LOOPS WITH EXPONENT THREE IN ALL ISOTOPES

MICHAEL KINYON AND IAN M. WANLESS†

ABSTRACT. It was shown by van Rees [18] that a latin square of order n cannot have more than $n^2(n-1)/18$ latin subsquares of order 3. He conjectured that this bound is only achieved if n is a power of 3. We show that it can only be achieved if $n \equiv 3 \bmod 6$. We also state several conditions that are equivalent to achieving the van Rees bound. One of these is that the Cayley table of a loop achieves the van Rees bound if and only if every loop isotope has exponent 3. We call such loops *van Rees loops* and show that they form an equationally defined variety.

We also show that (1) In a van Rees loop, any subloop of index 3 is normal, (2) There are exactly 6 nonassociative van Rees loops of order 27 with a non-trivial nucleus, (3) There is a Steiner quasigroup associated with every van Rees loop and (4) Every Bol loop of exponent 3 is a van Rees loop.

1. INTRODUCTION

The background prerequisites for this paper are the basic theories of quasigroups and loops [1, 17] and of latin squares [6]. Our results and proofs are a mix of the algebraic (quasigroups and loops) and combinatorial (latin squares) perspectives.

Throughout this paper $Q = (Q, \cdot)$ will denote a quasigroup or, in case there is a neutral element ε, a loop. We denote by L a latin square obtained from the (unbordered) Cayley table of Q (once an arbitrary ordering of the elements of Q has been fixed). For $x \in Q$, we define the *left* and *right translations* $L_x : Q \to Q$ and $R_x : Q \to Q$ by, respectively, $L_x(y) = xy$ and $R_x(y) = yx$ for $y \in Q$.

As usual, the latin square properties in which we are interested are those invariant, at the very least, under *isotopy*, that is, under permutations of the rows, of the columns and of the symbols. From the quasigroup perspective, we are interested in properties that hold in all *loop isotopes*. Given a quasigroup or loop $(Q, \cdot)$ and fixed elements $a, b \in Q$, we can define a loop $Q_{a,b} = (Q, \circ)$ with neutral element $\varepsilon = ba$ by $x \circ y = R_a^{-1}(x) \cdot L_b^{-1}(y)$. Further, all loops isotopic to (the quasigroup or loop) $(Q, \cdot)$ are isomorphic to isotopes of this form [1]. We will denote left and right translations in the loop isotope $Q_{a,b} = (Q, \circ)$ by L_x° and R_x°, respectively.

Since the notion of power of an element is not unambiguously defined in loops, in general it does not make sense to speak of the exponent of a loop. However, the loops we consider in this paper will satisfy the identity $xx \cdot x = x \cdot xx = \varepsilon$, and in this case we say that the loop has *exponent* 3.

A *subsquare* of a latin square is a submatrix that is itself a latin square. In [18], van Rees showed that no latin square of order n has more than $n^2(n-1)/18$ subsquares of order 3. For bounds on the number of subsquares of other orders, see [2, 3].

Our main result is the following.

Theorem 1. *Suppose $(Q, \cdot)$ is a quasigroup of order n with associated latin square L. The following conditions are equivalent:*

(1) *L has $n^2(n-1)/18$ subsquares of order 3.*
(2) *For any two occurrences of the same symbol in L, there is a subsquare of order 3 containing those two occurrences.*
(3) *Every cell in L is in $(n-1)/2$ subsquares of order 3.*
(4) *Every loop isotopic to Q has exponent 3.*

Date: February 28, 2011.
†Research supported by ARC grant DP0662946.

(5) *For any distinct* $x, y \in Q$, $L_x^{-1}L_y$ *and* $R_x^{-1}R_y$ *are regular permutations of order* 3.
(6) *In any loop isotope* $(Q, \circ)$ *and for each nonidentity element* $x \in Q$, L_x° *and* R_x° *are regular permutations of order* 3.
(7) *In any loop isotopic to* Q, *there are* $(n-1)/2$ *subloops of order* 3.

Note that (4), (6) and (7) are loop isotope conditions, (5) is a quasigroup (or loop) condition and (1), (2) and (3) are latin square conditions.

For reasons that will become apparent later, we call any quasigroup or loop satisfying Theorem 1(4) a *van Rees quasigroup* or *van Rees loop*, respectively, and any latin square satisfying Theorem 1(1) a *van Rees latin square*.

The outline of the paper is as follows. In the next section, after some preliminaries, we give the proof of Theorem 1, followed by some immediate consequences. In particular, quasigroups and loops satisfying the conditions of the theorem turn out to form varieties, not only of quasigroups (Theorem 2), but also of magmas, that is, sets with binary operations (Theorem 3). In §3 we give examples showing that the various conditions defining van Rees loops are, in fact, necessary. In §4, we examine a conjecture of van Rees regarding the possible orders of van Rees latin squares, and show that such a square has order congruent to 3 (mod 6) (Theorem 4). In §5, we look at several examples of nonassociative van Rees loops. In §6, we show that on the underlying set of a van Rees loop, there is a natural Steiner quasigroup structure (Theorem 9). Finally, in §7, we show that every Bol loop of exponent 3 is a van Rees loop (Theorem 10).

2. Proof of the Main Theorem

We will need the following two elementary results, which are well known and easy to prove.

Lemma 1. *Let* L *be a latin square.*
(1) *If two subsquares of a latin square* L *have nontrivial intersection, that intersection is itself a subsquare.*
(2) *If* S *is a subsquare of a latin square* L *and* $S \neq L$ *then the order of* S *cannot exceed half the order of* L.

Lemma 2. *Suppose* Q *is a loop with associated latin square* L *and neutral element* ε. *If* S *is a subsquare of* L *including the cell* $(\varepsilon, \varepsilon)$ *then the set of symbols occurring in* S *is a subloop of* Q.

Proof of Theorem 1. Let S_1, S_2 be subsquares of order 3 containing two different occurrences u, v of the same symbol x in L. Since $S_1 \cap S_2$ has order at least 2, Lemma 1 implies that $S_1 = S_2$. Thus any two occurrences of a symbol are in *at most* one subsquare of order 3.

Now, there are n choices for the symbol x and $\binom{n}{2}$ choices for the occurrences u, v. Each subsquare of order 3 contains $3\binom{3}{2} = 9$ pairs of entries with the same symbol. It follows that L can have at most

$$\frac{n\binom{n}{2}}{3\binom{3}{2}} = \frac{1}{18}n^2(n-1)$$

subsquares of order 3, with this bound being achieved if and only if condition (2) holds. That is, (1) $\iff$ (2)

(2)$\iff$(3): For a fixed choice of an occurrence u of a symbol, we have $n-1$ choices for a different occurrence v, and each subsquare of order 3 that includes u also includes two options for v.

(4) $\implies$ (5): If the loop isotope $Q_{a,b}$ has exponent 3, then for all $x \in Q$,

$$ba = xa \circ (xa \circ xa) = R_a^{-1}(xa) \cdot L_b^{-1}(R_a^{-1}(xa) \cdot L_b^{-1}(xa)) = L_x L_b^{-1} L_x L_b^{-1} L_x(a)\,,$$

and similarly, $ba = (bx \circ bx) \circ bx = R_x R_a^{-1} R_x R_a^{-1} R_x(b)$. Thus $(L_b^{-1}L_x)^3(a) = a$ and $(R_a^{-1}R_x)^3(b) = b$. We conclude that if every loop isotope of Q has exponent 3, then each $L_b^{-1}L_x$ and each $R_a^{-1}R_x$ is a regular permutation of order 3.

(5)$\Longleftrightarrow$(6): In the loop isotope $Q_{a,b}$, left translations are given by $L_x^\circ = L_{R_a^{-1}(x)} L_b^{-1}$ and right translations are given by $R_x^\circ = R_{L_b^{-1}(x)} R_a^{-1}$. Thus L_x° and R_x° are each regular of order 3 for *all* $x \in Q$ if and only if $L_x L_b^{-1}$ and $R_x R_a^{-1}$ are each regular of order 3 for *all* $x \in Q$. Universally quantifying a and b, we have the desired equivalence.

(5) $\Longrightarrow$ (2): Suppose s is a symbol in L occurring in the distinct cells (a, b) and (c, d) so that $s = ab = cd$ where $a \neq c$. Set $t = ad$ and $u = cb$. Since $L_a L_c^{-1}$ is regular of order 3, $t = L_a L_c^{-1}(s) = L_a L_c^{-1} L_a L_c^{-1}(cb) = L_c L_a^{-1}(u) = c \cdot L_a^{-1}(u)$. Similarly, since $R_d R_b^{-1}$ is regular of order 3, $t = R_d R_b^{-1}(s) = R_d R_b^{-1} R_d R_b^{-1}(cb) = R_b R_d^{-1}(u) = R_d^{-1}(u) \cdot b$. Now set $e = R_d^{-1}(u) = R_b^{-1}(t)$ and $f = L_a^{-1}(u) = L_c^{-1}(t)$. Note that $L_e^{-1}(u) = d$ and $L_e^{-1}(t) = b$. Since $L_c L_e^{-1}$ is regular of order 3, we have $s = cd = L_c L_e^{-1}(u) = L_c L_e^{-1} L_c(b) = L_c L_e^{-1} L_c L_e^{-1}(t) = L_e L_c^{-1}(t) = ef$. From these calculations, we deduce that L has a subsquare of order 3 containing the two occurrences of S, namely the subsquare labeled by the rows a, c, e and the columns b, d, f.

(2) $\Longrightarrow$ (4): Consider the loop isotope $Q_{a,b}$ with neutral element ba. Let $s \in Q \setminus \{ba\}$. By assumption, cells (ba, s) and (s, ba) are in a subsquare S of order 3, and hence by Lemma 1 are not in a subsquare of order 2. Thus $s^2 \neq ba$ and the symbols in S must be ba, s, s^2. Moreover, these symbols form a subloop of $Q_{a,b}$ by Lemma 2. As s was an arbitrary non-identity element, we conclude that $Q_{a,b}$ has exponent 3, that is, condition (4) holds.

(7) $\Longrightarrow$ (3): Let (a, b) be any cell in L. In the loop isotope $Q_{b,a}$ there are, by assumption, exactly $(n-1)/2$ subloops of order 3, each of which corresponds to a different subsquare of order 3 including the cell (a, b).

(3) $\Longrightarrow$ (7): In all loop isotopes $Q_{a,b}$, the cell (ba, ba) is in exactly $(n-1)/2$ subsquares of order 3, each of which corresponds to a different subloop of order 3, by Lemma 2. □

Corollary 1. *Any parastrophe of a van Rees quasigroup is also a van Rees quasigroup.*

Proof. Parastrophy preserves the number of subsquares of order 3. □

The permutations $L_x^{-1} L_y$ and $R_x^{-1} R_y$ that appear in Theorem 1(5) are important in the combinatorics of latin squares. Their expected structure in a randomly chosen latin square was studied in [5]. Meanwhile [4, 14, 20, 21] examine the case when $L_x^{-1} L_y$ and $R_x^{-1} R_y$ consist of a single cycle, regardless of the choice of distinct x, y.

We recall the universal algebraic definition of a quasigroup $(Q; \cdot, \backslash, /)$ is a set Q together with three operations $\cdot, \backslash, / : Q \times Q \to Q$ satisfying the identities $x\backslash(xy) = x(x\backslash y) = y$ and $(xy)/y = (x/y)y = x$.

Theorem 2. *The class of van Rees quasigroups [loops] $(Q, \cdot, \backslash, /)$ forms a variety of quasigroups [loops] defined by the identities*

(vR1) $$x(y\backslash(xz)) = y(x\backslash(yz))$$

(vR2) $$((xy)/z)y = ((xz)/y)z\,.$$

Proof. This is just Theorem 1(5) written explicitly in terms of the divisions $\backslash$ and $/$. □

The algebraic advantage of the three operation definition of quasigroups over the one operation definition is that homomorphic images under the latter definition need not be quasigroups. However, in this case, we can also view van Rees loops as varieties of magmas $(Q, \cdot)$.

Theorem 3. *The class of van Rees loops $(Q, \cdot)$ forms a variety of magmas (with neutral element) defined by the identities*

(vRL1) $$x(x \cdot xy) = y$$

(vRL2) $$(xy \cdot y)y = x$$

(vRL3) $$x \cdot y(y \cdot xz) = y \cdot x(x \cdot yz)$$

(vRL4) $$(xy \cdot z)z \cdot y = (xz \cdot y)y \cdot z\,.$$

Proof. If $(Q, \cdot, \backslash, /)$ satisfies (vR1), then taking $x = \varepsilon$, we obtain (vRL1), and similarly, (vR2) implies (vRL2). Now $x\backslash y = x \cdot xy$ and $x/y = xy \cdot y$, and so (vRL3) and (vRL4) are just (vR1) and (vR2) rewritten. Conversely, assume $(Q, \cdot, \backslash, /)$ satisfies (vRL1)–(vRL4). Define $x\backslash y = x(xy)$, and observe that (vRL1) implies $x\backslash(xy) = x(x\backslash y) = y$. Similarly defining $x/y = (xy)y$, (vRL2) implies $(xy)/y = (x/y)y = x$. Thus $(Q, \cdot, \backslash, /)$ is a quasigroup, and then (vR1) and (vR2) are just (vRL3) and (vRL4), respectively rewritten. □

The following is immediate from either Theorem 2 or 3.

Corollary 2. *Any subloop or homomorphic image of a van Rees quasigroup (loop) is a van Rees quasigroup (loop). Any subsquare of a van Rees latin square is a van Rees latin square.*

Proof. The first statement is just Birkhoff's theorem showing the equivalence of varieties and equational classes. The second statement follows because for any subsquare, there is a loop isotope that turns the subsquare into a subloop, in the sense of Lemma 2. □

3. Nonexamples

We now consider some examples of loops which are not van Rees loops to show that the various defining conditions are necessary. These examples were found by a mixture of the finite model builder Mace4 [15] and by home-grown software.

Example 1. Having exponent 3 is not, *a priori*, an isotopically invariant property of a loop. The smallest counterexample is given in Table 1. This loop has exponent 3, is commutative and has the weak inverse

·	ε	a	b	c	d	e	f
ε	ε	a	b	c	d	e	f
a	a	b	ε	e	f	c	d
b	b	ε	a	f	e	d	c
c	c	e	f	d	ε	a	b
d	d	f	e	ε	c	b	a
e	e	c	d	a	b	f	ε
f	f	d	c	b	a	ε	e

Table 1. A loop of exponent 3.

property, that is, it satisfies the identity $x(yx)^2 = y^2$. In fact, this loop is isotopic to the Steiner quasigroup of order 7. To see that it fails to be a van Rees loop, observe, for instance, that there is a subsquare of order 2 formed by rows a, b and columns c, d.

Example 2. A loop of exponent 3 can have all left and right translations be regular permutations of order 3, but still not have the van Rees property. Put another way, the identities (vRL3) and (vRL4) in Theorem 3 cannot be dispensed with. The smallest example showing this is given in Table 2. To see that this is not a van Rees loop, observe that the occurrences of d in the cells (ε, d) and (a, c) do not lie in a subsquare of order 3.

Example 3. Similarly, in Theorem 2, the conditions (vR1) and (vR2) are independent. In other words, for a quasigroup or loop to have the van Rees property, it is not sufficient that, say, $L_x^{-1}L_y$ be regular of order 3 for all distinct $x, y \in Q$. An example is the loop defined on $\mathbb{Z}_3 \times \mathbb{Z}_3$ by

$$(x, a)(y, b) = (x + y, a + b + x^2 y)\,.$$

This is one of the three nonassociative conjugacy closed loops of order 9, known as CCLoop(9,3) in the LOOPS package [16] for GAP [9]. This loop does not even have a well-defined exponent, for if $(xx)x = x(xx)$ for all x, then the loop would be power-associative, but the only power-associative conjugacy closed loops of order 9 are groups [13].

·	ε	a	b	c	d	e	f	g	h
ε	ε	a	b	c	d	e	f	g	h
a	a	b	ε	d	h	f	g	e	c
b	b	ε	a	e	f	g	h	c	d
c	c	g	h	f	a	b	ε	d	e
d	d	h	c	g	e	ε	a	b	f
e	e	c	g	h	ε	d	b	f	a
f	f	d	e	ε	g	h	c	a	b
g	g	e	f	a	b	c	d	h	ε
h	h	f	d	b	c	a	e	ε	g

TABLE 2. A loop of exponent 3 with left and right translations regular of order 3.

We have not been able to resolve the following.

Problem 1. *Let* $(Q, \cdot)$ *be a loop satisfying the identities* (vRL1), (vRL2) *and* (vRL3). *Must* $(Q, \cdot)$ *satisfy* (vRL4)?

4. van Rees' conjecture

In [18], van Rees conjectured that a latin square of order n cannot have $n^2(n-1)/18$ subsquares of order 3 unless n is a power of 3. This conjecture provided the original motivation for the present paper. In our terminology it can be stated like this:

Conjecture 1. *If* L *is a van Rees latin square, then the order of* L *is a power of* 3.

Example 4. Referring to Example 2, it is tempting to make a stronger conjecture than van Rees', namely that any loop of exponent 3 in which every left and right translation is a regular permutation of order 3 has order a power of 3. However, this is not true, as the loop given in Table 3 shows. If this were a

·	ε	a	b	c	d	e	f	g	h	i	j	k	l	m	n
ε	ε	a	b	c	d	e	f	g	h	i	j	k	l	m	n
a	a	b	ε	h	f	g	m	n	l	j	k	i	c	d	e
b	b	ε	a	g	h	f	j	k	i	d	e	c	n	l	m
c	c	d	e	f	i	n	ε	j	m	a	l	h	g	k	b
d	d	e	c	l	g	j	n	ε	k	f	a	m	b	h	i
e	e	c	d	k	m	h	i	l	ε	n	g	a	j	b	f
f	f	m	j	ε	l	k	c	e	d	b	i	g	h	n	a
g	g	n	k	i	ε	m	e	d	c	h	b	j	a	f	l
h	h	l	i	n	j	ε	d	c	e	k	f	b	m	a	g
i	i	f	m	b	k	d	g	a	n	l	h	e	ε	c	j
j	j	g	n	e	b	i	l	h	a	c	m	f	k	ε	d
k	k	h	l	j	c	b	a	m	f	g	d	n	e	i	ε
l	l	k	g	m	a	c	b	f	j	ε	n	d	i	e	h
m	m	i	h	d	n	a	k	b	g	e	ε	l	f	j	c
n	n	j	f	a	e	l	h	i	b	m	c	ε	d	g	k

TABLE 3. Another loop of exponent 3 with left and right translations regular of order 3.

van Rees loop, it would have 175 subsquares of order 3, but it has only 24 such subsquares. However, it does satisfy $L_x^3 = R_x^3 = 1$ for all x.

Lemma 3. *A finite loop of exponent* 3 *has odd order.*

Proof. Let Q be a loop of exponent 3, and consider the mapping $Q \to Q; x \mapsto x^2 = x^{-1}$. This map is an involution of the set $Q^* = Q\backslash\{1\}$ of nonidentity elements of Q, and does not fix any elements of Q^*. Thus $|Q^*|$ is even, and hence $|Q|$ is odd. □

We have been unable to settle Conjecture 1, but we can show:

Theorem 4. *A van Rees quasigroup or van Rees latin square has order $n \equiv 3 \bmod 6$.*

Proof. Suppose there is a van Rees quasigroup of order n. By Lemma 3, n is odd. By Theorem 1(6), n is divisible by 3. □

By computer search, we have established that there are no van Rees loops of orders 15 or 21. Hence the smallest possible order for a counterexample to van Rees' conjecture is 33. Also, given Corollary 2, we conclude that every subloop of a van Rees loop has order $m \equiv 3 \mod 6$ where m is a power of 3 or $m \geqslant 33$.

Theorem 5. *If S is a subloop of index 3 in a van Rees loop Q then S is normal in Q.*

Proof. For $q \in Q \setminus S$ define $T_q = \{x\backslash q : x \in S\}$ and $U_q = \{q/x : x \in S\}$. Let Σ_0 be the subsquare $\{(s_1, s_2, s_1 \circ s_2) : s_1, s_2 \in S\}$.

Suppose $r_1, c_1 \in S$. By Theorem 1 there is a subsquare Σ_3 of order 3 including the triples $(r_1, r_1\backslash q, q)$ and $(q/c_1, c_1, q)$. Suppose the rows and columns of Σ_3 are respectively $\{r_1, q/c_1, r_2\}$ and $\{r_1\backslash q, c_1, c_2\}$. Since $r_1, c_1 \in S$ and $q/c_1 \notin S$ we can see from Lemma 1 that $\Sigma_0 \cap \Sigma_3$ is a subsquare of order 1. This means that $\{q/c_1, r_2, r_1\backslash q, c_2\} \cap S = \emptyset$. Also $r_1 \circ (r_1\backslash q) = (q/c_1) \circ c_1 = r_2 \circ c_2 = q$. It follows that $r_2 \notin U_q$ and $c_2 \notin T_q$.

Consider fixing r_1 and allowing c_1 to vary over S. We find that $r_2 \circ (r_1\backslash q) = r_1 \circ c_1$ varies over S. Next allowing r_1 to vary over S, we conclude that the set of cells $\big(Q \setminus \big(S \cup U_q\big)\big) \times T_q$ form a subsquare with symbols S. Similarly, the cells $U_q \times \big(Q \setminus (S \cup T_q)\big)$ form a subsquare with symbols S. The position of these subsquares is a property of the loop independent of the choice of q. Hence for any $q' \in Q \setminus S$ we must have either $U_{q'} = U_q$ and $T_{q'} = T_q$ or else $U_{q'} = Q \setminus (S \cup U_q)$ and $T_{q'} = Q \setminus (S \cup T_q)$. It follows that the cells $U_q \times S$ and $S \times T_q$ form subsquares on the same symbols. Together with the subsquares already identified, these are sufficient to show that S is normal in Q. □

Theorem 5 cannot be generalised to subloops of index 9. For example, in the non-abelian group of exponent 3 and order 27, only 1 of the 13 subgroups of order 3 is normal.

Theorem 6. *Let the loop $(Q, \cdot)$ be a minimal counterexample to Conjecture 1. Then Q is simple.*

Proof. If Q had a proper normal subloop N, then by Corollary 2, both N and Q/N would be van Rees loops. By minimality of Q, each of $|N|$ and $|Q/N|$ are powers of 3, and hence, so is $|Q|$, a contradiction. □

5. Examples and Classification

In this section we consider various examples of van Rees loops. Obvious examples are elementary abelian 3-groups and nonabelian groups of exponent 3. These can never yield a counterexample to Conjecture 1. Thus we are primarily interested in nonassociative examples. We can obviously rule out order 3, and, by the following result, order 9.

Theorem 7. *A van Rees loop of order 9 is an elementary abelian 3-group.*

Proof. Let Q be a van Rees loop of order 9. Any nonidentity element generates a subloop of order 3, and every such subloop is normal by Theorem 5. Take any two distinct such subloops, say H and K. Noting that $|H| \cdot |K| = 9$ and $H \cap K = \{1\}$, we have that Q is a direct product of cyclic groups of order 3. Thus Q is associative and elementary abelian as claimed. □

Recall that the *left*, *middle* and *right nuclei* of a loop Q are the sets

$$N_\lambda(Q) = \{a \in Q \mid (ax)y = a(xy),\ \forall x, y \in Q\},$$
$$N_\mu(Q) = \{a \in Q \mid (xa)y = x(ay),\ \forall x, y \in Q\},$$
$$N_\rho(Q) = \{a \in Q \mid (xy)a = x(ya),\ \forall x, y \in Q\},$$

respectively. The *center* $Z(Q) = N_\lambda(Q) \cap N_\mu(Q) \cap N_\rho(Q) \cap \{a \in Q \mid ax = xa,\ \forall x \in Q\}$.

Loops Q_1, Q_2 are said to be *paratopic* (or *isostrophic*) if Q_1 is isotopic to a conjugate (or parastrophe) of the other. Using a computer search, we have classified up to paratopy all van Rees loops of order 27 such that at least one of the nuclei is nontrivial. (Note that it is irrelevant which nucleus is specified to be nontrivial. If a loop has, say, nontrivial left nucleus, then there is a paratope with nontrivial middle nucleus and a paratope with nontrivial right nucleus.) We do not know of any examples of van Rees loops with all nuclei trivial.

Theorem 8. *Up to paratopy, there are exactly six nonassociative van Rees loops of order* 27 *with at least one nontrivial nucleus.*

The six species in the theorem include the following representatives, each in a different class:

- A Bol loop with trivial center, discovered by Keedwell [11, 12] and described in [8].
- Two power-associative conjugacy closed loops, described in [13].
- A universal left conjugacy closed loop (which is not conjugacy closed) with the left inverse property; see Table 4.
- A commutative, weak inverse property loop; see Table 5.
- A (noncommutative) weak inverse property loop such that each inner mapping of the form $L_x^{-1}R_x$ is an automorphism; see Table 6.

The species with the Bol loop is the only one such that each loop in the species has trivial center.

Finally, we should mention that nonassociative Moufang loops of order 3^k, $k \geqslant 4$, are also examples of van Rees loops.

6. Steiner quasigroups

Recall that a quasigroup $(Q, \cdot)$ is said to be *Steiner* if it satisfies the identities $xx = x$, $x(yx) = y$ and $xy = yx$.

Theorem 9. *If $(Q, \cdot)$ is a van Rees loop, then $(Q, *)$ defined by*

$$x * y = x(y \cdot yx)$$

is a Steiner quasigroup.

Proof. That $x * x = x$ follows since $(Q, \cdot)$ has exponent 3. For commutativity, $x * y = x \cdot y(y \cdot x\varepsilon) = y \cdot x(x \cdot y\varepsilon) = y * x$ by (vRL3). Next, we compute

$$y = (xy \cdot y) \cdot [(xy \cdot y) \cdot (xy \cdot y)y] = (xy \cdot y) \cdot [(xy \cdot y)x],$$

using (vRL1) and (vRL2). Replacing y with $x \cdot xy$, we have

$$x \cdot xy = (x(x \cdot xy) \cdot (x \cdot xy)) \cdot [(x(x \cdot xy) \cdot (x \cdot xy))x] = y(x \cdot xy) \cdot [y(x \cdot xy) \cdot x],$$

using (vRL1). Thus

$$x * (y * x) = x\{y(x \cdot xy) \cdot [y(x \cdot xy) \cdot x]\} = x\{x \cdot xy\} = y,$$

by (vRL1). This completes the proof. □

In every example of a van Rees loop described in §5, the Steiner quasigroup $(Q, *)$ associated to a van Rees loop Q is itself a van Rees quasigroup. Nevertheless, we have not been able to resolve the following.

$\cdot$	ε	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
ε	ε	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	a	b	ε	e	g	f	c	h	d	j	k	i	m	n	l	p	q	o	s	t	r	v	w	u	y	z	x
b	b	ε	a	f	h	c	e	d	g	k	i	j	n	l	m	q	o	p	t	r	s	w	u	v	z	x	y
c	c	e	f	d	ε	g	h	a	b	o	p	q	r	s	t	w	u	v	y	z	x	j	k	i	n	l	m
d	d	g	h	ε	c	a	b	e	f	w	u	v	y	z	x	i	j	k	l	m	n	p	q	o	t	r	s
e	e	f	c	g	a	h	d	b	ε	p	q	o	s	t	r	u	v	w	z	x	y	k	i	j	l	m	n
f	f	c	e	h	b	d	g	ε	a	q	o	p	t	r	s	v	w	u	x	y	z	i	j	k	m	n	l
g	g	h	d	a	e	b	ε	f	c	u	v	w	z	x	y	j	k	i	m	n	l	q	o	p	r	s	t
h	h	d	g	b	f	ε	a	c	e	v	w	u	x	y	z	k	i	j	n	l	m	o	p	q	s	t	r
i	i	j	k	o	w	p	q	u	v	l	m	n	ε	a	b	r	s	t	c	e	f	z	x	y	h	d	g
j	j	k	i	p	u	q	o	v	w	m	n	l	a	b	ε	s	t	r	e	f	c	x	y	z	d	g	h
k	k	i	j	q	v	o	p	w	u	n	l	m	b	ε	a	t	r	s	f	c	e	y	z	x	g	h	d
l	l	m	n	r	y	s	t	z	x	ε	a	b	i	j	k	c	e	f	o	p	q	g	h	d	v	w	u
m	m	n	l	s	z	t	r	x	y	a	b	ε	j	k	i	e	f	c	p	q	o	h	d	g	w	u	v
n	n	l	m	t	x	r	s	y	z	b	ε	a	k	i	j	f	c	e	q	o	p	d	g	h	u	v	w
o	o	p	q	u	k	v	w	i	j	s	t	r	f	c	e	x	y	z	d	g	h	m	n	l	ε	a	b
p	p	q	o	v	i	w	u	j	k	t	r	s	c	e	f	y	z	x	g	h	d	n	l	m	a	b	ε
q	q	o	p	w	j	u	v	k	i	r	s	t	e	f	c	z	x	y	h	d	g	l	m	n	b	ε	a
r	r	s	t	z	n	x	y	l	m	f	c	e	p	q	o	d	g	h	v	w	u	b	ε	a	k	i	j
s	s	t	r	x	l	y	z	m	n	c	e	f	q	o	p	g	h	d	w	u	v	ε	a	b	i	j	k
t	t	r	s	y	m	z	x	n	l	e	f	c	o	p	q	h	d	g	u	v	w	a	b	ε	j	k	i
u	u	v	w	i	q	j	k	o	p	x	y	z	d	g	h	m	n	l	b	ε	a	s	t	r	c	e	f
v	v	w	u	j	o	k	i	p	q	y	z	x	g	h	d	n	l	m	ε	a	b	t	r	s	e	f	c
w	w	u	v	k	p	i	j	q	o	z	x	y	h	d	g	l	m	n	a	b	ε	r	s	t	f	c	e
x	x	y	z	m	r	n	l	s	t	g	h	d	w	u	v	ε	a	b	k	i	j	c	e	f	o	p	q
y	y	z	x	n	s	l	m	t	r	h	d	g	u	v	w	a	b	ε	i	j	k	e	f	c	p	q	o
z	z	x	y	l	t	m	n	r	s	d	g	h	v	w	u	b	ε	a	j	k	i	f	c	e	q	o	p

TABLE 4. A universal left conjugacy closed, left inverse property, van Rees loop.

Problem 2. *Let $(Q, \cdot)$ be a van Rees loop with associated Steiner quasigroup $(Q, *)$. Is $(Q, *)$ a van Rees quasigroup?*

We also do not know if van Rees' Conjecture 1 holds for Steiner quasigroups. Note that every *distributive* Steiner quasigroup is a van Rees quasigroup: $x(y \cdot xz) = xy \cdot (x \cdot xz) = xy \cdot z = yx \cdot z = yx \cdot (y \cdot yz) = y(x \cdot yz)$. An affirmative answer to Conjecture 1 in the Steiner case would generalize the well-known fact that every finite distributive Steiner quasigroup has order a power of 3. In fact, Conjecture 1 can be resolved affirmatively in general if it is resolved in the Steiner case, and if Problem 2 has an affirmative answer.

7. Bol loops of exponent 3

In this final section, we turn to the following problem:

Suppose $\mathcal{V}$ is an isotopically invariant variety of loops, and suppose $Q \in \mathcal{V}$ has exponent 3. Must Q be a van Rees loop?

The answer is no for the variety of *all* loops as Example 1 shows. The example also shows why it is reasonable to restrict the problem to isotopically invariant varieties; the example is commutative and has the weak inverse property, neither of which is an isotopically invariant property.

Every conjugacy closed loop of exponent 3 is also a van Rees loop; this follows from the fact that conjugacy closed loops are isotopic to all of their isotopes [10]. Also, every Moufang loop of exponent 3 is a van Rees loop [1].

$\cdot$	ε	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
ε	ε	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	a	b	ε	e	g	f	c	h	d	j	k	i	m	n	l	p	q	o	s	t	r	v	w	u	y	z	x
b	b	ε	a	f	h	c	e	d	g	k	i	j	n	l	m	q	o	p	t	r	s	w	u	v	z	x	y
c	c	e	f	d	ε	g	h	a	b	o	p	q	t	r	s	u	v	w	y	z	x	i	j	k	l	m	n
d	d	g	h	ε	c	a	b	e	f	w	u	v	z	x	y	k	i	j	l	m	n	q	o	p	s	t	r
e	e	f	c	g	a	h	d	b	ε	p	q	o	r	s	t	v	w	u	z	x	y	j	k	i	m	n	l
f	f	c	e	h	b	d	g	ε	a	q	o	p	s	t	r	w	u	v	x	y	z	k	i	j	n	l	m
g	g	h	d	a	e	b	ε	f	c	u	v	w	x	y	z	i	j	k	m	n	l	o	p	q	t	r	s
h	h	d	g	b	f	ε	a	c	e	v	w	u	y	z	x	j	k	i	n	l	m	p	q	o	r	s	t
i	i	j	k	o	w	p	q	u	v	l	m	n	ε	a	b	r	s	t	c	e	f	y	z	x	d	g	h
j	j	k	i	p	u	q	o	v	w	m	n	l	a	b	ε	s	t	r	e	f	c	z	x	y	g	h	d
k	k	i	j	q	v	o	p	w	u	n	l	m	b	ε	a	t	r	s	f	c	e	x	y	z	h	d	g
l	l	m	n	t	z	r	s	x	y	ε	a	b	i	j	k	f	c	e	q	o	p	d	g	h	v	w	u
m	m	n	l	r	x	s	t	y	z	a	b	ε	j	k	i	c	e	f	o	p	q	g	h	d	w	u	v
n	n	l	m	s	y	t	r	z	x	b	ε	a	k	i	j	e	f	c	p	q	o	h	d	g	u	v	w
o	o	p	q	u	k	v	w	i	j	r	s	t	f	c	e	x	y	z	g	h	d	m	n	l	ε	a	b
p	p	q	o	v	i	w	u	j	k	s	t	r	c	e	f	y	z	x	h	d	g	n	l	m	a	b	ε
q	q	o	p	w	j	u	v	k	i	t	r	s	e	f	c	z	x	y	d	g	h	l	m	n	b	ε	a
r	r	s	t	y	l	z	x	m	n	c	e	f	q	o	p	g	h	d	w	u	v	a	b	ε	k	i	j
s	s	t	r	z	m	x	y	n	l	e	f	c	o	p	q	h	d	g	u	v	w	b	ε	a	i	j	k
t	t	r	s	x	n	y	z	l	m	f	c	e	p	q	o	d	g	h	v	w	u	ε	a	b	j	k	i
u	u	v	w	i	q	j	k	o	p	y	z	x	d	g	h	m	n	l	a	b	ε	t	r	s	f	c	e
v	v	w	u	j	o	k	i	p	q	z	x	y	g	h	d	n	l	m	b	ε	a	r	s	t	c	e	f
w	w	u	v	k	p	i	j	q	o	x	y	z	h	d	g	l	m	n	ε	a	b	s	t	r	e	f	c
x	x	y	z	l	s	m	n	t	r	d	g	h	v	w	u	ε	a	b	k	i	j	f	c	e	o	p	q
y	y	z	x	m	t	n	l	r	s	g	h	d	w	u	v	a	b	ε	i	j	k	c	e	f	p	q	o
z	z	x	y	n	r	l	m	s	t	h	d	g	u	v	w	b	ε	a	j	k	i	e	f	c	q	o	p

TABLE 5. A commutative, weak inverse property, van Rees loop.

The main result of this section generalizes this last assertion. A loop Q is a *left Bol loop* if it satisfies the identity $(x \cdot yx)z = x(y \cdot xz)$ for all $x, y, z \in Q$. Every left Bol loop is *left alternative*, that is, it satisfies the identity $x \cdot xy = x^2y$. Also, every left Bol loop has the *left inverse property*, that is, it satisfies $x^{-1} \cdot xy = y$.

Theorem 10. *Let $(Q, \cdot)$ be a left Bol loop of exponent 3. Then Q is a van Rees loop.*

Proof. Set $x + y = (x \cdot y^2x)^2$. Then the magma $(Q, +)$ is a *Bruck* loop, that is, it is a Bol loop satisfying the additional identity $(x + y)^{-1} = x^{-1} + y^{-1}$; see, for instance, [7]. Further, $(Q, +)$ also has exponent 3. Bruck loops of exponent 3 are commutative [19]. Thus $(x \cdot y^2x)^2 = (y \cdot x^2y)^2$, and so

$$x \cdot y^2x = y \cdot x^2y\,. \tag{1}$$

Next, $x(y^2 \cdot xy^2) = (x \cdot y^2x)y^2 = (y \cdot x^2y)y^2 = y(x^2 \cdot yy^2) = yx^2$, using (1). Replacing y with y^2, we have

$$x(y \cdot xy) = y^2x^2\,. \tag{2}$$

For (vRL1): $x(x \cdot xy) = (x \cdot xx)y = y$.

For (vRL2): Using (2), we have $y^2 = x \cdot x^2y^2 = x \cdot y(x \cdot yx) = (x \cdot yx) \cdot yx$, and so $yx = (x \cdot yx)^{-1}y^2$. Replacing x with y^2x, we get $x = y \cdot y^2x = [y^2x \cdot (y \cdot y^2x)]^{-1}y^2 = [y^2x \cdot x]^{-1}y^2$. Thus $(y^2x \cdot x)x = y^2$. Replacing y with y^2, we obtain (vRL2).

For (vRL3): $x \cdot y(y \cdot xz) = x(y^2 \cdot xz) = (x \cdot y^2x)z = (y \cdot x^2y)z = y(x^2 \cdot yz) = y \cdot x(x \cdot yz)$, using (1).

·	ε	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
ε	ε	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	a	b	ε	e	g	f	c	h	d	j	k	i	m	n	l	p	q	o	s	t	r	v	w	u	y	z	x
b	b	ε	a	f	h	c	e	d	g	k	i	j	n	l	m	q	o	p	t	r	s	w	u	v	z	x	y
c	c	e	f	d	ε	g	h	a	b	o	p	q	s	t	r	u	v	w	y	z	x	i	j	k	m	n	l
d	d	g	h	ε	c	a	b	e	f	v	w	u	x	y	z	j	k	i	l	m	n	p	q	o	r	s	t
e	e	f	c	g	a	h	d	b	ε	p	q	o	t	r	s	v	w	u	z	x	y	j	k	i	n	l	m
f	f	c	e	h	b	d	g	ε	a	q	o	p	r	s	t	w	u	v	x	y	z	k	i	j	l	m	n
g	g	h	d	a	e	b	ε	f	c	w	u	v	y	z	x	k	i	j	m	n	l	q	o	p	s	t	r
h	h	d	g	b	f	ε	a	c	e	u	v	w	z	x	y	i	j	k	n	l	m	o	p	q	t	r	s
i	i	j	k	p	u	q	o	v	w	l	m	n	ε	a	b	s	t	r	e	f	c	x	y	z	d	g	h
j	j	k	i	q	v	o	p	w	u	m	n	l	a	b	ε	t	r	s	f	c	e	y	z	x	g	h	d
k	k	i	j	o	w	p	q	u	v	n	l	m	b	ε	a	r	s	t	c	e	f	z	x	y	h	d	g
l	l	m	n	r	y	s	t	z	x	ε	a	b	i	j	k	c	e	f	o	p	q	g	h	d	v	w	u
m	m	n	l	s	z	t	r	x	y	a	b	ε	j	k	i	e	f	c	p	q	o	h	d	g	w	u	v
n	n	l	m	t	x	r	s	y	z	b	ε	a	k	i	j	f	c	e	q	o	p	d	g	h	u	v	w
o	o	p	q	v	i	w	u	j	k	r	s	t	e	f	c	x	y	z	d	g	h	m	n	l	ε	a	b
p	p	q	o	w	j	u	v	k	i	s	t	r	f	c	e	y	z	x	g	h	d	n	l	m	a	b	ε
q	q	o	p	u	k	v	w	i	j	t	r	s	c	e	f	z	x	y	h	d	g	l	m	n	b	ε	a
r	r	s	t	x	m	y	z	n	l	c	e	f	p	q	o	g	h	d	u	v	w	ε	a	b	i	j	k
s	s	t	r	y	n	z	x	l	m	e	f	c	q	o	p	h	d	g	v	w	u	a	b	ε	j	k	i
t	t	r	s	z	l	x	y	m	n	f	c	e	o	p	q	d	g	h	w	u	v	b	ε	a	k	i	j
u	u	v	w	j	o	k	i	p	q	y	z	x	d	g	h	l	m	n	ε	a	b	r	s	t	e	f	c
v	v	w	u	k	p	i	j	q	o	z	x	y	g	h	d	m	n	l	a	b	ε	s	t	r	f	c	e
w	w	u	v	i	q	j	k	o	p	x	y	z	h	d	g	n	l	m	b	ε	a	t	r	s	c	e	f
x	x	y	z	l	s	m	n	t	r	g	h	d	u	v	w	ε	a	b	j	k	i	c	e	f	o	p	q
y	y	z	x	m	t	n	l	r	s	h	d	g	v	w	u	a	b	ε	k	i	j	e	f	c	p	q	o
z	z	x	y	n	r	l	m	s	t	d	g	h	w	u	v	b	ε	a	i	j	k	f	c	e	q	o	p

TABLE 6. A noncommutative, weak inverse property, van Rees loop with each $L_x^{-1}R_x$ an automorphism.

For (vRL4): Substituting $(xz{\cdot}y)y$ for x in $y = x^2{\cdot}xy$ gives $y = [(xz{\cdot}y)y]^2{\cdot}[(xz{\cdot}y)y{\cdot}y] = [(xz{\cdot}y)y]^2{\cdot}xz$, by (vRL2), so

$$\begin{aligned}
(xy\cdot z)z\cdot y &= (x\{[(xz\cdot y)y]^2\cdot xz\}\cdot z)z\cdot y \\
&= ((x\cdot[(xz\cdot y)y]^2x)z\cdot z)z\cdot y \\
&= (x\cdot[(xz\cdot y)y]^2x)y \\
&= ([(xz\cdot y)y]\cdot x^2[(xz\cdot y)y])y \\
&= (xz\cdot y)y\cdot x^2([(xz\cdot y)y]\cdot y) \\
&= (xz\cdot y)y\cdot x^2(xz) \\
&= (xz\cdot y)y\cdot z\,,
\end{aligned}$$

where we have used (vRL2) in the third equality, (1) in the fourth and (vRL2) again in the sixth.

Having verified the conditions of Theorem 3, we conclude that Q is a van Rees loop. □

REFERENCES

[1] R. H. Bruck, *A Survey of Binary Systems*, Springer-Verlag, 1971.

[2] J. Browning, D. S. Stones and I. M. Wanless, Bounds on the number of autotopisms and subsquares of a latin square, submitted.

[3] J. Browning, P. Vojtěchovský and I. M. Wanless, Overlapping latin subsquares and full products, *Comment. Math. Univ. Carolin.* **51** (2010) 175–184.
[4] D. Bryant, B. Maenhaut and I. M. Wanless, New families of atomic Latin squares and perfect one-factorisations, *J. Combin. Theory Ser. A*, **113** (2006), 608–624.
[5] N. J. Cavenagh, C. Greenhill and I. M. Wanless, The cycle structure of two rows in a random latin square, *Random Structures Algorithms*, **33** (2008), 286–309.
[6] J. Dénes and A. D. Keedwell, *Latin squares and their applications*, Academic Press, 1974.
[7] T. Foguel, M. K. Kinyon and J. D. Phillips, On twisted subgroups and Bol loops of odd order, *Rocky Mountain Math. J.* **36** (2006), 183–212.
[8] T. Foguel and M. Kinyon, Uniquely 2-divisible Bol loops, *J. Algebra Appl.* **9** (2010), 591–601.
[9] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.10*; 2007, (`http://www.gap-system.org`)
[10] E. G. Goodaire and D. A. Robinson, A class of loops which are isomorphic to all loop isotopes, *Canad. J. Math.* **34** (1982), 662–672.
[11] A. D. Keedwell, On the order of projective planes with characteristic, *Rend. Mat. e Appl.* (5) **22** (1963), 498–530.
[12] A. D. Keedwell, A search for projective planes of a special type with the aid of a digital computer, *Math. Comp.* **19** (1965), 317–322
[13] M. K. Kinyon and K. Kunen, Power-associative, conjugacy closed loops, *J. Algebra* **304** (2006), 679–711.
[14] B. M. Maenhaut and I. M. Wanless, Atomic Latin squares of order eleven, *J. Combin. Designs*, **12** (2004), 12–34.
[15] W. McCune, *Prover9 and Mace4*, version 2008-06A, (`http://www.cs.unm.edu/~mccune/prover9/`)
[16] G. Nagy and P. Vojtěchovský, *LOOPS: Computing with quasigroups and loops in GAP* – a GAP package, version 2.0.0, 2008, (`http://www.math.du.edu/loops`)
[17] H. O. Pflugfelder, *Quasigroups and Loops: Introduction*, Sigma Series in Pure Math. **8**, Heldermann Verlag, Berlin, 1990.
[18] G. H. J. van Rees, Subsquares and transversals in latin squares, *Ars Combin.* **29**B (1990) 193–204.
[19] D. Robinson, Bol quasigroups, *Publ. Math. Debrecen* **19** (1972), 151–153.
[20] I. M. Wanless, Perfect factorisations of bipartite graphs and Latin squares without proper subrectangles, *Electron. J. Combin.* **6** (1999), R9.
[21] I. M. Wanless, Atomic Latin squares based on cyclotomic orthomorphisms, *Electron. J. Combin.*, **12** (2005), R22.

Department of Mathematics, 2360 S Gaylord St, University of Denver, Denver, CO 80208 USA
E-mail address: `michael.kinyon@du.edu`

School of Mathematical Sciences, Monash University, Vic 3800, Australia
E-mail address: `ian.wanless@monash.edu`