$. This is the same set of conditions since $x - \varphi(x) = \psi(x)$ and $\psi(x) - x = -\varphi(x)$. $\square$

Corollary 3.7. *Let φ and ψ be automorphisms of an abelian group $(G, +)$ such that φ^2, ψ^2 and $\varphi\psi$ are fixed point free, and $\varphi + \psi = \mathrm{id}_G$. Then $\mathbf{a}(G_e, \circledast) = (|G| - 1)^2$ whenever $d \in G$ is chosen so that $2d \neq 0$ and $d \neq 2\psi(d)$.*

Proof: Put $n = |G|$. Lemma 3.1 contributes $n+1$ associative triples (x, e, x), Lemma 3.3 contributes n triples since the equality $(\mathrm{id}_G - \varphi\psi)(u) = \psi(d) - d$ is satisfied by exactly one $u \in G$, and Lemma 3.6 yields $n^2 - 4n$ triples. $\square$

The next step is to prolong $(G_e, \circledast)$. Let us relate quantities l_y, r_y and s_y defined in Theorem 1.1 to operation "$\circledast$". E.g., l_y gives the number of $x \in G_e$ such that $y \neq x$ and $y = (y \circledast x) \circledast x$.

Lemma 3.8. *Suppose that $\mathrm{Fix}(\varphi^2) = \mathrm{Fix}(\psi^2) = \{0\}$, $2\psi(d) \neq 0$ and $2\varphi(-d) \neq 0$, and $\psi(d) \neq -d$ and $\varphi(-d) \neq d$. Then $l_y = r_y = 0$ for all $y \in G_e$. Furthermore, $s_e = 0$, and $s_y = |\mathrm{Fix}(\psi\varphi)| - 1 + \varepsilon - \eta$, where $\varepsilon = 1$ if $2\psi(d) = d$ and $\eta = 1$ if $\varphi\psi(d) = d$.*

Proof: Suppose that $x, y \in G$ and $x \neq y$. Then $x * (x * y) \neq y$, by Lemma 2.1. If $y = x + d$, then $x \circledast (x \circledast y) = x \circledast e = x + \psi(d) \neq x + d = y$. Assume $y \neq x + d$ and $x + d = x + \psi(y - x)$. Then $y = x + \psi^{-1}(d) \neq x + \psi(d) = x \circledast (x \circledast y)$, as $\mathrm{Fix}(\psi^2) = \{0\}$. To see that $r_y = 0$ it remains to observe that $e \circledast (e \circledast y) = y + 2\varphi(-d)$ is assumed to be different from y. The equation $x \circledast (x \circledast e) = e$ yields $x \circledast (x + \psi(d)) = e$. That is never satisfied as $\psi(d) \neq d$. Thus $r_y = 0$ for all $y \in G_e$. By mirror argument, $l_y = 0$ for all $y \in G$ as well.

To see that $s_e = 0$, observe that $x \circledast (e \circledast x) = x \circledast (x + \varphi(-d))$ is equal to e if and only if $\varphi(-d) = d$. Consider now the equation $e \circledast (y \circledast e) = y$, where $y \in G$. This is true if and only if $\varphi(-d) + \psi(d) = 0$, which is the same as $2\psi(d) = d$.

If $x = y + d$, then $x \circledast (y \circledast x) = x + \psi(d) = y + d + \psi(d)$ is equal to y if and only if $\psi(d) = -d$. Since we are assuming that $\psi(d) \neq -d$ we may consider only cases $x \neq y + d$. Then $x \circledast (y \circledast x) = x \circledast (y + \psi(x - y))$. This gives e if $(x - y) + d = \psi(x - y)$, and that is the same as $d = \varphi(y - x)$. Such an x always exists since $y - x = -d$ yields $\varphi(-d) = d$. Hence $y \neq x \circledast (y \circledast x)$ if $x = y - \varphi^{-1}(d)$. If $y - x \notin \{-d, \varphi^{-1}(d)\}$, then $x \circledast (y \circledast x) = x * (y * x) = x + \psi\varphi(y - x)$ is equal to y if and only if $y - x \in \mathrm{Fix}(\psi\varphi)$. If $y - x = \varphi^{-1}(d)$, then the latter is equivalent to $\psi(d) = \varphi^{-1}(d)$, which is the same as $d \in \mathrm{Fix}(\varphi\psi)$. □

Proposition 3.9. *Put $Q = (G_e, \circledast)$, where $G = \mathbb{Z}_7$, $d = 3$ and ψ is described by (2.2). Then $\mathbf{a}(\widehat{Q}) = 253$.*

Proof: Use Theorem 1.1, Proposition 3.5 and Lemma 3.8. By Proposition 2.6, $\mathrm{Fix}(\varphi^2) = \mathrm{Fix}(\psi^2) = \{0\}$ and $\mathrm{Fix}(\varphi\psi) = \{0, 1\}$. Since G is of odd order, both $2\psi(d) \neq 0$ and $2\varphi(-d) \neq 0$ are true. Furthermore, $\psi(3) = 1 \neq 4$, $\varphi(4) = 5 \neq 3$ and $2\psi(3) = 2 \neq 3$. Also $\varphi\psi(3) = 3$. Thus $s_y = r_y = l_y = 0$ for all $y \in G_e$, and $\mathbf{a}(\widehat{Q}) = 217 + \mathbf{a}(Q) = 253$. □

Table 3.1 carries the operational table of a loop isomorphic to the loop $\widehat{Q}$ of Proposition 3.9. Elements of $\mathbb{Z}_7$ are represented by $1, 2, \dots, 7$, the element e by 8, and the added neutral element by 0.

Proposition 3.10. *Let G be an abelian group, and let Q be the loop $(G_e, \circledast)$ determined by $\varphi, \psi \in \mathrm{Aut}(G)$, $\varphi + \psi = \mathrm{id}_G$, and by $d \in G$ such that $2d \neq 0$ and $d \neq 2\psi(d)$. If $\mathrm{Fix}(\varphi^2) = \mathrm{Fix}(\psi^2) = \mathrm{Fix}(\varphi\psi) = \{0\}$, then $\mathbf{a}(\widehat{Q}) = 4n^2 - 9n + 10$, where $n = |Q| = |G| + 2$.*

Proof: This follows from Theorem 1.1 and Corollary 3.7 if we show that $l_y = r_y = s_y$ for every $y \in Q$. By Lemma 3.8 this requires to show that $\psi(d) \neq -d$ and $\varphi(d) \neq -d$. However, if $\psi(d) = -d$, then $\psi^2(d) = \psi(-d) = d$. □

If conditions of Proposition 3.10 are satisfied for $G = (\mathbb{Z}_7, +)$, then $\mathbf{a}(\widehat{Q}) = 253$ too. However, computational results show that up to isomorphism there is only

	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	0	6	5	8	4	7	3	2
2	2	4	0	7	6	8	5	1	3
3	3	2	5	0	1	7	8	6	4
4	4	7	3	6	0	2	1	8	5
5	5	8	1	4	7	0	3	2	6
6	6	3	8	2	5	1	0	4	7
7	7	5	4	8	3	6	2	0	1
8	8	6	7	1	2	3	4	5	0

Table 3.1. Involutory loop of order 9 with 253 associative triples.

one involutory loop of order 9 with 253 associative triples. This seems to be a contradiction. But it is not. There is no loop of order 9 that can be obtained by means of Proposition 3.10. Indeed, there must exist $a, b \in \mathbb{Z}_7 \setminus \{0, 1\}$ such that $a + b = 1$, $\varphi(x) = ax$ and $\psi(x) = bx$. With mirroring in mind the only possible choices to consider are $(a, b) = (2, 6)$, $(a, b) = (3, 5)$ and $(a, b) = (4, 4)$, since $a \neq 1$. If $b = 6$, then $\psi^2 = \mathrm{id}_G$. If $(a, b) = (3, 5)$, then $\varphi\psi = \mathrm{id}_G$. If $(a, b) = (4, 4)$, then $2\psi(d) = d$ for every $d \in G$.

If it were possible to construct Q of order 7 by means of Proposition 3.10 we would have $\mathbf{a}(\widehat{Q}) = 143$. By Table 1.1 no such Q exists since an involutory loop of order 7 possesses at least 153 associative triples. In fact, there is only one such loop, up to isomorphism, and that loop may be constructed as follows:

Proposition 3.11. *Let Q be the loop $(G_e, \circledast)$ where $G = \mathbb{Z}_5$, $\varphi = \psi \in \mathrm{Aut}(G)$, $\varphi(x) = 3x$ for every $x \in G$, and $d = 3$. Then $\mathbf{a}(\widehat{Q}) = 153$.*

Proof: Let us first compute $\mathbf{a}(Q)$. We have $2d \neq 0$ and $d = 2\psi(d)$. Hence Lemma 3.1 contributes 11 associative triples. Clearly, $\mathrm{Fix}(\varphi^2) = \mathrm{Fix}(\varphi\psi) = \mathrm{Fix}(\psi^2) = \{0\}$. Therefore Lemma 3.3 yields 5 associative triples, and Lemma 3.6 yields additional 5 associative triples. Hence $\mathbf{a}(Q) = 21$. By Lemma 3.8, $s_y = 1$ for each $y \in G$, while $s_e = 0$. Thus $\mathbf{a}(\widehat{Q}) = 127+21+5 = 153$, by Theorem 1.1. $\square$

Table 3.2 pictures the operational table of a loop isomorphic to the loop $\widehat{Q}$ of Proposition 3.11. Elements of $\mathbb{Z}_5$ are represented by $1, 2, \ldots, 5$, the element e by 6, and the added neutral element by 0.

By Proposition 3.4 loops pictured in Tables 3.1 and 3.2 possess a cyclic group of automorphisms of orders 7 and 5, respectively. It can be directly proved or verified by computer that these loops possess no other automorphisms.

	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	0	4	2	6	3	5
2	2	4	0	5	3	6	1
3	3	6	5	0	1	4	2
4	4	5	6	1	0	2	3
5	5	3	1	6	2	0	4
6	6	2	3	4	5	1	0

Table 3.2. Involutory loop of order 7 with 153 associative triples.

4. Small loops

Some of the quasigroups considered in Section 3 are *medial* (synonymously *entropic*), which means that the *medial law* $(xy)(uv) = (xu)(yv)$ is fulfilled. By Toyoda's theorem, a quasigroup is medial if and only if the operation of the quasigroup can be expressed as $\varphi(x) + \psi(y) + c$, where the addition takes place in an abelian group $(G, +)$, c is a fixed element of G, and $\varphi, \psi \in \mathrm{Aut}(G, +)$ are commuting automorphisms. Such a quasigroup is idempotent if and only if $\varphi + \psi = \mathrm{id}_G$ and $c = 0$. Medial idempotent quasigroups thus are the quasigroups with operation $x + \psi(y - x)$, where ψ is a fixed point free automorphism of G.

As is well known, all loops of order 4 are groups. From that it easily follows that up to isomorphism there is only one idempotent quasigroup of order 4. This quasigroup is medial. Its operation may be expressed as $\varphi(x) + \varphi^{-1}(y)$, where φ is a fixed point free automorphism of $\mathbb{Z}_2 \times \mathbb{Z}_2$. Note that $|\varphi| = 3$.

It is easy to verify that up to isomorphism there is only one commutative medial quasigroup of order 5. This quasigroup can be expressed upon $\mathbb{Z}_5$ by the operation $3(x + y)$.

Proposition 4.1. *Let Q be an idempotent quasigroup.*

(i) *If $|Q| = 4$, then $\mathbf{a}(\widehat{Q}) = 89$.*
(ii) *If $|Q| = 5$, and Q is medial commutative, then $\mathbf{a}(\widehat{Q}) = 116$.*

Proof: By Proposition 2.4, $\mathbf{a}(Q) = |Q|^2$. We have $|\operatorname{Fix}(\varphi^2)| = |\operatorname{Fix}(\psi^2)| = 1$ and $|\operatorname{Fix}(\varphi\psi)| = 4$ in case (i), and $|\operatorname{Fix}(\varphi^2)| = |\operatorname{Fix}(\psi^2)| = |\operatorname{Fix}(\varphi\psi)| = 1$ in case (ii). Using Theorems 1.1 and 1.2 yields $\mathbf{a}(\widehat{Q})$ as $89 = 61 + 16 + 12$ in case (i), and as $116 = 91 + 25$ in case (ii). □

Computer results show that *up to isomorphism there is only one involutory loop Q of order n, $5 \leq n \leq 9$, such that $\mathbf{a}(Q)$ is equal to* 89*,* 116*,* 153*,* 201 *and* 253*, respectively.* Automorphism groups of these loops are of orders 24, 20, 5, 1 and 7. With the exception of order $n = 8$ such loops have been constructed in Propositions 3.9, 3.11 and 4.1. The remaining case of $n = 8$ is given in Table 4.1.

Up to isomorphism there exists a unique involutory loop of order 10 with 280 associative triples. This loop may be obtained by means of Theorem 2.8. Its uniqueness is a consequence of the uniqueness of maximally nonassociative quasigroup of order 9, see [3].

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

Table 4.1. Involutory loop of order 8 with 201 associative triples.

It remains to present loops L_n, $5 \le n \le 9$, with the least possible number of associative triples among all loops of order n. All these loops where found by an exhaustive computer search.

There are up to isomorphism two loops of order 5 with the minimal number of associative triples and they are mirror symmetric. The same applies for $n = 9$. For $n \in \{6, 7, 8\}$ the loop L_n is determined uniquely, up to isomorphism. The automorphism group of L_7 and L_8 is trivial, $\mathrm{Aut}(L_5)$ is generated by $(3\,4\,5)$, $\mathrm{Aut}(L_6)$ by $(3\,5)(4\,6)$ and $\mathrm{Aut}(L_9)$ by $(2\,4\,6\,7)(3\,9\,5\,8)$. Observe that loops L_6 and L_9 have two-sided inverses.

Let us finish by repeating the problem whether there exists a loop Q of order $n > 1$ such that $\mathbf{a}(Q) = 3n^2 - 3n + 1$. In fact, up to now we know no loop Q with $\mathbf{a}(Q) < 3n^2 - 2n$.

References

[1] Dickson L. E., *On finite algebras*, Nachr. Ges. Wiss. Göttingen (1905), 358–393.

[2] Drápal A., Lisoněk P., *Maximal nonassociativity via nearfields*, Finite Fields Appl. **62** (2020), 101610, 27 pages.

[3] Drápal A., Valent V., *Extreme nonassociativity in order nine and beyond*, J. Combin. Des. **28** (2020), no. 1, 33–48.

[4] Drápal A., Wanless I. M., *Maximally nonassociative quasigroups via quadratic orthomorphisms*, accepted in Algebr. Comb., available at arXiv:1912.07040v1 [math.CO] (2019), 13 pages.

	1	2	3	4	5
1	1	2	3	4	5
2	2	1	4	5	3
3	3	4	5	1	2
4	4	5	2	3	1
5	5	3	1	2	4

Table 4.2. Loop L_5 with 74 associative triples.

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	4	5	6	3
3	3	6	5	1	4	2
4	4	3	1	6	2	5
5	5	4	6	2	3	1
6	6	5	2	3	1	4

Table 4.3. Loop L_6 with 104 associative triples.

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

Table 4.4. Loop L_7 with 146 associative triples.

[5] Evans A. B., *Orthogonal Latin Squares Based on Groups*, Developments in Mathematics, 57, Springer, Cham, 2018.

[6] Kepka T., *A note on associative triples of elements in cancellation groupoids*, Comment. Math. Univ. Carolin. **21** (1980), no. 3, 479–487.

[7] Wanless I. M., *Diagonally cyclic Latin squares*, European J. Combin. **25** (2004), no. 3, 393–413.

[8] Wanless I. M., *Atomic Latin squares based on cyclotomic orthomorphisms*, Electron. J. Combin. **12** (2005), Research Paper 22, 23 pages.

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

TABLE 4.5. Loop L_8 with 186 associative triples.

	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9
2	2	9	1	3	4	5	6	7	8
3	3	1	8	6	7	2	9	4	5
4	4	7	2	5	3	9	8	6	1
5	5	6	4	8	9	1	2	3	7
6	6	3	7	2	1	8	5	9	4
7	7	8	5	9	6	4	3	1	2
8	8	4	9	7	2	3	1	5	6
9	9	5	6	1	8	7	4	2	3

TABLE 4.6. Loop L_9 with 233 associative triples.

A. Drápal:
DEPARTMENT OF ALGEBRA, CHARLES UNIVERSITY, SOKOLOVSKÁ 83,
186 75 PRAHA 8, CZECH REPUBLIC

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

J. Hora:
DEPARTMENT OF MATHEMATICS, FACULTY OF ENGINEERING,
CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE, KAMÝCKÁ 129,
165 21 PRAHA 6 - SUCHDOL, CZECH REPUBLIC

E-mail: horaj@tf.czu.cz

(*Received* May 28, 2020, *revised* July 15, 2020)