ALGEBRAIC
COMBINATORICS

Aleš Drápal & Ian M. Wanless

Maximally nonassociative quasigroups via quadratic orthomorphisms

Volume 4, issue 3 (2021), p. 501-515.

<http://alco.centre-mersenne.org/item/ALCO_2021__4_3_501_0>

Algebraic Combinatorics
Volume 4, issue 3 (2021), p. 501–515
https://doi.org/10.5802/alco.165

Maximally nonassociative quasigroups via quadratic orthomorphisms

Aleš Drápal & Ian M. Wanless

Abstract A quasigroup Q is called *maximally nonassociative* if for $x, y, z \in Q$ we have that $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ only if $x = y = z$. We show that, with finitely many exceptions, there exists a maximally nonassociative quasigroup of order n whenever n is not of the form $n = 2p_1$ or $n = 2p_1p_2$ for primes p_1, p_2 with $p_1 \leqslant p_2 < 2p_1$.

1. Introduction

The goal of this paper is to show that for most positive integers n there exists a quasigroup Q of order n such that

$$(1) \qquad \forall x, y, z \in Q\colon \quad x \cdot (y \cdot z) = (x \cdot y) \cdot z \implies x = y = z.$$

Recall that 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 $a, b \in Q$. Quasigroups discussed in this paper are finite. There is a natural correspondence between quasigroups of order n and Latin squares of order n.

Quasigroups satisfying (1) are said to be *maximally nonassociative*. This is because for each quasigroup Q of order n there are at least n triples $(a, b, c) \in Q^3$ such that $a \cdot (b \cdot c) = (a \cdot b) \cdot c$. If there are exactly n such triples, then each of them satisfies $a = b = c$, and the quasigroup is *idempotent*, i.e. $x \cdot x = x$ for each $x \in Q$. This was shown already in 1980 by Kepka [8]. Consequently, whenever Q is a maximally nonassociative quasigroup then it satisfies the reverse implication in (1) as well (cf. Lemma 2.1 below). Grošek and Horák [7] discussed a potential application in cryptography, but conjectured that maximally nonassociative quasigroups do not exist. Despite the effort of several authors [7, 8, 9] the existence of maximally nonassociative quasigroups was not established until 2018, when an example of order nine was found by a computer search [4]. This was followed by a paper [1], in which Drápal and Lisoněk proved that maximally nonassociative quasigroups exist for all orders p^2, where p is an odd prime, and also for the order 64. The main result of this paper is as follows:

Theorem 1.1. *A maximally nonassociative quasigroup of order n exists for all $n \geqslant 9$, with the possible exception of $n \in \{11, 12, 15, 40, 42, 44, 56, 66, 77, 88, 90, 110\}$ and orders of the form $n = 2p_1$ or $n = 2p_1p_2$ for odd primes p_1, p_2 with $p_1 \leqslant p_2 < 2p_1$.*

Manuscript received 4th August 2020, revised 28th November 2020, accepted 7th December 2020.

Keywords. Quasigroup, maximally nonassociative, quadratic orthomorphism, idempotent.

If Q_i are maximally nonassociative quasigroups of order n_i for $1 \leqslant i \leqslant k$, then the direct product $Q_1 \times \cdots \times Q_k$ is a maximally nonassociative quasigroup of order $n_1 \cdots n_k$. Therefore our first objective was to try to decide for which odd primes and which powers of 2 there exists a maximally nonassociative quasigroup of such an order. By [2, 3, 7] there exists no maximally nonassociative quasigroup of order < 9. The status of order 11 is not known. The existence of maximally nonassociative quasigroups for each prime order $p \geqslant 13$ is proved in Section 4.

If $n \geqslant m \geqslant 3$ and there exists a maximally nonassociative quasigroup of order n, then such a quasigroup also exists for order nm. This is proved in Section 2 by means of a specific product construction. This construction allows us to develop maximally nonassociative quasigroups of all orders 2^k, for $k \geqslant 4$, from maximally nonassociative quasigroups of order 16 and 32. A quasigroup for each of the latter two orders is described in Section 5.

The above mentioned results imply the existence of maximally nonassociative quasigroups for all but finitely many of the orders claimed in Theorem 1.1. Details are given in Section 5, which also includes *ad hoc* constructions for the remaining orders. We believe that in the future a similar construction will be found for the missing orders 40, 42, 44, 56, 66, 77, 88, 90 and 110, although it is less clear what will happen for orders 11, 12 and 15 since they could well be genuine exceptions. We also suspect that maximally nonassociative quasigroups of orders $2p_1$ and $2p_1p_2$ will exist for all large enough primes p_1, p_2.

With the exception of product constructions, all maximally nonassociative quasigroups described in this paper were obtained by using an orthomorphism of an abelian group. An *orthomorphism* of a group G is a permutation ψ of G such that $x \mapsto \psi(x) - x$ is also a permutation of G. The orthomorphism ψ is *canonical* if $\psi(0) = 0$, where we use 0 to denote the identity element, since our groups are always abelian. Later we will use the observation that 0 is the only fixed point of a canonical orthomorphism. Orthomorphisms have been used in many different situations for creating interesting quasigroups and Latin squares. See [6, 12] for surveys. From any orthomorphism ψ of G we can define a quasigroup operation $*$ on G by

$$x * y = x + \psi(y - x) \tag{2}$$

for all $x, y \in G$. With the exception of Section 5, our G will be the additive group of a finite field $\mathbb{F} = \mathbb{F}_q$ of odd order q. In that case there are *quadratic orthomorphisms* available, namely orthomorphisms defined by

$$\psi(x) = \begin{cases} ax & \text{if } x \text{ is a square,} \\ bx & \text{if } x \text{ is a nonsquare,} \end{cases} \tag{3}$$

where a, b are fixed elements of $\mathbb{F}$. Note that $x \in \mathbb{F}$ is called a *square* if it can be expressed as $x = y^2$ for some $y \in \mathbb{F}$. The other elements are *nonsquares*.

If ψ is the orthomorphism defined by (3), then the quasigroup defined by (2) will be denoted by $Q_{a,b}$. These quasigroups will play a central role in this paper. Petr Lisoněk [10] has independently and concurrently obtained some of the results in our paper, also by using quadratic orthomorphisms. The following basic properties of quadratic orthomorphisms are known, see [6, 13].

Lemma 1.2. *For* (3) *to define a canonical orthomorphism of* $\mathbb{F}_q$ *it is necessary and sufficient that* ab *and* $(a-1)(b-1)$ *are both nonzero squares. Assuming that* (3) *does define an orthomorphism, the resulting quasigroup* $Q_{a,b}$ *has the following properties:*

(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 nonzero 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 nonsquare in $\mathbb{F}_q$.*

(v) *The opposite quasigroup of $Q_{a,b}$ is $Q_{1-a,1-b}$ if $q \equiv 1 \bmod 4$ and $Q_{1-b,1-a}$ if $q \equiv 3 \bmod 4$.*

Note that the *opposite* quasigroup $(Q, \cdot)$ of a quasigroup $(Q, *)$ is the quasigroup satisfying $a \cdot b = b * a$ for all $a, b \in Q$. In other words, the opposite quasigroup is obtained by transposing the operation table.

Lemma 1.3. *Let ψ be a canonical orthomorphism of an abelian group $(G, +)$. The idempotent quasigroup $(G, *)$ defined by (2) is maximally nonassociative if and only if there are no $x, y \in G \smallsetminus \{0\}$ such that*

$$\psi(\psi(x) + y) - \psi(y) = \psi(x + y - \psi(y)). \tag{4}$$

If $\psi \in \operatorname{Aut}(G)$, then $(x * y) * z = x * (y * z)$ if and only if $x = z$.

Proof. We have $x * (y * z) = x + \psi((y * z) - x) = x + \psi((y - x) + \psi(z - y))$ and $(x * y) * z = (x + \psi(y - x)) * z = x + \psi(y - x) + \psi((z - x) - \psi(y - x))$. Thus $(x * y) * z = x * (y * z)$ if and only if $\psi(\psi(v) + u) - \psi(u) = \psi(u + v - \psi(u))$, where $u = y - x$ and $v = z - y$. If $\psi \in \operatorname{Aut}(G)$, then this is true if and only if $\psi^2(v) = \psi(v) + \psi(u - \psi(u))$, which is equivalent to $\psi(v) - v = u - \psi(u)$ and hence also to $\psi(u + v) = u + v$. This last condition holds if and only if $u + v = 0$, i.e. $x = z$.

To finish the proof note that we have already shown that $(G, *)$ is maximally nonassociative if and only if (4) holds exactly when $x = y = 0$. However, if $x = 0$ and (4) holds, then $y = 0$ because $0 = \psi(y - \psi(y))$. Meanwhile $y = 0$ forces $x = 0$ since in such a case (4) reduces to $\psi^2(x) = \psi(x)$. It therefore suffices to test (4) for nonzero x, y. □

If G is of order n, then it might seem that $(n-1)^2$ tests are needed to verify (4). However, as we will formalise in Lemma 3.1, the number of tests can be reduced dramatically given the large number of automorphisms of $Q_{a,b}$ that we have at our disposal.

We say that a list of polynomials $g_1, \dots, g_k$ with coefficients in $\mathbb{F}$ *avoids squares* if there exists no sequence $1 \leqslant i_1 < \cdots < i_r \leqslant k$ such that $r \geqslant 1$ and $g_{i_1} \cdots g_{i_r}$ is a square (as a polynomial with coefficients in the algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$). Define $\chi\colon \mathbb{F} \to \{\pm 1, 0\}$ to be the quadratic character extended by $\chi(0) = 0$. The following consequence of the Weil bound will be used several times:

Theorem 1.4. *Let $g_1, \dots, g_k \in \mathbb{F}[t]$ be a list of polynomials that avoids squares. Suppose for $1 \leqslant i \leqslant k$ that g_i has degree $d_i \geqslant 1$ and that $\varepsilon_i \in \{-1, 1\}$. Denote by N the number of all $\alpha \in \mathbb{F}$ such that $\chi(g_i(\alpha)) = \varepsilon_i$, for all $1 \leqslant i \leqslant k$. Then $|N - 2^{-k} q| \leqslant (\sqrt{q} + 1)D/2 - \sqrt{q}(1 - 2^{-k})$ where $D = \sum_i d_i$.*

Proof. Consider

$$\sum_{\alpha \in \mathbb{F}} \prod_{1 \leqslant i \leqslant k} \bigl(1 + \varepsilon_i \chi(g_i(\alpha))\bigr) = 2^k N + R$$

where R is the contribution to the left hand side from all α that are roots of at least one of the $g_i(\alpha)$. We have $|R| \leqslant 2^{k-1} D$ because $D = \sum_i d_i$ is an upper bound on the number of α that contribute to R.

On the other hand, exploiting the multiplicative nature of χ we have

$$\begin{aligned}\sum_{\alpha \in \mathbb{F}} \prod_{1 \leqslant i \leqslant k} \bigl(1 + \varepsilon_i \chi(g_i(\alpha))\bigr) &= \sum_{\alpha \in \mathbb{F}} \Bigl(1 + \sum_U \Bigl(\prod_{i \in U} \varepsilon_i\Bigr) \chi\Bigl(\prod_{i \in U} g_i(\alpha)\Bigr)\Bigr) \\ &= q + \sum_U \Bigl(\prod_{i \in U} \varepsilon_i\Bigr) \sum_{\alpha \in \mathbb{F}} \chi\Bigl(\prod_{i \in U} g_i(\alpha)\Bigr),\end{aligned}$$

where U runs over all nonempty subsets $U \subseteq \{1, 2, \dots, k\}$. Therefore

$$\begin{aligned} |N - 2^{-k}q| &\leqslant 2^{-k}|R| + 2^{-k}\sum_U \Big|\sum_{\alpha\in\mathbb{F}} \chi\Big(\prod_{i\in U} g_i(\alpha)\Big)\Big| \\ &\leqslant D/2 + 2^{-k}\sqrt{q}\sum_U \Big(\sum_{i\in U} d_i - 1\Big) \\ &= D/2 + 2^{-k}\sqrt{q}\Big(2^{k-1}D - 2^k + 1\Big) \\ &= (\sqrt{q}+1)D/2 - \sqrt{q}(1-2^{-k}), \end{aligned}$$

the last inequality being the application of the Weil bound as formulated in [11, Theorem 6.2.2]. □

Corollary 1.5. *Under the hypotheses of the theorem, if* $2^{-k}q > (\sqrt{q}+1)D/2 - \sqrt{q}(1-2^{-k})$ *then* $N > 0$.

The structure of the paper is as follows. In Section 2 we define a particular product construction that allows us to build larger maximally nonassociative quasigroups from smaller ones. Sections 3 and 4 investigate the quasigroup $Q_{a,b}$. The first aim is to explain that $Q_{a,b}$ is maximally nonassociative unless a and b satisfy a number of conditions, each of which stipulates that several polynomials (two or three) in a and b yield a square (in some situations) or a nonsquare (in other situations). An argument based on Corollary 1.5 is then used in Section 4 to show that for all large enough primes p there exists at least one pair $(a, b) \in \mathbb{Z}_p^2$ for which none of the conditions is satisfied. The strategy used in Sections 3–4 thus mimics that of [1].

Orthomorphisms that yield maximally nonassociative quasigroups of orders 16, 20, 21, 24, 28, 32, 33, 35 and 55 are listed in Section 5. These provide the last piece of the proof of Theorem 1.1, which is given at the end of that section.

2. The product construction

This section uses a standard convention of quasigroup theory, by which a juxtaposition is of higher precedence than an explicitly stated operation. Thus $xy \cdot z = (x \cdot y) \cdot z$. A triple (x, y, z) is *associative* if and only if $xy \cdot z = x \cdot yz$.

Let us begin by mentioning two easy and well known facts of a general nature.

Lemma 2.1. *Let Q be a quasigroup satisfying* (1)*. Then Q is idempotent.*

Proof. Let $y \in Q$ and define $x, z \in Q$ by $xy = y = yz$. Then $x \cdot yz = xy = y = yz = xy \cdot z$. Hence, $x = y$ by (1), and so $yy = y$. As y was arbitrary, Q must be idempotent. □

Lemma 2.2. *Let Q be an idempotent quasigroup, and let $(x, y, z) \in Q^3$ be an associative triple. If $x = y$ or $y = z$ or $xy = z$ or $x = yz$, then $x = y = z$.*

Proof. If $x = y$, then $xz = xy \cdot z = x \cdot yz = x \cdot xz$. By cancellation, $xz = z = zz$ and $x = z$. If $x = yz$, then $yz = x = xx = x \cdot yz = xy \cdot z$. By cancellation, $xy = y = yy$ and $x = y$. The rest follows by mirror arguments. □

Although we are exclusively interested in finite quasigroups in this paper, we note in passing that both of the previous results apply when Q is infinite.

Theorem 2.3. *Let $(Q, \cdot)$ be a maximally nonassociative finite quasigroup and let $(U, *)$ be an idempotent quasigroup. Suppose that $|Q| \geqslant |U|$ so that there exists an injective* *mapping $j\colon U \to Q$. Choose an abelian group operation on Q, and denote it by $+$. Then*

$$(x,\, u)(y,\, v) = \begin{cases} (x \cdot y,\, u) & \text{if } u = v, \text{ and} \\ (x + y + j(u),\, u * v) & \text{if } u \neq v \end{cases} \tag{5}$$

defines a maximally nonassociative quasigroup operation on $Q \times U$.

Proof. First note that $\pi\colon (x,u) \mapsto u$ is a homomorphism onto $(U,*)$. By applying π we see that to show that $(x_1,u_1)(y,v) = (x_2,u_2)(y,v)$ implies both $x_1 = x_2$ and $u_1 = u_2$, only the case $u_1 = u_2 = u$ has to be treated. If $u = v$, then $x_1 = x_2$ since $(Q,\cdot)$ is a quasigroup. Assume $u \neq v$. Then $x_1 + y + j(u) = x_2 + y + j(u)$ and $x_1 = x_2$. We have thus verified cancellation on the left, and cancellation on the right can be verified in a similar manner. This means that (5) defines a quasigroup. Note that this fact does not depend upon the injectivity of j.

Now consider an associative triple $((x,u),(y,v),(z,w))$. If $u = v = w$, then $x = y = z$, by the assumption on $(Q,\cdot)$. The triple (u,v,w) is also associative since π is a quasigroup homomorphism. Hence it may be assumed that $u \neq v$, $u * v \neq w$, $v \neq w$ and $u \neq v * w$, by Lemma 2.2. This means that

$$(x,u) \cdot (y,v)(z,w) = \big(x + y + z + j(u) + j(v),\, u * (v * w)\big),$$

while

$$(x,u)(y,v) \cdot (z,w) = \big(x + y + z + j(u) + j(u * v),\, (u * v) * w\big).$$

The associativity of the triple $((x,u),(y,v),(z,w))$ thus yields $j(v) = j(u*v)$, which is the same as $u = v$ since j is injective and $v = v * v$. Hence no nondiagonal associative triples exist. □

Corollary 2.4. *If $n \geqslant m \geqslant 3$ are integers, and there exists a maximally nonassociative quasigroup of order n, then there exists a maximally nonassociative quasigroup of order nm.*

Proof. This follows directly from Theorem 2.3 since for each order $m \geqslant 3$ it is well known that there exists an idempotent quasigroup of that order. □

3. Quadratic orthomorphisms

Let $\mathbb{F}$ be a finite field of odd order q. Denote by Σ the set of all $(a,b) \in \mathbb{F} \times \mathbb{F}$ such that $0 \notin \{a, b, a-1, b-1\}$, $a \neq b$, and both ab and $(a-1)(b-1)$ are squares. By Lemma 1.2 each pair $(a,b) \in \Sigma$ *induces* a quasigroup $Q_{a,b}$. The condition $a \neq b$ has been included in the definition of Σ, since $Q_{a,a}$ is not maximally nonassociative. Indeed, in this case each triple $(x,y,x) \in \mathbb{F}^3$ is associative, by Lemma 1.3.

Replacing y with $-y$ in (4) yields

$$\psi(\psi(x) - y) = \psi(-y) + \psi(x - y - \psi(-y)). \tag{6}$$

In this section (6) is given preference over (4) since it makes the connection to the opposite quasigroup easier to handle. Equation (6) will henceforth be called the *Associativity Equation*. By Lemma 1.3, the quasigroup $Q_{a,b}$ is maximally nonassociative if and only if the Associativity Equation has no solution $(x,y) \neq (0,0)$, where ψ is defined by (3). Our next result will reduce the number of tests required to check if there is a solution. It will show that it suffices to test just two values of x provided one of those values is a square and the other is not.

Lemma 3.1. *For $(a,b) \in \Sigma$ define ψ by* (3) *and $*$ by* (2)*. Then*

$$x - y - \psi(-y) = x - (y * 0) \quad \text{and} \quad \psi(x) - y = (0 * x) - y. \tag{7}$$

An ordered pair $(x,y) \in \mathbb{F}^2$ fulfils (6) *if and only if $y*(0*x) = (y*0)*x$. Furthermore, if $(x,y) \neq (0,0)$ fulfils* (6)*, then none of x, y, $x - y - \psi(-y)$ and $\psi(x) - y$ vanishes, and (cx, cy) fulfils* (6) *too, for any square $c \in \mathbb{F}$.*

Proof. By definition, $0 * x = \psi(x)$ and $y * 0 = y + \psi(-y)$, which yields (7). We have

$$(y * 0) * x = y + \psi(-y) + \psi(x - y - \psi(-y)) \text{ and } y * (0 * x) = y + \psi(\psi(x) - y).$$

Hence (x,y) fulfils (6) if and only if $(y, 0, x)$ is an associative triple in $Q_{a,b}$. Assume $(x,y) \neq (0,0)$ and suppose that $(y,0,x)$ is an associative triple. Then $0 \notin \{x,y\}$, $y + \psi(-y) \neq x$ and $y \neq \psi(x)$, by Lemma 2.2. To conclude, note that $(y,0,x)$ is an associative triple if and only if $(cy, 0, cx)$ is an associative triple, for any square $c \in \mathbb{F}$, by Lemma 1.2 (iii). □

Define $\eta : \mathbb{F} \to \{0,1\}$ by $\eta(x) = 0$ if x is a square, and $\eta(x) = 1$ if x is a nonsquare. As illustrated by (8), the Associativity Equation (6) takes different shapes depending upon the values of $\eta(x)$ and $\eta(-y)$:

(8)

$\eta(x)$	$\eta(-y)$	$\psi(x)$	$\psi(-y)$	The Associativity Equation
0	0	ax	$-ay$	$\psi(ax - y) = \psi(x - y + ay) - ay$
0	1	ax	$-by$	$\psi(ax - y) = \psi(x - y + by) - by$
1	0	bx	$-ay$	$\psi(bx - y) = \psi(x - y + ay) - ay$
1	1	bx	$-by$	$\psi(bx - y) = \psi(x - y + by) - by$

The shape of the Associativity Equation depends not only upon $\eta(x)$ and $\eta(-y)$, but also upon $\eta(\psi(x) - y)$ and $\eta(x - y - \psi(-y))$:

(9)

$\eta(\psi(x) - y)$	$\eta(x - y - \psi(-y))$	The Associativity Equation
0	0	$a(\psi(x) - y) = \psi(-y) + a(x - y - \psi(-y))$
0	1	$a(\psi(x) - y) = \psi(-y) + b(x - y - \psi(-y))$
1	0	$b(\psi(x) - y) = \psi(-y) + a(x - y - \psi(-y))$
1	1	$b(\psi(x) - y) = \psi(-y) + b(x - y - \psi(-y))$

For $(a,b) \in \Sigma$ and $i,j,r,s \in \{0,1\}$ denote by $E_{ij}^{rs}(a,b)$ the set of all nontrivial solutions (x,y) to the Associativity Equation (6) that fulfil

$$i = \eta(x),\ j = \eta(-y),\ r = \eta(\psi(x) - y) \text{ and } s = \eta(x - y - \psi(-y)). \tag{10}$$

Put $\rho = (a-1)/(b-1)$ and consider the case $(i,j,r,s) = (0,1,1,1)$ as an example. Note that ρ is a square, by the definition of Σ. By (9), the Associativity Equation takes the form $b(\psi(x) - y) = \psi(-y) + b(x - y - \psi(-y))$. By (8), $\psi(x)$ is to be replaced by ax and $\psi(-y)$ by $-by$. The Associativity Equation thus yields

$$\begin{aligned} bax - by &= -by + bx - by + b^2y, \\ x(a-1) &= y(b-1), \text{ and} \\ y &= \rho x. \end{aligned} \tag{11}$$

Any solution to (11) thus fulfils $\eta(x) = \eta(y)$. This means that if -1 is a square, then we cannot have $\eta(x) = 0$ and $\eta(-y) = 1$. Therefore if -1 is a square, then $E_{01}^{11} = \varnothing$. Let -1 be a nonsquare, and x a square. Then $(x, \rho x) \in E_{01}^{11}$ if $ax - \rho x$ is a nonsquare, i.e. if $\rho - a$ is a square, and if $x - \rho x + b\rho x$ is a nonsquare, i.e. if $\rho - 1 - b\rho = (1-b)\rho - 1 = -a$ is a square.

Since $(1,\rho)$ is a solution of (11), then every solution to (11) is equal to $(x,\rho x)$ for some $x\in\mathbb{F}$. However, if x is a nonsquare, then this solution does not fulfil (10). Hence

$$E^{11}_{01}(a,b)=\begin{cases}\{(c^2,c^2\rho);\ c\in\mathbb{F}^*\} & \text{if } -1 \text{ and } a \text{ are nonsquares and } \rho-a \text{ is a square,}\\ \varnothing & \text{otherwise.}\end{cases}$$

The equations (11) have been obtained by combining the row $(r,s)=(1,0)$ of (9) with the row $(i,j)=(0,1)$ of (8). There are 16 combinations altogether. However, the workload in studying these different combinations can be reduced by the following observations.

Lemma 3.2. *Let $(a,b)\in\Sigma$ and suppose that ζ is a nonsquare. Then*

$$(x,y)\in E^{rs}_{ij}(a,b) \iff (\zeta x,\zeta y)\in E^{1-r,1-s}_{1-i,1-j}(b,a),$$

for all $i,j,r,s\in\{0,1\}$.

Proof. Let ψ and $\bar\psi$ denote the orthomorphisms for $(Q_{a,b},*)$ and $(Q_{b,a},\bar{*})$, respectively. By Lemma 3.1, (x,y) fulfils the Associativity Equation (6) if and only if $(y,0,x)$ is an associative triple in $Q_{a,b}$. By Lemma 1.2(iv) we know that $x\mapsto\zeta x$ is an isomorphism from $Q_{a,b}$ to $Q_{b,a}$. Hence,

$$y*(0*x)=(y*0)*x \iff (\zeta y)\,\bar{*}\,(0\,\bar{*}\,(\zeta x))=((\zeta y)\,\bar{*}\,0)\,\bar{*}\,(\zeta x),$$

for all $x,y\in\mathbb{F}$. Therefore (x,y) fulfils Lemma 3.1 with respect to $*$ if and only if $(\zeta x,\zeta y)$ fulfils Lemma 3.1 with respect to $\bar{*}$.

Let $x,y\in\mathbb{F}$ and $i,j,r,s\in\{0,1\}$ be such that $(x,y)\in E^{rs}_{ij}(a,b)$. Note that $\psi(x)-y\neq 0$ and $x-y-\psi(-y)\neq 0$, by Lemma 3.1. Also, $\zeta(\psi(x)-y)=\zeta(0*x)-\zeta y=(0\,\bar{*}\,\zeta x)-\zeta y=\bar\psi(\zeta x)-\zeta y$ and $\zeta(x-y-\psi(-y))=\zeta x-\zeta(y*0)=\zeta x-((\zeta y)\,\bar{*}\,0)=\zeta x-\zeta y-\bar\psi(-\zeta y)$. It follows that

$$\frac{\zeta x}{x}=\frac{\zeta y}{y}=\frac{\bar\psi(\zeta x)-\zeta y}{\psi(x)-y}=\frac{\zeta x-\zeta y-\bar\psi(-\zeta y)}{x-y-\psi(-y)}=\zeta.$$

This verifies that $(\zeta x,\zeta y)\in E^{1-r,1-s}_{1-i,1-j}(b,a)$ given our earlier observations. □

Lemma 3.3. *If $(a,b)\in\Sigma$ and $i,j,r,s\in\{0,1\}$, then*

$$(x,y)\in E^{rs}_{ij}(a,b) \iff (y,x)\in E^{sr}_{ji}(1-a,1-b) \text{ if } -1 \text{ is a square,}$$

and

$$(x,y)\in E^{rs}_{ij}(a,b) \iff (y,x)\in E^{1-s,1-r}_{1-j,1-i}(1-b,1-a) \text{ if } -1 \text{ is a nonsquare.}$$

Proof. Let $*$ and $\tilde{*}$ denote the operations of $Q_{a,b}$ and the opposite of $Q_{a,b}$, respectively (see Lemma 1.2(v)). Define ψ by (3) and put $\tilde\psi(x)=x+\psi(-x)$ for each $x\in\mathbb{F}$. Then $\tilde\psi$ is an orthomorphism of $(\mathbb{F},+)$, and the operation $\tilde{*}$ is defined by $x\,\tilde{*}\,y=x+\tilde\psi(y-x)$ for all $x,y\in\mathbb{F}$. This is because

$$x\,\tilde{*}\,y=y*x=y+\psi(x-y)=x+(y-x)+\psi(-(y-x))=x+\tilde\psi(y-x),$$

for $x,y\in\mathbb{F}$.

Since $y*(0*x)=(y*0)*x$ is equivalent to $x\,\tilde{*}\,(0\,\tilde{*}\,y)=(x\,\tilde{*}\,0)\,\tilde{*}\,y$, a pair $(x,y)\in\mathbb{F}\times\mathbb{F}$ fulfils the Associativity Equation (6) with respect to ψ if and only if the equation is fulfilled by (y,x) with respect to $\tilde\psi$.

Let $i,j,r,s\in\{0,1\}$ and $x,y\in\mathbb{F}$ be such that $i=\eta(x)$, $j=\eta(-y)$, $r=\eta(\psi(x)-y)$ and $s=\eta(x-y-\psi(-y))$. Define $(\tilde\imath,\tilde\jmath,\tilde r,\tilde s)$ to be (j,i,s,r) if -1 is a square, and to be $(1-j,1-i,1-s,1-r)$ if -1 is a nonsquare. What remains is to verify that $\tilde\imath=\eta(y)$,

$\tilde{\jmath} = \eta(-x)$, $\tilde{r} = \eta(\tilde{\psi}(y) - x)$ and $\tilde{s} = \eta(y - x - \tilde{\psi}(-x))$. Now, $\tilde{\imath} = \eta(y)$ and $\tilde{\jmath} = \eta(-x)$ follow immediately from the definition of $\tilde{\imath}$ and $\tilde{\jmath}$. As for $\tilde{r}$ and $\tilde{s}$, observe that

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

and

$$y - x - \tilde{\psi}(-x) = y - x - (-x + \psi(x)) = -(\psi(x) - y). \qquad \square$$

We need one further technical lemma before stating the main result of this section.

Lemma 3.4. *Suppose that $(a, b) \in \Sigma$. Then at least one of the following holds:*

(i) $b \neq a^2$,
(ii) $a, b, 1 - a$ *and* $1 - b$ *are all squares, or*
(iii) *there exists* $y \in \mathbb{F}$ *such that* $\eta(-y) = 1$, $\eta(a - y) = 0$ *and* $\eta(1 - y + by) = 1$.

Proof. As $(a, b) \in \Sigma$ we know that $\eta(a) = \eta(b)$ and $\eta(1-a) = \eta(1-b)$. If condition (i) fails then b is a square, so $\eta(a) = \eta(b) = 0$. If condition (ii) also fails then $\eta(1 - a) = \eta(1-b) = 1$ and hence $a \neq 1/(1-b)$. It then follows that the list of linear polynomials $-y, a - y, 1 - (1 - b)y$ avoids squares since no pair of them have a root in common. Thus we may apply Corollary 1.5 with $k = D = 3$ to find that condition (iii) holds provided $q/8 > (\sqrt{q} + 1)3/2 - \sqrt{q}(7/8)$. This proves the lemma for all $q \geqslant 46$. For smaller fields the lemma can be checked by direct computation. □

With the preliminary results in place, we can now characterise the quadratic orthomorphisms that produce maximally nonassociative quasigroups.

Theorem 3.5. *For $(a, b) \in \Sigma$, define $\mu = b^2 - 2b + a$, $\nu = a^2 - 2a + b$, $\sigma = a^2b - a^2 - ab + b$, and $\tau = a^2b - ab - a + b$. The necessary and sufficient conditions for $Q_{a,b}$ to be maximally nonassociative are*

(1) $a^2 \neq b$ *or* $a \neq 2b - b^2$,
(2) *at least one of* -1, $a - 1$ *or* a *is nonsquare,*
(3) *at least one of* b, $(1 - a)(a^2 - b)$ *or* $\sigma(a - 1)$ *is square,*
(4) *at least one of* $a\nu$, $1 - b$ *or* $a\tau$ *is square,*
(5) -1 *is nonsquare or* $\sigma a(b - 1)$ *is square or* $\tau a(b - 1)$ *is square,*
(6) -1 *is square or* $b - 1$ *is nonsquare or* $(ab - a + b)b$ *is nonsquare,*
(7) $(b - a^2)\mu$ *is square or* $b\mu(ab - 2a + 1)$ *is nonsquare or* $(a - 1)(ab - a + b)\mu$ *is square,*
(8) -1 *is square or* $a - 1$ *is square or* b *is nonsquare,*
(9) *at least one of* -1, a *or* $(ab - 2a + 1)(b - 1)$ *is square, and*
(10) *conditions* (1)–(9) *all apply when a and b are interchanged* (*which also interchanges μ with ν, and changes σ and τ accordingly*).

Proof. We consider the 8 possibilities for the quadruple $ijrs$ with $i = 0$. The 8 possibilities with $i = 1$ can then be obtained by employing Lemma 3.2, and will lead to the same restrictions but with a and b interchanged. Note that the case $ijrs = 0111$ was already worked through in some detail before Lemma 3.2.

For specific values of $ijrs$ we can use (8) and (9) to convert the Associativity Equation (6) into a linear equation in x and y. As we are assuming that $0 = i = \eta(x)$ we may then without loss of generality substitute $x = 1$, by Lemma 3.1. In this way, for each of the 8 cases, the Associativity Equation (6) reduces to the form given in Table 1. Common factors of a, b, $1 - a$ or $1 - b$ have been cancelled from both sides of the Associativity Equation if they were present. These quantities are assumed to be nonzero since $(a, b) \in \Sigma$.

If the coefficient of y in the Associativity Equation is nonzero, then there is a unique solution, denoted by $y = y_{ij}^{rs}$ as listed in the rightmost column of Table 1.

$ijrs$	The Associativity Equation	Solution y_{ij}^{rs}
0000	$1 = y$	1
0001	$a^2 - b = b(a-1)y$	$(a^2 - b)/b(a-1)$
0010	$a(b-1) = (a^2 - 2a + b)y$	$a(b-1)/\nu$
0011	$b(a-1) = a(b-1)y$	$(a-1)b/(b-1)a$
0100	$a = by$	a/b
0101	$a^2 - b = (b^2 - 2b + a)y$	$(a^2 - b)/\mu$
0110	$1 = y$	1
0111	$a - 1 = (b-1)y$	$(a-1)/(b-1)$

Table 1.

There are two of the 8 cases where the coefficient of y may be zero depending on the values of a and b. When $ijrs = 0010$ we have $\nu y = a(b-1) \neq 0$, so there will be no solution if $\nu = 0$ and a unique solution otherwise.

The case $ijrs = 0101$ needs more care because it is possible that both sides of the Associativity Equation are zero if $\mu = 0$ and $b = a^2$. If that happens then any y will be a solution and $Q_{a,b}$ will not be maximally nonassociative (note that by Lemma 3.4 we can assume that a suitable y exists or that one of conditions (2) or (8) of the theorem fails). If precisely one of the conditions $\mu = 0$ and $b = a^2$ holds, then there is no solution to the Associativity Equation (we are assuming $y \neq 0$ by Lemma 1.3). If $\mu \neq 0$ and $b \neq a^2$, there is a unique solution $y_{01}^{01} = (a^2 - b)/\mu$ as presented in Table 1.

The interpretation of Table 1 is that in each case there will be no nondiagonal associative triples unless substituting $x = 1$ and $y = y_{ij}^{rs}$ into (10) produces the correct values for i, j, r, s for the case in question. The condition $i = \eta(x)$ is automatically satisfied but the other three conditions produce restrictions. These restrictions can be simplified using $\eta(ab) = \eta((1-a)(1-b)) = \eta(c^2) = 0$ for all $c \in \mathbb{F}$, producing Table 2.

$ijrs$	$j = \eta(-y)$	$r = \eta(a-y)$	$s = \eta(x - y - \psi(-y))$
0000	$\eta(-1) = 0$	$\eta(a-1) = 0$	$\eta(a) = 0$
0001	$\eta((a^2 - b)b(1-a)) = 0$	$\eta(\sigma b(a-1)) = 0$	$\eta(b) = 1$
0010	$\eta(a\nu(1-b)) = 0$	$\eta(a\nu) = 1$	$\eta(\tau\nu) = 0$
0011	$\eta(-1) = 0$	$\eta(\sigma a(b-1)) = 1$	$\eta(\tau a(b-1)) = 1$
0100	$\eta(-1) = 1$	$\eta(b-1) = 0$	$\eta((ab - a + b)b) = 0$
0101	$\eta((b - a^2)\mu) = 1$	$\eta(b(ab - 2a + 1)\mu) = 0$	$\eta((a-1)(ab - a + b)\mu) = 1$
0110	$\eta(-1) = 1$	$\eta(a-1) = 1$	$\eta(b) = 0$
0111	$\eta(-1) = 1$	$\eta((ab - 2a + 1)(b-1)) = 1$	$\eta(a) = 1$

Table 2.

If for any row of Table 2 all three conditions are met, then $(y_{ij}^{rs}, 0, 1)$ will be an associative triple, by Lemma 3.1. So we are interested in the case when at least one condition fails in each row of Table 2. For most rows this translates directly to a condition in the theorem. For the case $ijrs = 0001$ we consider the $\eta(b) = 0$ and $\eta(b) = 1$ cases separately to get the condition that at least one of b, $(1-a)(a^2-b)$ or $\sigma(a-1)$ is square. Similarly, for the case $ijrs = 0010$ we consider the $\eta(a\nu) = 0$ and $\eta(a\nu) = 1$ cases separately to get the condition that at least one of $a\nu$, $1-b$ or $a\tau$ is square. Note that this covers the case when $\nu = 0$ and there was no solution to the Associativity Equation, so that condition does not need separate treatment. Similarly, in the subcase of $ijrs = 0101$ where there is no solution to the Associativity Equation, we have $\mu = 0$ and this is subsumed by the conditions for the general case. □

In practice, when applying Theorem 3.5 the value of $\eta(-1)$ will be determined by the value of $q \bmod 4$ and a number of the conditions will be trivially satisfied. Also, it is legitimate to replace any occurrence of "square" in Theorem 3.5 by "nonzero square". This is because the arguments of η in (10) are known to be nonzero, by Lemma 3.1.

It follows from Lemma 1.2(iv) that $Q_{a,b}$ is maximally nonassociative if and only if $Q_{b,a}$ is maximally nonassociative. This is reflected in condition (10) of Theorem 3.5. It is also easy to see that the opposite quasigroup for a maximally nonassociative quasigroup is itself a maximally nonassociative quasigroup (see also Lemma 3.3). It follows then from Lemma 1.2 parts (iv) and (v) that $Q_{a,b}$ is maximally nonassociative if and only if $Q_{1-a,1-b}$ is maximally nonassociative. Hence substituting $a \mapsto 1-a$ and $b \mapsto 1-b$ into the conditions of Theorem 3.5 should produce an equivalent set of conditions. This can be verified with some effort.

Similarly, it can be checked that making the substitution $b = a$ into the conditions (2)–(9) of Theorem 3.5 yields eight conditions which between them exclude all the possibilities for the triple $(\eta(-1), \eta(a), \eta(a-1))$. In this way, we demonstrate that $Q_{a,a}$ is never maximally nonassociative. This was already remarked when we defined Σ at the start of this section, but it does provide another consistency check for Theorem 3.5.

4. Weil bound applications

Throughout this section, $\mathbb{F}$ will be a finite field of odd order q. Our main goal is to use Corollary 1.5 to show that the conditions of Theorem 3.5 are satisfied by some pair (a,b), provided q is large enough (although for technical reasons, we will exclude fields of certain small characteristics). We treat the $q \equiv 1 \bmod 4$ and $q \equiv 3 \bmod 4$ cases separately. For both cases we find it useful to assume a particular (but different) relationship between a and b. Each case will begin with some preliminary lemmas that establish conditions under which that relationship creates the desired outcome. We begin with the case $q \equiv 1 \bmod 4$.

Lemma 4.1. *Suppose that $q \equiv 1 \bmod 4$. Let $a \in \mathbb{F}$ be such that $a^3 - a^2 + 2a - 1$ is square, while a, $a-1$, a^2+a-1, and a^2-3a+1 are nonsquares. Then $Q_{a,1-a}$ is maximally nonassociative.*

Proof. Let $b = 1-a$ and note that $\eta(-1) = 0$ since $q \equiv 1 \bmod 4$. Also $\eta(ab) = \eta((1-a)(1-b)) = 0$. Note that $\eta(a) = \eta(1-a) = 1$ implies that $a \neq \{0,1\}$. It follows that ab and $(a-1)(b-1)$ are nonzero squares.

By assumption, $a, b, a-1, b-1$, $\nu = a^2-2a+b = a^2-3a+1 = b^2-a$ and $\mu = b^2-2b+a = a^2+a-1 = a^2-b$, are nonsquares while -1 and $\sigma = a^2b-a^2-ab+b = -a^3+a^2-2a+1$ are squares. It follows that $a^2 \neq b$, $b^2 \neq a$ and that all of the conditions of Theorem 3.5 are met. □

Lemma 4.2. *The list of polynomials x, $x-1$, x^2+x-1, x^2-3x+1 and x^3-x^2+2x-1 avoids squares over any field $\mathbb{F}$ with* $\mathrm{char}(\mathbb{F}) \notin \{2,5\}$.

Proof. It is trivial to check that none of the nonlinear polynomials can share a root with either of the linear polynomials. So we can ignore the linear polynomials when it comes to looking for a subset of the polynomials that might multiply to give a perfect square. That leaves only one polynomial of odd degree, which can therefore also be ruled out. It is routine to check that the two quadratics between them have four distinct roots in $\overline{\mathbb{F}}$ provided $\mathrm{char}(\mathbb{F}) \notin \{2,5\}$. □

Armed with these preliminary lemmas we can now show the existence of maximally nonassociative quasigroups in large fields of order $q \equiv 1 \bmod 4$ (except for fields of characteristic 5).

Theorem 4.3. *Let $\mathbb{F}$ be a field of prime power order $q \equiv 1 \bmod 4$ such that $\mathrm{char}(\mathbb{F}) \neq 5$. If $q \neq 17$, then there exists $a \in \mathbb{F}$ such that $Q_{a,1-a}$ is a maximally nonassociative quasigroup.*

Proof. It is enough to find $a \in \mathbb{F}$ that fulfils the conditions of Lemma 4.1. By Lemma 4.2 the number of such elements can be estimated by Theorem 1.4. In terms of Corollary 1.5 we have $k = 5$ and $d_1 = d_2 = 1$, $d_3 = d_4 = 2$ and $d_5 = 3$, so that $D = 9$. Hence it suffices if $q/32 > (\sqrt{q}+1)9/2 - \sqrt{q}(31/32)$, which is true if $q \geqslant 13056$. For all smaller q we use direct computation (the results of which are given at [14]). For prime powers $q \equiv 1 \bmod 4$ in the range $9 \leqslant q < 13056$ that are not powers of 5 there is $a \in \mathbb{F}_q$ satisfying Lemma 4.1 except for $q \in \{17, 37, 49\}$. For $q = 37$, $Q_{18,20}$ is maximally nonassociative and for $q = 49$, $Q_{3t,1-3t}$ is maximally nonassociative over $\mathbb{Z}_7[t]/(t^2 + t + 3)$ (note that the conditions in Lemma 4.1 are sufficient but not necessary). □

In $\mathbb{F}_{17}$ there are no maximally nonassociative quasigroups of the form $Q_{a,1-a}$; however $Q_{4,8}$ is maximally nonassociative. Although characteristic 5 fields are excluded from Theorem 4.3, there are quadratic orthomorphisms of $\mathbb{F}_{25}$ that produce maximally nonassociative quasigroups. For example, we can take Q_{t,t^3} in $\mathbb{Z}_5[t]/(t^2+t+2)$. Note also that [1] gives a construction for order p^2 for all odd primes p.

It is worth noting that the quasigroup $Q_{a,1-a}$ involved in Theorem 4.3 is isomorphic to its opposite quasigroup, by Lemma 1.2. This makes Theorem 3.5 easier to satisfy since many of the conditions coincide. The same approach does not work for $q \equiv 3 \bmod 4$ since in that case $Q_{a,1-a}$ is actually equal to its opposite by Lemma 1.2, which is the same as saying that $Q_{a,1-a}$ is commutative. It is not possible for a commutative quasigroup of order $n > 1$ to be maximally nonassociative since $x*(y*x) = (y*x)*x = (x*y)*x$ for all x, y in a commutative quasigroup, which means that there will always be at least n^2 associative triples. Hence we need a different approach for $q \equiv 3 \bmod 4$.

Lemma 4.4. *Suppose that $\mathbb{F}$ is a field of order $q \equiv 3 \bmod 4$ and $\mathrm{char}(F) > 19$. Let $a \in \mathbb{F}_q$ be such that a, $a-1$, $a+2$, $4a-1$ and $16a-7$ are squares, while $a-4$, $4a-3$, $4a+3$ and $16a-1$ are nonsquares. Then $Q_{a,4a}$ is maximally nonassociative.*

Proof. Let $b = 4a$ and note that $\eta(-1) = 1$ since $q \equiv 3 \bmod 4$. Also $\eta(ab) = \eta(4a^2) = 0$ and $\eta((a-1)(b-1)) = \eta(a-1)+\eta(4a-1) = 0$. Since we are insisting that $\eta(4a-1) = 0$ and $\eta(4a-3) = \eta(4a+3) = 1$, we know that $a \neq \{0, 1, 1/4\}$. It follows that ab and $(a-1)(b-1)$ are nonzero squares.

Next we consider condition (1) in Theorem 3.5. If $4a = b = a^2$ then $a = 4$ (since $a \neq 0$). If in addition $0 = 2b - b^2 - a = -228$ then $\mathbb{F}$ must have characteristic at most 19, which we are assuming is not the case. Similarly, we cannot have $4a = b = 2a - a^2$ unless $a = -2$ which together with $a = b^2$ would force $0 = 66$. Hence the restriction $\mathrm{char}(\mathbb{F}) > 19$ ensures that we can ignore the condition (2) in Theorem 3.5 (and its image under interchange of a and b).

By assumption, $a, b, a-1, b-1$, $\mu = b^2 - 2b + a = 16a^2 - 7a = a(16a - 7)$, $b - a^2 = a(4-a)$, $\nu = a^2 - 2a + b = a(a+2)$ and $a - b^2 = a(1-16a)$ are all squares, while -1, $ab-a+b=a(4a+3)$ and $ab-b+a=a(4a-3)$ are nonsquares. It follows that all of the conditions of Theorem 3.5 are met. □

Lemma 4.5. *If* $\mathrm{char}(\mathbb{F}) > 19$*, then the list of polynomials* x*,* $x-1$*,* $x+2$*,* $4x-1$*,* $16x-7$*,* $x-4$*,* $4x-3$*,* $4x+3$ *and* $16x-1$ *avoids squares.*

Proof. The roots $0, 1, -2, 1/4, 7/16, 4, 3/4, -3/4$ and $1/16$ of these linear polynomials are all distinct when $\mathrm{char}(\mathbb{F}) > 19$. It follows that the list of polynomials avoids squares. □

Again these preliminary lemmas will now allow us to show the existence of maximally nonassociative quasigroups in fields of large order $q \equiv 3 \bmod 4$ and large characteristic.

Theorem 4.6. *Let* $\mathbb{F}$ *be a field of prime power order* $q \equiv 3 \bmod 4$ *such that* $\mathrm{char}(\mathbb{F}) > 19$*. If* $q \neq 79$*, then there exists* $a \in \mathbb{F}$ *such that* $Q_{a,4a}$ *is a maximally nonassociative quasigroup.*

Proof. It is enough to find $a \in \mathbb{F}$ that fulfils the conditions of Lemma 4.4. By Lemma 4.5 the number of such elements can be estimated by Theorem 1.4. In terms of Corollary 1.5 we have $k = 9$ and $d_1 = \cdots = d_9 = 1$. Hence it suffices if $q/512 > (\sqrt{q}+1)9/2 - \sqrt{q}(511/512)$, which is true if $q \geqslant 3219456$. For smaller orders, again we do a direct computation [14]. For $1663 < q < 3219456$ we found $a \in \mathbb{F}$ satisfying Lemma 4.4. For $19 < q \leqslant 1663$ we found $a \in \mathbb{F}$ for which $Q_{a,4a}$ is a maximally nonassociative quasigroup, unless $q = 79$. □

Although $\mathbb{F}_{79}$ allows no maximally nonassociative quasigroup of the form $Q_{a,4a}$, it does allow the maximally nonassociative quasigroup $Q_{10,26}$. Also $Q_{5,6}$ is a maximally nonassociative quasigroup when $q = 19$.

5. Additional orthomorphisms

In this final section we will wrap up the proof of Theorem 1.1. To do that we will need to construct maximally nonassociative quasigroups of certain small orders. First we give an orthomorphism ψ of the cyclic group $\mathbb{Z}_n$ which produces a maximally nonassociative quasigroup, via (2), for orders $n \in \{21, 33, 35, 55\}$. We present each orthomorphism as a permutation in cycle notation. In all but the first case this permutation is an involution. There are no involutions in $\mathbb{Z}_{21}$ which work.

$$\begin{aligned}
\mathbb{Z}_{21} :\ & (1,2)(3,8,17,13,19,9,6,4,12,16,10,20,15,18,11)(5,7,14)\\
\mathbb{Z}_{33} :\ & (1,2)(3,5)(4,15)(6,23)(7,14)(8,29)(9,27)(10,19)(11,21)(12,32)(13,16)\\
& (17,31)(18,26)(20,24)(22,28)(25,30)\\
\mathbb{Z}_{35} :\ & (1,2)(3,5)(4,8)(6,16)(7,19)(9,33)(10,15)(11,24)(12,30)(13,28)(14,23)\\
& (17,31)(18,34)(20,27)(21,29)(22,25)(26,32)\\
\mathbb{Z}_{55} :\ & (1,9)(2,44)(3,35)(4,15)(5,25)(6,33)(7,41)(8,22)(10,20)(11,37)(12,27)\\
& (13,32)(14,31)(16,38)(17,18)(19,28)(21,23)(24,36)(26,50)(29,54)(30,46)\\
& (34,52)(39,43)(40,45)(42,49)(47,53)(48,51)
\end{aligned}$$

For even orders, there are no orthomorphisms of the cyclic group, so we need to use noncyclic groups. In the following permutations we omit commas within cycles and also adopt a shorthand notation for group elements. We write (a, b) as a_b and

(a,b,c,d) as a_{bcd}. In this way we present orthomorphisms which produce a maximally nonassociative quasigroup, via (2), for orders $n \in \{16,20,24,28,32\}$:

$$\begin{aligned}
\mathbb{Z}_8 \times \mathbb{Z}_2 &: (0_1 1_0 4_1 7_1 5_0 2_1)(1_1 6_1 5_1 7_0 3_1 3_0 4_0 6_0 2_0)\\
\mathbb{Z}_{10} \times \mathbb{Z}_2 &: (0_1 4_0)(1_0 1_1 6_1)(2_0 4_1 2_1 9_1 6_0 5_1 3_0 5_0 8_1 9_0)(3_1 7_1)(7_0 8_0)\\
\mathbb{Z}_{12} \times \mathbb{Z}_2 &: (0_1 3_1 7_0 7_1 6_1 2_0 3_0 1_1 6_0 8_0 5_0 9_0 10_1 1_0)(2_1 4_0 10_0 5_1 11_0 8_1 4_1 11_1 9_1)\\
\mathbb{Z}_{14} \times \mathbb{Z}_2 &: (0_1 12_1 2_0 3_0 1_1 9_0 8_0 11_1 7_1 4_1 5_0 2_1 11_0 13_1 6_1 13_0 5_1 9_1 3_1 8_1 4_0 6_0 12_0\\
&\quad\; 7_0 10_0 10_1 1_0)\\
\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 &: (0_{001} 3_{110} 0_{010} 0_{111} 2_{000})(0_{011} 2_{011} 3_{001} 2_{001} 2_{010} 1_{110} 1_{000})(0_{100} 3_{010})\\
&\quad (0_{101} 1_{010} 3_{000} 2_{101} 2_{111} 3_{111} 2_{110})(0_{110} 1_{011} 1_{100})\\
&\quad (1_{001} 1_{101} 3_{011} 1_{111} 2_{100} 3_{101} 3_{100})
\end{aligned}$$

We are now finally in a position to complete the proof of Theorem 1.1:

Proof. The strategy is to find a suitable factorisation $n = f_1 f_2 \cdots f_m \geqslant 9$ where $f_1 \geqslant f_2 \geqslant \cdots \geqslant f_m > 2$ and there exists a maximally nonassociative quasigroup of order f_1. We will then be able to iteratively use Corollary 2.4 to produce maximally nonassociative quasigroups of order $f_1 f_2$, $f_1 f_2 f_3, \ldots, f_1 f_2 \cdots f_m$.

Start with a factorisation of n into primes. We then modify the factorisation by taking the following steps in the given order:

(1) Repeatedly replace pairs of factors that both equal 2 by a single factor equal to 4, until there is at most one factor that equals 2.
(2) If the largest factor is currently at most 11 then look for two or three factors whose product is in $\{9,16,20,21,24,25,28,32,33,35,49,55,121\}$ and replace those factors by their product. If there are several options then choose one with the largest product.
(3) If there is a factor that equals 2, combine it with the next smallest factor.
(4) Sort the factors into weakly decreasing order.

It is possible that step (2) may fail; however that only happens if

$$n \in \{10,11,12,14,15,22,30,44,77,88,154\}$$

and these cases are excluded from Theorem 1.1. Assume that step (2) works and that $n = f_1 f_2 \cdots f_m$ is the factorisation that we arrive at after step (4). By design, $f_1 \geqslant f_2 \geqslant \cdots \geqslant f_m > 2$. Thus it suffices to find a maximally nonassociative quasigroup of order f_1.

If f_1 was created by step (4) then $n \in \{40,42,56,66,90,110\}$ or $n = 2p_1$ or $n = 2p_1p_2$ for odd primes p_1, p_2 with $p_1 \leqslant p_2 < 2p_1$. These cases are all excluded from Theorem 1.1. So we may assume that f_1 was not created by step (4). That means that f_1 is a prime larger than 11 or was created in step (2).

In Theorem 4.3, Theorem 4.6 and the surrounding comments we showed that there exists a maximally nonassociative quasigroup of order p for any prime $p > 11$ as well as of orders $3^2, 5^2, 7^2$ and 11^2. We have also given explicit examples of order 16, 20, 21, 24, 28, 32, 33, 35 and 55 earlier in this section. Thus in all cases there is a maximally nonassociative quasigroup of order f_1, which completes the proof. □

We finish by describing some questions raised by our work. The most obvious is to resolve the possible exceptions in Theorem 1.1. Another is to estimate the asymptotic proportion of quadratic orthomorphisms that satisfy the conditions of Theorem 3.5. Numerical experiments suggest that roughly 1/8 of quadratic orthomorphisms work when $q \equiv 1 \bmod 4$, whereas the proportion for $q \equiv 3 \bmod 4$ is closer to 1/20. The true asymptotic proportions have been established in a follow-up paper [5].

Another direction for research is to consider how few associative triples a quasigroup can achieve when it is not idempotent. Both [7] and [3] give lower bounds for the number of associative triples in this case. It remains to be determined whether these bounds are achieved and for what orders.

Our final research direction concerns the symmetry groups of maximally nonassociative quasigroups. The *automorphism group* of a quasigroup of order n is its stabiliser under the natural action of the symmetric group $\mathcal{S}_n$. Its *autoparatopism group* is its stabiliser under the action of $\mathcal{S}_n \wr \mathcal{S}_3$. Orbits under these actions are called *isomorphism classes* and *species* respectively. Examples built directly from quadratic orthomorphisms have a very large automorphism group, by Lemma 1.2. For example, there are 12 quadratic orthomorphisms of $\mathbb{F}_{27}$ that produce maximally nonassociative quasigroups. These form four isomorphism classes, which come from only two different species. Representatives of each species have automorphism group of order 351 (the minimum order possible, by Lemma 1.2) and autoparatopism groups of order 702 and 1053, respectively. In contrast, employing the product construction in Theorem 2.3 can destroy all symmetry. For example, suppose that we take Q to be the unique maximally nonassociative quasigroup of order 9 (which has automorphism group of order 72 and autoparatopism group of order 432, see [4]) and take U to be the unique idempotent quasigroup of order 3. There are $9 \times 8 \times 7 = 504$ choices for the injection j, and these produce 17 isomorphism classes of maximally nonassociative quasigroups of order 27. Examining representatives of the 17 classes, we find one with an automorphism group of order 6, another with an automorphism group of order 3, three with an automorphism group of order 2 and twelve with trivial automorphism group. All 17 representatives come from different species and have autoparatopism group equal to their automorphism group. In light of these observations, we ask what is the smallest order of a maximally nonassociative quasigroup with trivial automorphism group? Also it would be interesting to understand what automorphisms/autoparatopisms a maximally nonassociative quasigroup can have.

Supplementary data. Data that was generated in the computational proofs of Lemma 3.4, Theorem 4.3 and Theorem 4.6 for this article is available on the journal's website under `https://doi.org/10.5802/alco.165`. In addition, a number of examples of maximally nonassociate quasigroups are given on the second author's homepage [14].

Acknowledgements. This work was supported in part by Australian Research Council grant DP150100506. We thank Petr Lisoněk for keeping us informed regarding his paper [10] and Gabriel Verret for posing the question to us as to whether a maximally nonassociative quasigroup can have trivial automorphism group.

References

[1] Aleš Drápal and Petr Lisoněk, *Maximal nonassociativity via nearfields*, Finite Fields Appl. **62** (2020), 101610, 27pp.

[2] Aleš Drápal and Viliam Valent, *Few associative triples, isotopisms and groups*, Des. Codes Cryptogr. **86** (2018), 555–568.

[3] ———, *High nonassociativity in order 8 and an associative index estimate*, J. Combin. Des. **27** (2019), 205–228.

[4] ———, *Extreme nonassociativity in order nine and beyond*, J. Combin. Des. **28** (2020), 33–48.

[5] Aleš Drápal and Ian M. Wanless, *On the number of quadratic orthomorphisms that produce maximally nonassociative quasigroups*, `https://arxiv.org/abs/2005.11674`, 2020.

[6] Anthony B. Evans, *Orthogonal Latin squares based on groups*, Developments in Mathematics, vol. 57, Springer, Cham, 2018.

[7] Otokar Grošek and Peter Horák, *On quasigroups with few associative triples*, Des. Codes Cryptogr. **64** (2012), 221–227.

[8] Tomáš Kepka, *A note on associative triples of elements in cancellation groupoids*, Comment. Math. Univ. Carolin. **21** (1980), 479–487.

[9] Anton Kotzig and Corina Reischer, *Associativity index of finite quasigroups*, Glas. Mat. Ser. III **18** (1983), 243–253.

[10] Petr Lisoněk, *Maximal nonassociativity via fields*, Des. Codes Cryptogr. **88** (2020), 2521–2530.

[11] Antonio Rojas-León, *More general exponential and character sums*, in Handbook of Finite Fields (Gary L. Mullen and Daniel Panario, eds.), CRC Press, Boca Raton FL, 2013, pp. 161–169.

[12] Ian M. Wanless, *Diagonally cyclic Latin squares*, European J. Combin. **25** (2004), 393–413.

[13] ———, *Atomic Latin squares based on cyclotomic orthomorphisms*, Electron. J. Combin. **12** (2005), Paper no. R22 (23 pages).

[14] ———, *Author homepage*, `http://users.monash.edu.au/~iwanless/data`, 2020.

Aleš Drápal, Department of Mathematics, Charles University, Sokolovská 83, 186 75 Praha 8, Czech Republic
E-mail : `drapal@karlin.mff.cuni.cz`

Ian M. Wanless, School of Mathematics, Monash University, Clayton Vic 3800, Australia
E-mail : `ian.wanless@monash.edu`