The Order of Automorphisms of Quasigroups

Brendan D. McKay,[1] Ian M. Wanless,[2] and Xiande Zhang[2]

[1]Research School of Computer Science, Australian National University, Canberra, ACT 0200, Australia, E-mail: bdm@cs.anu.edu.au

[2]School of Mathematical Sciences, Monash University, Clayton, Vic 3800, Australia, E-mail: ian.wanless@monash.edu; xdzhangzju@gmail.com

Received October 8, 2013; revised January 3, 2014

Published online 13 February 2014 in Wiley Online Library (wileyonlinelibrary.com).
DOI 10.1002/jcd.21389

Abstract: **We prove quadratic upper bounds on the order of any autotopism of a quasigroup or Latin square, and hence also on the order of any automorphism of a Steiner triple system or 1-factorization of a complete graph. A corollary is that a permutation σ chosen uniformly at random from the symmetric group $\mathcal{S}_n$ will almost surely not be an automorphism of a Steiner triple system of order n, a quasigroup of order n or a 1-factorization of the complete graph K_n. Nor will σ be one component of an autotopism for any Latin square of order n. For groups of order n it is known that automorphisms must have order less than n, but we show that quasigroups of order n can have automorphisms of order greater than n. The smallest such quasigroup has order 7034. We also show that quasigroups of prime order can possess autotopisms that consist of three permutations with different cycle structures. Our results answer three questions originally posed by D. Stones.** © 2014 Wiley Periodicals, Inc. J. Combin. Designs 23: 275–288, 2015

Keywords: *quasigroup; automorphism; Latin square; autotopism; autoparatopism; Steiner triple system; 1-factorization*

MSC Classification: *05B15; 20N05 (05B05; 05C70)*

1. INTRODUCTION

An $n \times n$ *Latin square* is an $n \times n$ array of n symbols such that each symbol occurs exactly once in each row and exactly once in each column. A *quasigroup* Q is a nonempty set with

Contract grant sponsor: Australian Research Council; contract grant numbers: DP1093320 and FT110100065; contract grant numbers: NSFC; contract grant numbers: 11301503 (to X.Z.).

one binary operation $\star$ such that for every $a, b \in Q$ there is a unique $x \in Q$ and a unique $y \in Q$ satisfying $a \star x = b$ and $y \star a = b$. Multiplication tables of finite quasigroups are Latin squares.

Let $[n] = \{1, 2, \dots, n\}$ and let $\mathcal{S}_n$ denote the symmetric group on $[n]$. It is convenient to associate a quasigroup (or Latin square) of order n with a set of n^2 triples in $[n] \times [n] \times [n]$, with the property that no two distinct triples agree in more than one coordinate. If (r, c, s) is one of the triples then the interpretation is that $r \star c = s$. This interpretation in terms of triples allows for a natural action of $\mathcal{S}_n \times \mathcal{S}_n \times \mathcal{S}_n$ on quasigroups of order n. This action is known as *isotopism* and its diagonal subgroup is known as *isomorphism*. There is also a natural action of $\mathcal{S}_n \wr \mathcal{S}_3$ on triples, which is known as *paratopism*. The orbits of a quasigroup under isomorphism, isotopism, and paratopism, respectively, are known as its isomorphism class, isotopism class, and paratopism class (this last is also known as *species* or *main class*). The stabilizers of a quasigroup under isomorphism, isotopism, and paratopism are known respectively as its automorphism group, autotopism group, and autoparatopism group. For a quasigroup Q we denote these groups by aut(Q), atp(Q), and par(Q), respectively. These symmetries of quasigroups play an important role in various enumeration problems (e.g. [2,7,9,12,13]). For studies of which symmetries can be achieved, see [3,14,16].

This paper is motivated by several questions posed by D. Stones [11], which were also published in [14]. Specifically, we resolve the following conjecture and two open questions.

Conjecture 1. *For $n > 0$ let $\mathbb{P}(n)$ be the probability that a randomly chosen $\alpha \in \mathcal{S}_n$ is a component of an autotopism (α, β, γ) of some quasigroup of order n. Then* $\lim_{n\to\infty} \mathbb{P}(n) = 0$.

Problem 1. *Suppose θ is an autotopism of a quasigroup of order n. Is the order of θ at most n?*

Problem 2. *Let (α, β, γ) be an autotopism of a quasigroup of prime order p. Must it be true that either*

1. *one of α, β or γ is the identity and the other two are p-cycles; or*
2. *α, β, and γ all have the same cycle structure?*

It was previously known that both open problems have an affirmative answer for small orders, but we show for both that the answer is negative in general. Interestingly, Horoševskiĭ [6] proved that if G is a group of order $n > 1$, then any automorphism of G has order at most $n - 1$. We show in Section 4 that this property does not extend to quasigroups, but in Section 3 we show that there is a quadratic upper bound on the order of any automorphism. Our bound necessarily applies to several combinatorial objects related to quasigroups. In particular, it is well known that a totally symmetric idempotent quasigroup is equivalent to a Steiner triple system, whereas a symmetric idempotent quasigroup is equivalent to a 1-factorization of a complete graph.

A number of computational results are reported in this paper. To reduce the likelihood of programming errors, all such results were independently checked by at least two of the authors.

2. NOTATION AND TERMINOLOGY

The *cycle structure* of a permutation $\sigma \in \mathcal{S}_n$ is the partition of n determined by the lengths of the cycles of σ. We denote a partition of n by listing its parts in decreasing order, with exponents denoting multiplicities. Hence $6^2 3^1 1^3$ is a partition of 18 with two parts of size 6, one part of size 3 and three parts of size 1.

For any partition π of an integer n, we define $\psi(\pi, k)$ to be the sum of the parts of π that are divisible by k. For a permutation $\sigma \in \mathcal{S}_n$ with cycle structure π we define $\psi(\sigma, k) = \psi(\pi, k)$.

Suppose $\theta = (\alpha, \beta, \gamma) \in \mathcal{S}_n \times \mathcal{S}_n \times \mathcal{S}_n$. The *cycle structure* of θ is the multiset containing three elements, namely the cycle structures of α, β, and γ. The cycle structure of θ entirely determines whether or not θ is realized as the autotopism of some quasigroup [14].

Paratopisms, that is, elements of $\mathcal{S}_n \wr \mathcal{S}_3$, will be written in the form $(\alpha, \beta, \gamma; \delta)$, where $\alpha, \beta, \gamma \in \mathcal{S}_n$, and $\delta \in \mathcal{S}_3$. This paratopism acts on quasigroups by sending the triple (i, j, k) to $(\alpha(i), \beta(j), \gamma(k))^{\delta}$, where δ acts on the triple by permuting its three coordinates.

We will borrow the idea of *block diagrams* from [14]. Suppose Q is a quasigroup with an automorphism $\alpha \in \mathcal{S}_n$ that has r cycles, $\alpha_1, \alpha_2, \ldots, \alpha_r$ of respective lengths $c_1, c_2, \ldots, c_r$. A block diagram for Q (with respect to α) is an $r \times r$ matrix B where the cell $B(i, j)$ specifies the composition of the submatrix Q_{ij} of the Cayley table of Q defined by the rows in the orbit of α_i and the columns in the orbit of α_j. We write $\alpha_k : f_k$ in a block $B(i, j)$ if every symbol in α_k appears in Q_{ij} precisely $f_k = f_k(i, j)$ times. If $f_k(i, j) = 0$, we usually omit $\alpha_k : f_k$ from $B(i, j)$. The result is the *block diagram* of Q according to the cycles of α. Figure 1 and Figure 2 show two block diagrams whose relevance to the paper will be explained in Section 4.

	α_1	α_2	α_3	α_4	α_5	α_6
α_1	$\alpha_1 : 2379$ $\alpha_6 : 2380$	$\alpha_3 : 1545$ $\alpha_4 : 1456$ $\alpha_5 : 1326$	$\alpha_2 : 1188$ $\alpha_4 : 847$ $\alpha_5 : 986$	$\alpha_2 : 820$ $\alpha_3 : 655$ $\alpha_5 : 68$	$\alpha_2 : 372$ $\alpha_3 : 180$ $\alpha_4 : 77$	$\alpha_1 : 1$
α_2	$\alpha_3 : 1565$ $\alpha_4 : 1281$ $\alpha_5 : 1683$	$\alpha_2 : 1784$ $\alpha_6 : 1785$	$\alpha_1 : 840$ $\alpha_4 : 497$ $\alpha_5 : 102$	$\alpha_1 : 633$ $\alpha_3 : 220$	$\alpha_1 : 312$ $\alpha_4 : 7$	$\alpha_2 : 1$
α_3	$\alpha_2 : 1204$ $\alpha_4 : 1029$ $\alpha_5 : 476$	$\alpha_1 : 1044$ $\alpha_4 : 63$	$\alpha_3 : 1427$ $\alpha_6 : 1428$	$\alpha_1 : 312$ $\alpha_2 : 176$ $\alpha_5 : 952$	$\alpha_1 : 72$ $\alpha_2 : 48$ $\alpha_4 : 336$	$\alpha_3 : 1$
α_4	$\alpha_2 : 860$ $\alpha_3 : 560$ $\alpha_5 : 221$	$\alpha_1 : 552$ $\alpha_3 : 220$ $\alpha_5 : 459$	$\alpha_1 : 432$ $\alpha_2 : 160$ $\alpha_5 : 340$	$\alpha_4 : 1019$ $\alpha_6 : 1020$	$\alpha_1 : 36$ $\alpha_3 : 240$	$\alpha_4 : 1$
α_5	$\alpha_2 : 316$ $\alpha_3 : 255$ $\alpha_4 : 70$	$\alpha_1 : 189$ $\alpha_3 : 20$ $\alpha_4 : 266$	$\alpha_1 : 156$ $\alpha_2 : 80$ $\alpha_4 : 84$	$\alpha_1 : 75$ $\alpha_2 : 24$ $\alpha_3 : 145$	$\alpha_5 : 419$ $\alpha_6 : 420$	$\alpha_5 : 1$
α_6	$\alpha_1 : 1$	$\alpha_2 : 1$	$\alpha_3 : 1$	$\alpha_4 : 1$	$\alpha_5 : 1$	$\alpha_6 : 1$

FIGURE 1. Block diagram for Q_{7034}.

	α_1	α_2	α_3	α_4	α_5
α_1	$\alpha_1 : 9009$	$\alpha_3 : 6318$ $\alpha_4 : 6435$	$\alpha_2 : 4361$ $\alpha_5 : 4914$	$\alpha_2 : 3528$ $\alpha_5 : 4095$	$\alpha_2 : 1120$ $\alpha_3 : 2691$ $\alpha_4 : 2574$
α_2	$\alpha_3 : 5121$ $\alpha_4 : 2453$ $\alpha_5 : 6435$	$\alpha_2 : 6435$	$\alpha_1 : 2170$ $\alpha_4 : 3091$	$\alpha_1 : 2195$ $\alpha_3 : 1314$	$\alpha_1 : 2070$ $\alpha_4 : 891$
α_3	$\alpha_2 : 3738$ $\alpha_4 : 5005$ $\alpha_5 : 156$	$\alpha_1 : 1710$ $\alpha_5 : 4849$	$\alpha_3 : 5005$	$\alpha_1 : 1900$ $\alpha_2 : 525$	$\alpha_1 : 1395$ $\alpha_2 : 742$
α_4	$\alpha_2 : 1848$ $\alpha_3 : 3321$ $\alpha_5 : 2418$	$\alpha_1 : 2315$ $\alpha_5 : 1586$	$\alpha_1 : 1780$ $\alpha_2 : 644$ $\alpha_5 : 91$	$\alpha_4 : 4095$	$\alpha_2 : 1603$ $\alpha_3 : 774$
α_5	$\alpha_2 : 3423$ $\alpha_3 : 567$ $\alpha_4 : 1551$	$\alpha_1 : 2410$ $\alpha_3 : 117$	$\alpha_1 : 1055$ $\alpha_4 : 1914$	$\alpha_2 : 42$ $\alpha_3 : 2781$	$\alpha_5 : 3465$

FIGURE 2. Block diagram for Q_{28009}.

When constructing a block diagram, it is helpful to keep in mind that in every block $B(i, j)$ we must have

$$\sum_{1\leqslant k\leqslant r} c_k f_k(i, j) = c_i c_j, \tag{1}$$

in order to have the correct number of entries in Q_{ij}. In addition, each symbol must occur exactly once in each row and column, which implies that

$$\sum_{1\leqslant j\leqslant r} f_k(i, j) = c_i \tag{2}$$

for $1 \leqslant i, k \leqslant r$ and

$$\sum_{1\leqslant i\leqslant r} f_k(i, j) = c_j \tag{3}$$

for $1 \leqslant j, k \leqslant r$. An important tool when considering block diagrams is the following result from [14].

Lemma 1. *Let $\theta = (\alpha, \beta, \gamma)$ be an autotopism of some quasigroup $(Q, \star)$. If i belongs to an a-cycle of α and j belongs to a b-cycle of β, then $i \star j$ belongs to a c-cycle of γ, for some c such that* $\mathrm{lcm}(a, b) = \mathrm{lcm}(b, c) = \mathrm{lcm}(a, c) = \mathrm{lcm}(a, b, c)$.

It is immediate from this result that

$$f_k(i, j) = 0 \text{ unless } \mathrm{lcm}(c_i, c_j) = \mathrm{lcm}(c_i, c_k) = \mathrm{lcm}(c_j, c_k). \tag{4}$$

Another consequence of Lemma 1 is:

Lemma 2. *Suppose* $\{\pi_1, \pi_2, \pi_3\}$ *is the cycle structure of an autotopism of some quasigroup. For each part of size* a *in* π_1*, the number of parts of size* b *in* π_2 *cannot exceed* $\frac{1}{b}\sum c$ *where the sum is over all parts* c *of* π_3 *that satisfy* $\mathrm{lcm}(b, c) = \mathrm{lcm}(b, a) = \mathrm{lcm}(c, a)$.

More generally, let a *be a part of* π_1*,* B *be a set of parts of* π_2*, and* C *the set of all parts* c *of* π_3 *such that* $\mathrm{lcm}(b, c) = \mathrm{lcm}(b, a) = \mathrm{lcm}(c, a)$ *for some* $b \in B$*. Then*

$$\sum_{b \in B} b \leqslant \sum_{c \in C} c. \tag{5}$$

Proof. Let (α, β, γ) be the autotopism in question. Let r be one row in an orbit of α of size a. Let X be the columns in orbits of β of size b. For there to be enough distinct symbols available to fill the columns X in row r, we must have $|X| \leqslant \sum c$, where the sum is over all parts c of π_3 that satisfy $\mathrm{lcm}(b, c) = \mathrm{lcm}(b, a) = \mathrm{lcm}(c, a)$. The first claim follows.

Applying the same logic, if we choose any set B of parts of π_2 and consider which symbols are available to fill the corresponding columns in row r, then we derive (5). □

3. SYMMETRIES HAVE SMALL ORDER

Our aim for this section is to find polynomial bounds on the order of automorphisms, autotopisms, and autoparatopisms of quasigroups. As a corollary, we will prove Conjecture 1.

We begin with a theorem of McKay et al. [9]. An autotopism is *trivial* if all three of its components are the identity permutation, and *nontrivial* otherwise.

Theorem 1. *Let* Q *be a quasigroup of order* n *and let* (α, β, γ) *be a nontrivial autotopism of* Q*. Then one of the following holds:*

(a) α*,* β*, and* γ *have the same cycle structure with at least* 1 *and at most* $\lfloor \frac{1}{2}n \rfloor$ *fixed points,*
(b) one of α*,* β*, or* γ *has at least* 1 *fixed point and the other two permutations have the same cycle structure with no fixed points,*
(c) α*,* β*, and* γ *have no fixed points.*

An interesting parallel to Lemma 1 is obtained by considering the order of the three components of an autotopism. We use $\mathrm{ord}(\sigma)$ to denote the order of a permutation σ, that is, the least positive integer k such that σ^k is the identity.

Lemma 3. *Let* $\theta = (\alpha, \beta, \gamma)$ *be an autotopism of some quasigroup* $(Q, \star)$*. Let* $a = \mathrm{ord}(\alpha)$*,* $b = \mathrm{ord}(\beta)$ *and* $c = \mathrm{ord}(\gamma)$*. Then* $\mathrm{lcm}(a, b) = \mathrm{lcm}(b, c) = \mathrm{lcm}(a, c) = \mathrm{lcm}(a, b, c)$.

Proof. As $\theta^{\mathrm{lcm}(a,b)}$ has two trivial components, it must be the trivial autotopism, by Theorem 1. Thus c divides $\mathrm{lcm}(a, b)$. The result follows by symmetry. □

From Theorem 1, we can also infer some other useful consequences.

Lemma 4. *Suppose Q is a quasigroup of order n and that $\alpha \in \operatorname{aut}(Q)$. If α has a cycle of length c, and there are more than $n/2$ points in cycles of α whose length divides c, then* $\operatorname{ord}(\alpha) = c$.

Proof. Clearly $\operatorname{ord}(\alpha) \geqslant c$. However, $\alpha^c \in \operatorname{aut}(Q)$ has more than $n/2$ fixed points, so by Theorem 1 it must be the identity. Therefore $\operatorname{ord}(\alpha) = c$. □

We note in particular that the hypotheses of Lemma 4 are satisfied if α has any cycle of length more than $n/2$.

Lemma 5. *Suppose Q is a quasigroup of order n and that $\theta = (\alpha, \beta, \gamma)$ is an autotopism of Q. If k is any prime power divisor of* $\operatorname{ord}(\theta)$ *then one of the following holds*

$$\begin{aligned} &\psi(\alpha, k) = \psi(\beta, k) = \psi(\gamma, k) \geqslant \frac{1}{2}n, \qquad (6)\\ &\psi(\alpha, k) = \psi(\beta, k) = n,\\ &\psi(\alpha, k) = \psi(\gamma, k) = n,\\ &\psi(\beta, k) = \psi(\gamma, k) = n. \end{aligned}$$

Proof. Let $\operatorname{ord}(\theta) = q^a\ell$ for some prime q and positive integers a and ℓ, with ℓ not divisible by q. Suppose that $k = q^b$, where $1 \leqslant b \leqslant a$. Let $m = q^{b-1}\ell$. Note that every cycle length in α^m, β^m, or γ^m is a power of q.

Suppose that two of α^m, β^m, and γ^m have fixed points. Applying Theorem 1 to θ^m tells us that α^m and β^m have the same cycle structure with at most $n/2$ fixed points. Hence

$$\psi(\alpha, q^b) = \psi(\alpha^m, q) = \psi(\beta^m, q) = \psi(\beta, q^b).$$

By symmetry $\psi(\alpha, q^b) = \psi(\gamma, q^b)$. Now (6) follows by observing that $\psi(\alpha^m, q)$ is the number of points not fixed by α^m.

It remains to consider the case when at least two of α^m, β^m , and γ^m do not have fixed points. However, if α^m has no fixed points then $\psi(\alpha, q^b) = \psi(\alpha^m, q) = n$. Similar statements for β^m and γ^m imply the claimed result. □

The condition (6) holds whenever θ is an automorphism. However, there are plenty of autotopisms listed in [14] for which it fails. For example, there is a quasigroup of order 12 with an autotopism with cycle structure $\{4^3, 6^1 3^2, 12^1\}$. This autotopism fails the equalities in (6) for $k \in \{2, 3, 4\}$. The inequality in (6) fails, for example, for $k \in \{2, 3\}$ in an autotopism with cycle structure $\{12^1, 12^1, 3^1 2^1 1^7\}$.

We are now in a position to prove our bounds.

Theorem 2. *Suppose Q is a quasigroup of order $n \geqslant 4$. Then* $\operatorname{ord}(\theta) \leqslant n^2/4$ *for all* $\theta \in \operatorname{atp}(Q)$ *and* $\operatorname{ord}(\phi) \leqslant 3n^2/4$ *for all* $\phi \in \operatorname{par}(Q)$.

Proof. Suppose $\theta = (\alpha, \beta, \gamma) \in \operatorname{atp}(Q)$. First consider the case when α has a cycle of some length $c > n/2$. Let d be the largest prime power divisor of c. By examining the catalog in [14] of autotopisms for $n \leqslant 17$ we can eliminate small orders. In particular, we may assume that $n \geqslant 12$ and hence $d \geqslant 4$. By Lemma 5 there must be a cycle of β or γ that has length divisible by d. If e is the length of the smallest cycle in β^c or γ^c, then $e \leqslant n/d \leqslant n/4$. There are more than $n/2$ fixed points in α^{ce} and at least e fixed points in β^{ce} or γ^{ce}. By Theorem 1, we see that θ^{ce} must be trivial, so $\operatorname{ord}(\theta) \leqslant ce \leqslant n^2/4$.

From now on we may assume that α has no cycle of length more than $n/2$. By symmetry, we may also assume that β and γ have the same property.

For each $i \in [n]$ and $\pi \in \mathcal{S}_n$, let $\ell_i(\pi)$ be the length of the cycle of π that includes i. Define $P = \prod_{i=1}^{n} \ell_i(\alpha)\ell_i(\beta)\ell_i(\gamma)$ and note that $P \leqslant (n/2)^{3n}$. By Lemma 5, we have $\psi(\alpha, k) + \psi(\beta, k) + \psi(\gamma, k) \geqslant 3n/2$ for every prime power divisor k of $\mathrm{ord}(\theta)$. It follows that $\mathrm{ord}(\theta)^{3n/2}$ divides P and hence $\mathrm{ord}(\theta) \leqslant (n/2)^2$ as claimed.

Finally, suppose that $\phi = (\alpha, \beta, \gamma; \delta) \in \mathrm{par}(Q)$. Then $\delta \in \mathcal{S}_3$ has order 1, 2, or 3, so either $\phi^2 \in \mathrm{atp}(Q)$ or $\phi^3 \in \mathrm{atp}(Q)$. Applying the above bound for the order of autotopisms now yields the claimed bound for the order of autoparatopisms. □

Corollary 1. *Suppose ρ is chosen uniformly at random from $\mathcal{S}_n$. Then with probability approaching* 1 *as $n \to \infty$, all the following statements hold:*

1. *ρ is not an automorphism of any quasigroup of order n,*
2. *ρ is not an automorphism of any Steiner triple system of order n,*
3. *ρ is not an automorphism of any* 1*-factorization of K_n,*
4. *there do not exist $\sigma, \tau \in \mathcal{S}_n$ such that (ρ, σ, τ) is an autotopism of any quasigroup of order n.*

Proof. Much work has been done on the order of random permutations (see, e.g. [15]). It is known from [4] that the order of ρ will, with probability approaching 1, exceed $n^{(1/2+o(1))\log n}$. In particular the order of a random permutation in $\mathcal{S}_n$ is not bounded by any polynomial in n. Hence Claim 4 of the corollary follows from Theorem 2. The first three claims are special cases of Claim 4. □

In particular, Corollary 1 proves Conjecture 1. On hearing Theorem 2, but without seeing the proof, a slightly weaker (but still quadratic) bound was found by Babai (see [1]).

4. AN AUTOMORPHISM OF ORDER EXCEEDING *n*

Although Theorem 2 gives a quadratic bound on the order of a quasigroup automorphism, it is natural to wonder whether this bound is of the right order. At this time, we are unable to answer that question, however, we will shed some light on it in this section.

Recall that Horoševskiĭ [6] proved that, if G is a group of order $n > 1$ then any automorphism of G has order at most $n - 1$. Problem 1 was motivated by the observation that for all small orders n, the largest order of a quasigroup autotopism is exactly n. It is not hard to prove the following existence result (see, e.g. [14], Thms 3.4 and 5.2]).

Lemma 6. *For each odd n it is possible to find a quasigroup of order n with an automorphism of order n. For each even n we can find a quasigroup of order n with an automorphism of order $n - 1$, and another quasigroup of order n with an autotopism of order n.*

Given the above context, it is of considerable interest to know whether a quasigroup of order n can ever have an automorphism of order greater than n. We answer this now.

Theorem 3. *For $n \leqslant 7033$ there is no quasigroup of order n possessing an automorphism of order more than n. However, there is a quasigroup of order* 7034 *having an automorphism of order* 7140.

Proof. Suppose there is a quasigroup of some order $n \leqslant 7033$ possessing an automorphism of order more than n. Among all such quasigroups let Q be one of smallest order, and let n be that order. Among all automorphisms of Q, suppose α has the smallest order that still exceeds n. Let m be the order of α. Suppose π is the partition of n determined by the cycle structure of α. We note the following immediate consequences of our choices.

1. m is the lowest common multiple of the parts of π.
2. m is not divisible by any prime p for which $m > pn$, since otherwise α^p would be an automorphism of Q of order $m/p > n$, contradicting the choice of α.
3. By Lemma 4, there is no part c of π for which the sum of the parts of π that divide c exceeds $n/2$ (in particular, no single part of π exceeds $n/2$).
4. $\psi(\pi, k) \geqslant n/2$ for any prime power k that divides m, by Lemma 5.
5. For any parts a, b of π there exists a part c satisfying $\mathrm{lcm}(a, b) = \mathrm{lcm}(b, c) = \mathrm{lcm}(a, c)$. Indeed, for each part a of π, (5) holds for all sets B of parts of π.
6. m is divisible by at least three distinct primes. If $m = p^k$ where p is prime, then π has a part of size p^k and so $m \leqslant n$. Suppose instead that $m = p^k q^\ell$ for distinct primes p, q and $k, \ell > 0$. If $m > n$ then π has no part divisible by $p^k q^\ell$, so $\psi(\pi, p^k) = \psi(\pi, q^\ell) = n/2$ since they count disjoint sets of parts. But this implies $n/2$ is a multiple of both p^k and q^ℓ and so $n \geqslant 2m$.
7. A corollary of conditions 2 and 6 above is that $m < n^{3/2}$.

Our aim was to try each plausible value of m and show that it cannot be realized by any $n \leqslant 7033$ and π. For each $m < 7033^{3/2}$ with at least three distinct prime factors we did the following. First we found the prime factorization of $m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ where $p_1 < p_2 < \cdots < p_r$ are primes. We treated m as a constant and n as a variable. For each divisor d of m we allocated a variable v_d that counts the number of cycles of length d. The constraints 1 to 7 above can then be encoded as the following integer linear program.

$$\begin{aligned} 0 \leqslant v_d &\leqslant n/(2d) && \text{for all } d \text{ by 3,} \\ \lceil m^{2/3} \rceil \leqslant n = \sum_d d v_d &\leqslant m - 1 && \text{by 7,} \\ m/p_1 \leqslant n &\leqslant 7033 && \text{by 2,} \\ \sum_{d \text{ a multiple of } p_i^{a_i}} d v_d &\geqslant n/2 && \text{for } \quad 1 \leqslant i \leqslant r, \text{ by 1 and 4.} \end{aligned} \tag{7}$$

If $v_d > 0$ for some d, extra constraints can be applied:

$$\begin{aligned} &\sum_{a|d} a v_a \leqslant n/2 && \text{by 3,} \\ &\sum_{b \in B} b v_b \leqslant \sum_{c \in C(d,B)} c v_c && \text{for all sets } B \text{ of divisors of } m \text{, by 5,} \end{aligned} \tag{8}$$

where $C(d, B)$ is the set of all block sizes c of π such that $\mathrm{lcm}(d, b) = \mathrm{lcm}(d, c) = \mathrm{lcm}(b, c)$ for some $b \in B$.

Next, we explain two independent computations that showed that there are no m, n, π satisfying the above inequalities and also satisfying the block constraints (1)–(4), except for the case

$$n = 7033, \quad m = 7144, \quad \pi = 2380^1\, 1785^1\, 1428^1\, 1020^1\, 420^1. \tag{9}$$

One of the computations used the constraint-satisfaction program MINION [5]. Since the number of solutions without the block constraints is very large, and they often differ only in the number of fixed points, we instead sought solutions for m, n', π', where $n' = n - v_1$ is the number of points not fixed, and π' is the same as π except that the singletons are removed. Considering the justifications for the various constraints above, we find that they apply also to m, n', π' except that $\lceil m^{2/3} \rceil \leqslant n$ must be replaced by $\lceil m^{2/3} \rceil \leqslant 2n'$ and $m/p_1 \leqslant n$ must be replaced by $m/p_1 \leqslant 2n'$. These are justified since $n' \geqslant n/2$. The validity of inequality (8) is less obvious but comes from the block constraints, as we now show.

For each triple a, b, c of part sizes of π, define

$$g_c(a, b) = c \sum_{i:c_i=a} \sum_{j:c_j=b} \sum_{k:c_k=c} f_k(i, j).$$

It follows from (1)–(3) that these nonnegative integers satisfy

$$\sum_d g_d(a, b) = av_a\, bv_b, \qquad \sum_d g_c(d, b) = bv_b\, cv_c, \qquad \sum_d g_c(a, d) = av_a\, cv_c, \tag{10}$$

for all a, b, c. Also, it follows from (4) that $g_c(a, b) = 0$ unless $\operatorname{lcm}(a, b) = \operatorname{lcm}(a, c) = \operatorname{lcm}(b, c)$. Applying the three parts of (10) for $a = 1$, $b = 1$, and $c = 1$, respectively, we find that $g_d(1, d) = g_d(d, 1) = g_1(d, d) = v_1 d v_d$ for all d. Therefore, if we define $g'_c(a, b) = g_c(c, c) + v_1 c v_c$ when $a = b = c$ and $g'_c(a, b) = g_c(a, b)$ otherwise, we find that (10) holds for π' with g replaced by g'.

For a being a block size of π' and B being a set of block sizes of π', we have

$$\sum_{b\in B} av_a\, bv_b = \sum_{b\in B}\ \sum_{c\in C(a,B)} g'_c(a, b) = \sum_{c\in C(a,B)}\ \sum_{b\in B} g'_c(a, b) \leqslant \sum_{c\in C(a,B)} av_a\, cv_c,$$

where the first and third steps come from the first and third equations of (10). If $v_a > 0$, this implies $\sum_{b\in B} bv_b \leqslant \sum_{c\in C(a,B)} cv_c$. In practice there are too many choices for B to use all such inequalities, so we used all those for which $C(a, B) = C(a, \{b\})$ for some $b \in B$.

MINION took about 30 minutes to find about 12 million solutions to these constraints apart from (10). The smallest was $n = 389$, $m = 420$, $\pi' = 140^1\, 105^1\, 84^1\, 60^1$. For each solution, Gaussian elimination was used to test if (10) was satisfiable modulo a large prime (a necessary condition if (10) has a solution over the integers). Only the solution (9) remained.

The same result was obtained by an independent and lengthier computation using Maple. This computation only used the constraints described prior to and including (7), together with the $|B| = 1$ case of (8). These constraints were subject to a backtrack search that made iterative use of Maple's exact simplex algorithm to bound the variables. The search branched by allocating values to the variables v_i in decreasing order of i, although we did not allocate values to v_3, v_2, or v_1. Rather, when v_i for $i > 3$ was known, we found it was sufficient to apply the block constraint (1) for distinct $c_i, c_j > 3$, (2) for distinct $c_i, c_k > 3$, (3) for distinct $c_j, c_k > 3$, and (4). These block constraints were found to be inconsistent over the rationals in all cases except (9).

The infeasibility of (9) is shown by Lemma 6.3(ii) in [14]. However, there is an easy patch. By adding one fixed point, we get a cycle structure that is achievable. To be precise, we found a quasigroup Q_{7034} that has an automorphism α with cycle structure $2380^1 1785^1 1428^1 1020^1 420^1 1^1$. The order of α is $m = 7140 > n = 7034$, so its existence completes the proof of the theorem. A block diagram for the Cayley table L of Q_{7034} is given in Figure 1. We assume that the last row and column of L are in natural order. Then, to specify Q_{7034} it suffices to give 5 rows from L, one from each orbit of α on the rows other than the last row. Five such rows can be downloaded from [17]. □

The example just described is not the only instance that we found of a quasigroup of order n with an automorphism of order $m > n$. Another example, Q_{28009}, has $n = 28009 < 45045 = m$. The cycle structure of the automorphism α is $9009^1 6435^1 5005^1 4095^1 3465^1$. A block diagram for Q_{28009} is given in Figure 2. To specify Q_{28009} it suffices to give 5 rows from its Cayley table, one from each orbit of α on the rows. Five such rows can be downloaded from [17].

The idea that led us to Q_{28009} is the following. Suppose that we have a set X of s relatively prime positive integers of comparable size. We aim to choose cycle lengths that are products of elements of X, and then to build Q with an automorphism with these cycle lengths. Each cycle length c is associated with the subset of X consisting of the factors of c. The cycle structure of the automorphism therefore corresponds to a system $\mathcal{Z}$ of subsets of X. To avoid redundancy, we assume that every element of X is in at least one set in $\mathcal{Z}$. We then know that m, the order of the automorphism, will be the product of all elements of X. The order n of the quasigroup Q will be minimized by keeping $\mathcal{Z}$ and the sets in $\mathcal{Z}$ small. However, the sets must be compatible with Lemma 1. Hence for each $A, B \in \mathcal{Z}$ there must be $C \in \mathcal{Z}$ such that

$$A \cup B = A \cup C = B \cup C. \tag{11}$$

We now discuss set systems that satisfy this property.

Suppose we take $\mathcal{Z}$ to be all subsets of X of size t. Roughly, this gives $n \approx \binom{s}{t} m^{t/s}$. Choosing $X = \{5, 7, 9, 11, 13\}$ and $t = 4$ provided us with Q_{28009}. A necessary condition for this construction to work is that $t \geqslant 2s/3$. However, we now present an example showing that it is possible to achieve (11) using sets that are smaller relative to the ground set.

Take X to be the nonzero binary vectors of length k. Take $\mathcal{Z}$ to consist of one set S_Y for every nonempty subset Y of $\{1, \ldots, k\}$. We define S_Y to be the set of vectors whose coordinates in the positions indexed by Y add up to 1 mod 2. If A and B are two distinct subsets of $\{1, \ldots, k\}$ then their symmetric difference C satisfies (11), because the symmetric difference of S_A and S_B is S_C. The cardinality of X in this example is $2^k - 1$. The cardinality of each S_Y is 2^{k-1}, which is only very marginally more than half the size of the ground set. This is best possible in the following sense:

Lemma 7. *Let $\mathcal{Z}$ be a system of subsets of a ground set X such that each of the s elements of X occurs in at least one set in $\mathcal{Z}$. If* (11) *holds then $\mathcal{Z}$ contains at least one set of cardinality greater than $s/2$.*

Proof. The claim is trivial for $s = 1$. Aiming for a contradiction, suppose $s > 1$ is the smallest integer for which there exists $\mathcal{Z}$ satisfying (11) but where all sets in $\mathcal{Z}$ have cardinality at most $s/2$. Let $L \in \mathcal{Z}$ be a largest set in $\mathcal{Z}$. By assumption $1 \leqslant |L| \leqslant s/2$. Now construct a new set system by taking $X' = X \setminus L$ and $\mathcal{Z}' = \{B \setminus L : B \in \mathcal{Z}\}$. We will argue that $\mathcal{Z}'$ contradicts the minimality of $\mathcal{Z}$.

First note that $|X'| = s - |L| \geqslant s/2$. For each $B \in \mathcal{Z}$, there exists $C \in \mathcal{Z}$ such that $B \cup C = B \cup L = C \cup L$. It follows that $|L| \geqslant |C| \geqslant |B \setminus L| + |L \setminus B| = |B \setminus L| + |L| - |B \cap L|$ and hence $|B \setminus L| \leqslant |B \cap L|$. Thus $|B \setminus L| \leqslant |B|/2 \leqslant s/4 \leqslant |X'|/2$. So each set in $\mathcal{Z}'$ has cardinality no more than half $|X'|$.

Secondly, take any $B_1, B_2 \in \mathcal{Z}$ and let $B_1' = B_1 \setminus L$ and $B_2' = B_2 \setminus L$. By the choice of $\mathcal{Z}$ there exists $B_3 \in \mathcal{Z}$ satisfying $B_1 \cup B_2 = B_1 \cup B_3 = B_2 \cup B_3$. It is immediate that $B_3' = B_3 \setminus L \in \mathcal{Z}'$ satisfies $B_1' \cup B_2' = B_1' \cup B_3' = B_2' \cup B_3'$, so $\mathcal{Z}'$ satisfies (11) as claimed. □

In practice, for each A and B there should be several choices of C that satisfy (11) in order to provide enough flexibility to satisfy Lemma 2 and the block diagram constraints. We conjecture that this is possible without making the largest set much larger than half the size of the groundset.

Conjecture 2. *Let μ be a fixed positive integer. There exists an infinite family of set systems parametrized by s, the size of the ground set, in which no set has cardinality exceeding $s/2 + o(s)$ and which has the property that for each choice of sets A and B there are at least μ different choices of C that satisfy* (11).

With such a family of set systems, say for $\mu = 3$, it would be possible to choose plausible cycle structures for automorphisms whose order grows quadratically in the order of the quasigroups. We simply take s coprime integers of large, comparable size, and use the set system to determine how to multiply them to produce the cycle lengths of the automorphism. Our empirical experience with small examples leads us to suspect that such automorphisms would exist, but constructing the quasigroups is not a simple task with present methods.

We announced Conjecture 2 at the 2012 meeting of the Australian Mathematical Society, and were shortly afterwards sent a proof by Gyula Károlyi [8]. Thus we are emboldened to conjecture that Theorem 2 is sharp in this sense:

Conjecture 3. *Let $\varepsilon > 0$. There is no $O(n^{2-\varepsilon})$ bound on the order of automorphisms of quasigroups of order n.*

Although we have not resolved the question with which we opened this section, we have at least shown that the answer to Problem 1 is negative for general n. We have two examples where the order of the automorphism exceeds the order of the quasigroup. An infinite family of such examples can now be found by taking direct products. If quasigroups Q_1 and Q_2 have automorphisms of respective orders m_1 and m_2, where m_1 and m_2 are relatively prime, then $Q_1 \times Q_2$ has an automorphism of order $m_1 m_2$ (see e.g. [14, Lem 3.2]). Choosing Q_1 to be either Q_{7034} or Q_{28009} and using Lemma 6 to provide Q_2, we get infinitely many examples of quasigroups possessing an automorphism whose order exceeds the order of the quasigroup. Examples for some other orders can then be obtained by prolongations (see, e.g. [3]). Although we have not attempted a proof, we suspect that for all large enough n there is a quasigroup of order n with an automorphism of order more than n.

5. QUASIGROUPS OF PRIME ORDER

In this last section, we answer Problem 2 by giving examples that show that other possibilities are attained. However, first we give at least a partial explanation of why, for small primes, only the two possibilities listed in Problem 2 occur.

Suppose Q is a quasigroup of order n and that θ is an autotopism of Q. Suppose further that k is a prime power divisor of ord(θ) and k does not divide n. Examining Lemma 5, we see that the only possibility is that (6) holds. In practice, this is quite a strong restriction, especially for quasigroups of prime order (since in that case the condition that k does not divide n only rules out $k = n$). Indeed, we have the following result, in the spirit of Problem 2.

Lemma 8. *Let $\theta = (\alpha, \beta, \gamma)$ be an autotopism of a quasigroup of prime order p. Then either*

1. *one of α, β or γ is the identity and the other two are p-cycles; or*
2. *$\psi(\alpha, k) = \psi(\beta, k) = \psi(\gamma, k)$ for every prime power k and hence α, β, γ have the same order as permutations.*

Proof. First suppose that one of α, β, γ is a p-cycle. By Lemma 5 at least two of α, β, γ must be p-cycles. Hence θ^p must be trivial, by Theorem 1. Consequently, we are either in the first case of the lemma, or else each of α, β, γ is a p-cycle, which falls within the second case.

Hence we may assume that none of α, β, γ is a p-cycle. Let k be any prime power dividing ord(θ). Since k does not divide p, we know that $\psi(\alpha, k)$, $\psi(\beta, k)$, and $\psi(\gamma, k)$ are all strictly less than p. So Lemma 5 implies that (6) holds. For any prime power k that does not divide ord(θ), we have $\psi(\alpha, k) = \psi(\beta, k) = \psi(\gamma, k) = 0$. The lemma follows. □

With Lemma 8 in mind, we undertook a computer search of all partitions of primes $p \leqslant 29$ to find possible cycle structures for θ. Aside from the options listed in Problem 2, the only 3 possibilities that satisfy (6) are that

- $p = 23$ and one of α, β, γ has cycle structure $6^2 3^1 2^1 1^6$ while the other two have cycle structure $6^1 3^3 2^4$.
- $p = 29$ and one of α, β, γ has cycle structure $6^2 3^1 2^4 1^6$ while the other two have cycle structure $6^1 3^3 2^7$.
- $p = 29$ and one of α, β, γ has cycle structure $6^3 3^1 2^1 1^6$ while the other two have cycle structure $6^2 3^3 2^4$.

Of these options, the first two can be seen to be infeasible using [14, Lemma 3.8]. In contrast, we now show that the last option is achieved, providing the smallest witness that the answer to Problem 2 is negative. Take

$$\begin{aligned}\alpha = \beta = {} & (1, 2, 3, 4, 5, 6)(7, 8, 9, 10, 11, 12)(13, 14, 15)(16, 17, 18)(19, 20, 21)\\ & (22, 23)(24, 25)(26, 27)(28, 29)\\ \gamma = {} & (1, 2, 3, 4, 5, 6)(7, 8, 9, 10, 11, 12)(13, 14, 15, 16, 17, 18)(19, 20, 21)(22, 23)\end{aligned}$$

and use the following for the rows indexed 1, 7, 13, 16, 19, 22, 24, 26, 28, respectively:

$$\begin{array}{l}
[24, 25, 19, 12, 13, 26, 23, 27, 28, 6, 7, 29, 22, 1, 18, 3, 15, 9, 14, 2, 8, 5, 21, 4, 20, 11, 17, 16, 10] \\
[27, 28, 29, 17, 6, 7, 24, 25, 19, 26, 18, 1, 2, 8, 14, 22, 10, 15, 23, 11, 5, 9, 3, 16, 4, 13, 21, 12, 20] \\
[22, 6, 7, 23, 3, 10, 17, 12, 1, 14, 9, 4, 19, 21, 20, 24, 25, 26, 27, 28, 29, 15, 18, 11, 8, 2, 5, 13, 16] \\
[10, 4, 13, 7, 1, 16, 22, 11, 6, 23, 8, 3, 27, 28, 29, 19, 21, 20, 24, 25, 26, 18, 15, 17, 14, 12, 9, 5, 2] \\
[23, 5, 18, 22, 2, 15, 16, 9, 17, 13, 12, 14, 24, 25, 26, 27, 28, 29, 19, 21, 20, 10, 7, 8, 11, 1, 4, 6, 3] \\
[19, 2, 21, 4, 20, 6, 1, 8, 3, 10, 5, 12, 14, 18, 16, 11, 9, 7, 13, 17, 15, 22, 24, 23, 25, 26, 28, 27, 29] \\
[21, 8, 20, 10, 19, 12, 13, 1, 15, 3, 17, 5, 4, 2, 6, 18, 16, 14, 11, 9, 7, 27, 29, 22, 24, 23, 25, 26, 28] \\
[13, 1, 15, 3, 17, 5, 19, 7, 21, 9, 20, 11, 12, 10, 8, 4, 2, 6, 18, 16, 14, 26, 28, 27, 29, 22, 24, 23, 25] \\
[18, 7, 14, 9, 16, 11, 21, 13, 20, 15, 19, 17, 8, 12, 10, 5, 3, 1, 2, 6, 4, 23, 25, 26, 28, 27, 29, 22, 24]
\end{array}$$

Then use the specified autotopism to complete the Latin square of order 29. The full Latin square, together with another example of order 41, can be downloaded from [17]. This latter example, for which α and β have cycle structure $6^4 3^3 2^4$ while γ has cycle structure $6^5 3^1 2^1 1^6$, is referred to by [10]. Our new example above does not answer Problem 4.2 in [10], since its multiplication group is the symmetric group $\mathcal{S}_{29}$.

Looking back at Theorem 1, there is another type of autotopism which we have not yet witnessed in quasigroups of prime order, namely one for which the three component permutations in the autotopism have pairwise different cycle structures. We call such an autotopism a *triceratopism*. We found an example of a quasigroup of order 131 that has a triceratopism with cycle structures $30^1 15^2 10^3 6^6 5^1$, $30^2 10^3 6^1 5^1 3^{10}$, and $30^2 15^2 6^1 5^1 2^{15}$. The example can be downloaded from [17]. We now explain the process that allowed us to find this example, and to conclude that there are no smaller examples of quasigroups of prime order that possess a triceratopism.

For a prime p and positive integer m to be chosen below, we did the following. Suppose $\theta = (\alpha, \beta, \gamma)$ is a triceratopism of order m for a quasigroup of order p. By Theorem 1, none of α, β, γ have fixed points. We next argue that none of α, β, γ is a p-cycle. Say α is a p-cycle, which means that all cycles in β and γ are of length relatively prime to p. Hence β^p has the same cycle structure as β, and similarly γ^p has the same cycle structure as γ. Now, applying Theorem 1 to θ^p we find that β must have the same cycle structure as γ. This contradiction justifies our first step, which was to identify $\Lambda = \{x : 1 < x < p$ and x divides $m\}$, the set of possible cycle lengths. We then found Ω, the set of all partitions π of the integer p satisfying

- Each part of π is a member of Λ.
- For each prime power q dividing m we have $\psi(\pi, q) \geqslant p/2$.

We then found all sets of three distinct $\pi_1, \pi_2, \pi_3 \in \Omega$ that satisfy (6), assuming the cycle structures of α, β, γ to be π_1, π_2, π_3. For the few thousand candidates that made it this far we had one final test. For all choices of $\{a, b, c\} = \{1, 2, 3\}$ we checked that for each choice of a part from π_a and a part from π_b, the parts of π_c satisfied Lemma 2.

We performed these checks for $p \leqslant 131$ and $m \leqslant p^2/4$, and the only candidate that passed all the checks was the example given above. Hence, on the basis of Theorem 2, we know that it is the smallest. To construct the quasigroup, we first chose a plausible block diagram, then used a simple backtracking algorithm to find a quasigroup with that block diagram.

We close the paper with a few comments on *loops*, that is, quasigroups with an identity element. Since loops are quasigroups, results such as Theorem 2 apply to loops without change. Also, every quasigroup is isotopic to a loop, and isotopisms preserve the cycle structure of autotopisms. This observation allows us to directly translate the results from the present section to loops. For example, the smallest loop with a triceratopism has order 131. Finally, we note that Q_{7034} from Section 4 is a loop, thereby demonstrating that loops can have automorphisms with order greater than the order of the loop. The quasigroup Q_{28009} can also be used to build a loop of order 28010 with a similar property.

ACKNOWLEDGEMENTS

The authors are grateful for interesting discussions with Gyula Károlyi and László Babai about aspects of this paper.

REFERENCES

[1] L. Babai and A. Seress, Element order versus minimal degree in permutation groups: an old lemma with new applications, arXiv:1401.0489v1 [math.CO].

[2] J. Browning, D. S. Stones, and I. M. Wanless, Bounds on the number of autotopisms and subsquares of a Latin square, Combinatorica 33 (2013), 11–22.

[3] D. Bryant, M. Buchanan, and I. M. Wanless, The spectrum for quasigroups with cyclic automorphisms and additional symmetries, Discrete Math 304 (2009), 821–833.

[4] P. Erdős and P. Turán, On some problems of a statistical group theory III, Acta Math Acad Sci Hungar 18 (1967), 309–320.

[5] I. P. Gent, C. Jefferson, and I. Miguel, Minion: a fast, scalable, constraint solver, Proc. 17th European Conference on Artificial Intelligence (ECAI'06), Italy, 2006, 98–102.

[6] M. V. Horoševskiĭ, Automorphisms of finite groups, Math Sb (N.S.) 93 (135) (1974), 576–587.

[7] A. Hulpke, P. Kaski, and P. R. J. Östergård, The number of Latin squares of order 11, Math Comp 80 (2011), 1197–1219.

[8] G. Károlyi, An atypical extremal problem for set systems with a constraint on pairwise unions, manuscript.

[9] B. D. McKay, A. Meynert, and W. Myrvold, Small Latin squares, quasigroups and loops, J Combin Des 15 (2007), 98–119.

[10] J. D. H. Smith, Homotopies of central quasigroups, Comm Algebra 40 (2012), 1878–1885.

[11] D. Stones, On the number of Latin rectangles, Ph.D. Thesis, Monash University, 2009.

[12] D. Stones and I. M. Wanless, Divisors of the number of Latin rectangles, J Combin Theory Ser A 117 (2010), 204–215.

[13] D. Stones and I. M. Wanless, How not to prove the Alon–Tarsi conjecture, Nagoya Math J 205 (2012), 1–24.

[14] D. S. Stones, P. Vojtěchovský, and I. M. Wanless, Cycle structure of autotopisms of quasigroups and Latin squares, J Combin Designs 20 (2012), 227–263.

[15] R. Stong, The average order of a permutation, Electron J Combin 5 (1998), R41.

[16] I. M. Wanless, Diagonally cyclic Latin squares, Eur J Combin 25 (2004), 393–413.

[17] I. M. Wanless, Author's homepage, http://users.monash.edu.au/∼iwanless/data/autotopisms.