CONNECTED QUANDLES WITH ORDER EQUAL TO TWICE AN ODD PRIME

JAMES MCCARRON

Abstract. We show that there is an unique connected quandle of order twice an odd prime number greater than 3. It has order 10 and is isomorphic to the conjugacy class of transpositions in the symmetric group of degree 5. This establishes a conjecture of L. Vendramin.

1. Introduction

Quandles were introduced independently in 1982 by D. Joyce [13] and S. Matveev [16] as invariants of knots. To each knot one associates a (generally) non-associative algebraic system called the knot quandle which turns out to be a very strong algebraic invariant.

The number q_n of isomorphism classes of quandles of order n is known to grow very quickly with n. This was already evident with the computational determination of the number of quandles of small orders [11, 10, 17]. Recently, Blackburn showed that q_n grows like 2^{n^2}, asymptotically [2]. Because the complete set of quandles of even small orders appears to be intractably large there has, in recent years, been considerable interest in counting and constructing quandles of more restricted classes. Connected quandles are of particular importance because knot quandles are connected, and homomorphic images of connected quandles are connected. Therefore, the finite quandles that appear as homomorphic images of knot quandles are necessarily connected, and it is these quandles that figure in computable invariants of knots [7, 14, 4]. Thus, the connected quandles of prime order, and of order equal to the square of a prime, have been determined [6, 9].

Clauwens [5] computed the connected quandles up to order 14 and showed, in particular, that no connected quandles of order 14 exist. L. Vendramin computed the connected quandles to order 35 [21]. This is sequence A181771 [18] in the Online Encyclopaedia of Integer Sequences [20].

Date: May 3, 2014.

From this data, it may be observed that, apart from $n = 2$, the values for which *no* connected quandles appear are the numbers $14 = 2 \cdot 7$, $22 = 2 \cdot 11$, $26 = 2 \cdot 13$ and $34 = 2 \cdot 17$. Each is equal to twice an odd prime number. Moreover, these are all the numbers of the form $2p$, with $p > 5$ and $2p \leq 35$. There is, however, a connected quandle of order $10 = 2 \cdot 5$.

Example 1 (Connected Quandle of Order 10)**.** *The conjugacy class of transpositions in the symmetric group S_5 of degree 5 has length $10 = 2 \cdot 5$. Regarded as a quandle under the operation of conjugation, it is simple and therefore connected.*

These observations suggest our main theorem, which establishes a conjecture of L. Vendramin [22].

Theorem 2. *Let Q be a connected quandle of order $2p$, where $p > 3$ is a prime number. Then Q has order 10 and is isomorphic to the quandle of the conjugacy class of transpositions in the symmetric group of degree 5.*

Our strategy for the proof is as follows. First, we use an important theorem of Clauwens [5] to show that our quandle is simple. The importance of this is that we have quite a lot of information about the structure of the inner automorphism group, thanks to [1]. From this description of the inner automorphism group, we construct a faithful permutation representation of degree $2p$ on a conjugacy class. Now, this action of the inner automorphism group may, or may not, be primitive, and we analyse these two possibilities separately. For the primitive case, we need to know the primitive groups of degree $2p$. We derive a list of primitive groups of degree $2p$ from a result of Liebeck and Saxl. [15] Having determined these, the conclusion follows quite easily. For the imprimitive case, we have to work a bit harder. We construct a different faithful permutation representation of the inner automorphism group of prime degree p. Using this, we are able to conclude that the inner automorphism group is, in fact, doubly transitive with simple socle, and to construct a subgroup of index p in the socle. We then use an observation due to D. Holt on point stabilisers in doubly transitive groups to conclude that this case cannot occur. The conclusion, then, is that there are no imprimitive examples so that the result of the primitive case applies, and we arrive at the apocalyptic conclusion of the theorem.

The remainder of the paper is organised as follows. We gather some relevant background material in Section 2. Then, in Section 3, we prove our main theorem for primitive quandles. Section 4 deals with the case of an imprimitive quandle, and Section 5 contains the proof of Proposition 18 which classifies the primitive groups of degree equal to twice an odd prime.

Acknowledgement. The author thanks Erik Postma and Leandro Vendramin for reading earlier drafts of this paper.

2. Preliminaries

Let us begin by defining the principal objects of study.

Definition 3 (Quandle). *A* ***quandle*** *is a set Q together with a binary operation $\triangleright : Q \times Q \to Q$ which satisfies the following axioms.*

(Q1) *For all a and b in Q, there is a unique x in Q such that $b = x \triangleright a$.*
(Q2) *For all a, b and c in Q, we have $(a \triangleright b) \triangleright c = (a \triangleright c) \triangleright (b \triangleright c)$.*
(Q3) *For all a in Q, we have $a \triangleright a = a$.*

We give several standard examples of quandles.

Example 4 (Conjugation Quandle). *Let G be a group and, for a and b in G, define $a \triangleright b = b^{-1}ab$. Then the system $\langle G, \triangleright \rangle$ is a quandle, called the* ***conjugation quandle*** $\operatorname{Conj} G$ *of G. Moreover, any conjugacy class, or union of conjugacy classes of G forms a quandle with conjugation as the quandle operation.*

The ***order*** of a quandle is the cardinality of its underlying set.

Example 5 (Trivial Quandle). *The* ***trivial quandle*** *on a set Q is defined by the binary operation $\triangleright$ for which $a \triangleright b = b$, for all a and b in Q. This is the only associative quandle operation on a set Q. Any two trivial quandles of the same order are isomorphic, and we denote the trivial quandle of order n by T_n.*

Example 6 (Affine Quandle). *Let A be an Abelian group, and let τ be an automorphism of A. We obtain a quandle structure on the underlying set of A by defining, for a and b in A, $a \triangleright b = \tau a + (1 - \tau)b$. A quandle of this form is called an* ***Alexander quandle*** *(or an* ***affine quandle****).*

Example 7 (Dihedral Quandle). *The* ***dihedral quandle*** *of order n, where n is a positive integer, is defined to be the set $\mathbb{Z}_n$ of integers modulo n, together with the binary operation $\triangleright$ defined by $a \triangleright b = 2b - a \pmod{n}$, for all a and b in $\mathbb{Z}_n$.*

Homomorphisms, automorphisms and subquandles are defined in the natural way. Thus, if Q and R are quandles, then a map $\varphi : Q \to R$ is a quandle ***homomorphism*** if $\varphi(a \triangleright b) = (\varphi a) \triangleright (\varphi b)$ for all a and b

in Q. A homomorphism is an ***isomorphism*** if it is bijective, and an ***automorphism*** of a quandle Q is an isomorphism $Q \to Q$. The set of all automorphisms of a quandle Q forms a group $\operatorname{Aut} Q$.

Let Q be a quandle. Because of the quandle axiom (Q1), the right translation mappings

$$\rho_a : Q \to Q : q \mapsto q \triangleright a,$$

for a in Q, are bijective. Furthermore, axiom (Q2) guarantees that the map ρ_a is an endomorphism of Q. For, if x and y belong to Q, then we have

$$\rho_a(x \triangleright y) = (x \triangleright y) \triangleright a = (x \triangleright a) \triangleright (y \triangleright a) = (\rho_a x) \triangleright (\rho_a y).$$

Therefore, each right translation map ρ_a is an automorphism of Q.

The set $\{\rho_a : a \in Q\}$ of right translations does not typically form a subgroup of the symmetric group on Q, but the subgroup generated by these maps is of great importance in the theory of quandles.

Definition 8 (Inner Automorphism Group)**.** *Let Q be a quandle. The group $\langle \rho_q : q \in Q \rangle$ generated by the right translation maps ρ_q, for q in Q, is called the* ***inner automorphism group*** *of Q, and is denoted by* $\operatorname{Inn} Q$.

We frequently think of the inner automorphism group of a quandle as a subgroup of the symmetric group on the underlying set of the quandle. In this way, we can apply directly the theory of permutation groups to the group of inner automorphisms. If, as is often the case, a quandle is represented by its Cayley table, then the right translation maps which generate the inner automorphism group can be read off of the Cayley table directly, as they form its columns.

Of considerable interest are the "connected" quandles, which we define presently.

Definition 9 (Connected Quandle)**.** *A quandle is* ***connected*** *if its inner automorphism group acts transitively on the quandle.*

This paper is really about simple quandles, formally defined as follows.

Definition 10 (Simple Quandle)**.** *A quandle is* ***simple*** *if it has more than one element and its only proper homomorphic image is the singleton quandle.*

It is easy to see that a simple quandle is connected, but there are connected quandles that are not simple.

TABLE 1. Cayley table of the first connected quandle of order 6

$\triangleright$	a	b	c	d	e	f
a	a	a	d	c	f	e
b	b	b	e	f	c	d
c	d	e	c	a	b	c
d	c	f	a	d	d	b
e	f	c	b	e	e	a
f	e	d	f	b	a	f

TABLE 2. Cayley table of the second connected quandle of order 6

$\triangleright$	a	b	c	d	e	f
a	a	a	d	e	f	c
b	b	b	f	c	d	e
c	f	d	c	a	c	b
d	c	e	b	d	a	d
e	d	f	e	b	e	a
f	e	c	a	f	b	f

Example 11 (A Non-Simple Connected Quandle). *There are two connected quandles of order equal to* 6*. They are given by the Cayley tables Table 1 and Table 2 (where we take the underlying set, in each case, to be* $\{a, b, c, d, e, f\}$*). Neither quandle is simple, however, as each admits a homomorphism onto the (unique) connected quandle with three elements.*

Let us now turn our attention to specific background needed for the proof of our main result. We begin by noting that Theorem 2 has been proved, computationally, for primes $p < 19$.

Proposition 12 ([21]). *Theorem 2 is true for* $p \leq 17$*.*

Proof. This is a statement of the computational results from [21], from which connected quandles are known up to order 35. We note only that the present author has independently replicated Vendramin's results up to order 30 (see [19]). $\square$

We quote the following result of Clauwens, which is the starting point for our investigations.

Theorem 13 ([5]). *If* p *is a prime and* $p > 3$*, then a connected quandle of order* $2p$ *is simple.*

In [1], Andruskiewitsch and Graña described the structure of the inner automorphism group of a simple quandle. We summarise the results from [1] that we need in the following theorem.

Theorem 14 ([1])**.** *Let Q be a simple quandle, and let $G = \operatorname{Inn} Q$ be its inner automorphism group. Suppose that the order of Q is not a prime power. Then:*

(a) *every proper quotient of G is cyclic;*
(b) *the centre $Z(G)$ of G is trivial;*
(c) *the map $\rho : Q \to G : q \mapsto \rho_q$ is injective, where $a\rho_q = a \triangleright q$, for all $a \in Q$;*
(d) *$C = Q\rho$ is a single conjugacy class in G, and $G = \langle C \rangle$ (that is, C generates G, and we can identify Q with the conjugacy class C in G); and,*
(e) *G has a unique minimal normal subgroup*
$$D = [G, G] = T_1 \times T_2 \times \cdots \times T_k,$$
for some $k \geq 1$, where each subgroup T_i is isomorphic to a finite non-abelian simple group T.

We note that [1] also describes the structure of $\operatorname{Inn} Q$ for a simple quandle Q of prime power order, but we do not need those results here.

We observe that, under the identification of the quandle Q with the conjugacy class C in G, the actions of G on Q by automorphisms and on C by conjugation, are equivalent. For, given arbitrary elements a and b in C, and any element $g \in G$, the conjugates a^g and b^g belong to C, and we have
$$(a^g \triangleright b^g) = (b^g)^{-1}a^g b^g = (g^{-1}bg)^{-1}g^{-1}agg^{-1}bg = g^{-1}b^{-1}abg = (a \triangleright b)^g.$$

We shall use the following result from [19].

Lemma 15 ([19])**.** *A finite quandle with at least four members and with a triply transitive group of automorphisms is trivial.*

Note that a quandle can have a doubly transitive automorphism group [8].

3. Primitive Quandles

Let Q be a quandle with inner automorphism group $G = \operatorname{Inn} Q$. If Q is connected, then G acts (by definition) transitively on Q. However, the action of G on Q may, or may not, be primitive.

Definition 16 (Primitive and Imprimitive Quandles)**.** *A connected quandle is said to be* ***primitive*** *if its inner automorphism group acts* *primitively on it. A connected quandle is* ***imprimitive*** *if its inner automorphism group acts imprimitively on it.*

By considering the contrapositive, it is easy to see that a primitive quandle is simple. However, there do exist simple, imprimitive quandles.

Example 17 (A Simple, Imprimitive Quandle)**.** *The conjugacy class of the* 5*-cycle* $(1, 2, 3, 4, 5)$ *in the alternating group* A_5 *of degree* 5 *is a simple quandle of order* 12*, but its inner automorphism group, which is* A_5*, does not act primitively on it.*

In the remainder of this section, we shall prove Theorem 2 for primitive quandles. To this end, we shall need the following classification of primitive groups of degree $2p$, for an odd prime p.

Proposition 18. *Let G be a finite primitive permutation group of degree $2p$, where p is an odd prime, and suppose that $A_{2p} \not\leq G$. Let $S = \mathrm{Socle}(G)$. Then G is either soluble of degree p, and $G \leq \mathrm{AGL}(1, p)$, or G is an almost simple group among the following cases:*

1. *$S = A_5$ acting on 2-sets, of degree 10 ($p = 5$);*
2. *$S = M_{22}$ of degree 22 ($p = 11$).*
3. *$S = \mathrm{PSL}(2, q)$ in its natural action of degree $q + 1$ on the projective line, where q is an odd prime, and $p = \frac{q+1}{2}$ is prime;*
4. *$S = \mathrm{PSL}(2, 5)$ acting on cosets of a dihedral subgroup of degree 10 ($p = 5$);*
5. *$S = \mathrm{PSL}(2, 4)$ acting on cosets of a dihedral subgroup of degree 6 or 10 ($p \in \{3, 5\}$);*
6. *$S = \mathrm{PSL}(2, 4)$ acting on cosets of $\mathrm{PGL}(2, 2)$, of degree 10 ($p = 5$);*
7. *$S = \mathrm{Sp}(4, 2)$, of degree 6 or 10 (two actions) ($p \in \{3, 5\}$).*

The proof of Proposition 18 will be given below in Section 5.

We now proceed to prove our main result for primitive quandles.

Theorem 19. *Let Q be a primitive quandle of order $2p$, where p is an odd prime. Then Q is isomorphic to the quandle of transpositions in the symmetric group of degree* 5*.*

Proof. We may (and do) suppose that $p > 17$, by Proposition 12.

Since Q is primitive it is, by definition, connected. By Theorem 13, Q is simple. Let $G = \mathrm{Inn}\, Q$ be the inner automorphism group of Q. Since the order of Q is a not a prime power, we have from Theorem 14 that G is a non-abelian group whose proper quotients are cyclic, and G has an unique minimal normal subgroup D isomorphic to a direct power of a non-abelian finite simple group T. Furthermore, G has a generating conjugacy class C, of length $2p$, such that Q is isomorphic to the conjugation quandle defined on the conjugacy class C. Finally, the action of G on Q is permutation isomorphic to the action of G on C by conjugation.

By hypothesis, Q is a primitive quandle, so the action of G on C is primitive. If G has alternating socle (in its natural action) then, since $2p > 5$, it follows that G is (at least) triply transitive. This case is excluded by Lemma 15. From the supposition that $p > 17$, and the classification of primitive groups of degree $2p$, we see that G is an almost simple group with socle $\mathrm{PSL}(2, q)$, for q a power of an odd prime, acting naturally on 1-dimensional subspaces of $\mathbb{F}_q^2$. Thus, $\mathrm{PSL}(2, q) \leq G \leq \mathrm{P\Gamma L}(2, q)$ and so, if H is the stabiliser of a point, then H has trivial centre, by [6, Lemma 7]. But this means that H cannot be the centraliser of any element $x \in C$, since every such element x belongs to its own centraliser. This completes the proof. □

4. Imprimitive Quandles

We consider in this section the case of an imprimitive quandle Q, by showing that none of order equal to twice an odd prime exist.

We shall need a number of results on finite permutation groups. The following result is due to Burnside.

Theorem 20 ([3])**.** *A transitive permutation group of prime degree is either soluble or doubly transitive.*

We also need the following result. The author thanks Derek Holt for explaining his proof of this result.

Lemma 21 ([12])**.** *Let G be a doubly transitive group of prime degree p, acting on a set Ω. Let H be the stabiliser of a point in Ω, and let N be a subgroup of index 2 in H. Then the centre of N is trivial.*

Proposition 22. *A connected quandle of order $2p$, where p is an odd prime, is primitive.*

Proof. Let Q be a connected quandle of order $2p$, where $p > 17$ is an odd prime. Again, by Clauwen's Theorem 13, Q is simple. As in the primitive case, $G = \mathrm{Inn}\, Q$ has a generating conjugacy class $C = x^G$, where $x \in G$, of length $\mid C \mid = 2p$, and an unique minimal normal subgroup $D = [G, G] = T_1 \times T_2 \times \cdots \times T_k$, with each $T_i \simeq T$, a finite non-abelian simple group. (Hence $D = \mathrm{Socle}(G)$.)

Suppose, for an eventual contradiction, that Q is imprimitive; that is, (after identifying Q with C) the action of G on C is imprimitive.

Since G acts imprimitively on C, the centraliser $Z := Z_G(x)$ is not maximal in G. Therefore, there is a subgroup M of G such that

$$Z < M < G,$$

with each inclusion proper. Since the index $[G : Z] = 2p$, it follows that either $[G : M] = 2$ or $[G : M] = p$. If M has index 2 in G, then M is normal in G. But then, since $x \in Z \leq M$, it follows that M contains $C = x^G$. Since C generates G, we have $M = G$, a contradiction. Therefore,

$$[G : M] = p.$$

Since $[G : Z] = 2p$, it follows that $[M : Z] = 2$ (and so, Z is normal in M).

Now, $M \leq MD \leq G$, and MD is a subgroup of G since D is normal, so either $MD = M$ or $MD = G$, by the maximality of M in G.

Suppose, first, that $MD = M$, so that $D \leq M$.

Now, $Z \leq ZD \leq M$, so either $ZD = Z$ or $ZD = M$, because Z is maximal in M.

Suppose that $ZD = Z$; then $D \leq Z$, so that D commutes with x. Let $y \in C$ and choose $g \in G$ such that $y = x^g$. Then

$$D = D^g \leq Z^g = Z_G(x^g) = Z_G(y).$$

Since $y \in C$ was arbitrary, it follows that

$$D \leq \bigcap_{c \in C} Z_G(c) \leq Z(G) = 1,$$

since $G = \langle C \rangle$. This is a contradiction, so $ZD \neq Z$, and therefore $ZD = M$.

Since $ZD = M$, we have

$$| M |=| DZ |= \frac{| D || Z |}{| D \cap Z |}.$$

Using $| M |= \frac{|G|}{[G:M]} = \frac{|G|}{p}$, and $| Z |= \frac{|G|}{[G:Z]} = \frac{|G|}{2p}$, we obtain

$$\frac{| G |}{p} = \frac{| D || G |}{2p | D \cap Z |};$$

whence

$$2 = \frac{| D |}{| D \cap Z |} = [D : D \cap Z].$$

Consequently, $D \cap Z$ is a normal subgroup of index 2 in D. But D is a direct power of a non-abelian simple group, so this is impossible. (The normal subgroups of $D = T_1 \times T_2 \times \cdots \times T_k$ are all of the form $\prod_{i \in I} T_i$, for some subset I of $\{1, 2, \ldots, k\}$.)

Consequently, we must have $G = MD$.

From the formula

$$| G |= \frac{| M || D |}{| D \cap M |}$$

we get

$$[D : D \cap M] = p.$$

In particular, $D \cap M$ is properly contained in D.

The core M_G of M in G is a normal subgroup of G, so the intersection $D \cap M_G$ is a normal subgroup of G contained in D. By the minimality of D, we must therefore have either $D \cap M_G = 1$ or $D \cap M_G = D$. But $D \cap M_G \leq D \cap M < D$, so $D \cap M_G = 1$.

Now, since M_G is normal in G, if $M_G \neq 1$, then M_G contains a minimal normal subgroup of G disjoint from D. But this contradicts the uniqueness of D. Therefore, $M_G = 1$, and G acts faithfully on the cosets of M in G. This means that G is a transitive group of degree $p = [G : M]$. By Burnside's Theorem 20 (since G is insoluble), this action of G on the cosets of M is doubly transitive. Since G is insoluble, it is almost simple and, in particular, D is a simple group. Now Lemma 21 supplies a final contradiction, since Z, being a centraliser of x, has nontrivial centre, and has index equal to 2 in the point stabiliser M.

This completes the proof. □

5. Proof of Proposition 18

Our proof of Proposition 18 is based on the following result of M. W. Liebeck and J. Saxl.

Theorem 23 ([15]). *Let G be a primitive permutation group of degree mp, where p is a prime and $m < p$, and assume that G does not contain A_{mp}. Then either G is soluble or G is one of the groups in* [15, Table 3].

We do not reproduce Table 3 from [15], though we do use it to analyse the various cases that arise. Instead, we simply give a description for the corresponding case. The groups that occur are almost simple groups, and they are described according to the action of their socles in [15, Table 3]. We have also organised the various cases into sections, as follows.

5.1. **Alternating Socle.** There are, of course, for each odd prime p, the primitive groups with socle the alternating group A_{2p} in its natural action.

Case 1. The only other alternating groups that occur have degrees 15, 35 or $\frac{c(c-1)}{2}$, where $p \in \{c, c-1\}$. The only primes for which the Diophantine equation $\binom{c}{2} = 2p$ has a solution are $p = 3$ and $p = 5$. This gives rise to Case (1) in Proposition 18.

5.2. **Classical Socle.** There are a variety of cases involving classical groups.

5.2.1. *PSL.* There are a number of cases in which the socle is a projective special linear group.
Case 2. There is an action of $\mathrm{PSL}(d, q)$ on $1-$ or $(d-1)$-dimensional subspaces. The degrees are of the form

$$n = \frac{(q^d - 1)}{(q-1)},$$

where p divides n and $d \geq 2$.

Using $2p = n$, we have

$$2p = \frac{(q^d - 1)}{(q-1)} = 1 + q + \cdots + q^{d-1}.$$

If q is even, then $1 + q + \cdots + q^{d-1}$ is odd, so q must be odd. Now, $1 + q + \cdots + q^{d-1}$ is an even sum of odd terms, so the number d of summands must be even. Write $d = 2\delta$.

Suppose that $d > 2$, so that $\delta > 1$. Then

$$q^d - 1 = (q^\delta)^2 - 1 = (q^\delta - 1)(q^\delta + 1).$$

Hence,

$$2p = \frac{(q^\delta + 1)(q^\delta - 1)}{(q-1)} = (q^\delta + 1)(1 + q + \cdots + q^{\delta-1}).$$

Since $q \geq 2$, we have

$$1 + q + \cdots + q^{\delta-1} \geq 1 + q \geq 3.$$

Hence, $1 + q + \cdots + q^{\delta-1} = p$ and $q^\delta + 1 = 2$. But then, $q^\delta = 1$ and $\delta = 0$, a contradiction. Therefore, $d = 2$, and we get

$$2p = \frac{(q^2 - 1)}{(q-1)} = q + 1,$$

and so $\frac{(q+1)}{2}$ is a prime. This yields Case (3) in Proposition 18.

Case 3. Next, there is an action of $\mathrm{PSL}(d,q)$ on 2- or $(d-2)$-dimensional subspaces, where the degrees are of the form

$$n = \frac{(q^d-1)(q^{d-1}-1)}{(q^2-1)(q-1)},$$

and where $d \geq 4$, and either $p = \frac{(q^{d-1}-1)}{(q-1)}$ or p divides $\frac{(q^d-1)}{(q-1)}$.

To handle this case, suppose first that $p = \frac{(q^{d-1}-1)}{(q-1)}$. Then, using $2p = n$, we obtain

$$2\frac{(q^{d-1}-1)}{(q-1)} = \frac{(q^d-1)(q^{d-1}-1)}{(q^2-1)(q-1)},$$

which yields

$$2 = \frac{q^d-1}{q^2-1},$$

or

$$2(q^2-1) = q^d-1.$$

Dividing by $q-1$, we obtain

$$2q+2 = 2(q+1) = 1+q+\cdots+q^{d-1}.$$

so that

$$q+1 = q^2+\cdots+q^{d-1}.$$

But, from $q \geq 2$ it follows that $q^2 > q$, and

$$q+1 < q^2+1 < q^2+q^3+\cdots+q^{d-1},$$

unless $d-1 = 2$, so that $d = 3$. But we assumed that $d \geq 4$, so this cannot be the case.

Now suppose that p divides $\frac{(q^d-1)}{(q-1)}$, and write

$$sp = \frac{(q^d-1)}{(q-1)},$$

where s is a positive integer. Then we have (using $n = 2p$),

$$2p = sp\frac{(q^{d-1}-1)}{(q^2-1)},$$

which gives

$$2(q^2-1) = s(q^{d-1}-1),$$

or, dividing the common factor of $q-1$ from both sides,

$$2(q+1) = s(1+q+\cdots+q^{d-2}).$$

But $s \geq 1$, so we obtain

$$\begin{aligned} 2(q+1) &= s(1+q+\cdots+q^{d-2}) \\ &\geq 1+q+\cdots+q^{d-2}. \end{aligned}$$

Now subtracting $q-1$ from both sides of this inequality yields

$$q+1 \geq q^2+\cdots+q^{d-2}.$$

This can occur only if $d=4$ so that there is only one summand on the right hand side, in which case we get $q+1 \geq q^2$. But this is impossible, since $q \geq 2$ then implies that

$$0 \geq q^2-q-1 > q^2-2q+1 = (q-1)^2 \geq 1.$$

Therefore, this case cannot occur.
Case 4. Next, we consider the action of $\mathrm{PSL}(7,q)$ on 3- or 4-dimensional subspaces, where the degree is

$$n = \frac{(q^7-1)(q^6-1)(q^5-1)}{(q^3-1)(q^2-1)(q-1)},$$

and where $p = \frac{(q^7-1)}{(q-1)}$.

Using $2p = n$, we obtain

$$2\frac{(q^7-1)}{(q-1)} = \frac{(q^7-1)(q^6-1)(q^5-1)}{(q^3-1)(q^2-1)(q-1)},$$

which yields

$$2 = \frac{(q^6-1)(q^5-1)}{(q^3-1)(q^2-1)},$$

or, equivalently,

$$2(q^3-1)(q^2-1) = (q^6-1)(q^5-1).$$

But, since $q \geq 2$, we have

$$\begin{aligned} 2(q^3-1)(q^2-1) &< (8q^3-1)(8q^2-1) \\ &\leq (q^6-1)(q^5-1), \end{aligned}$$

a contradiction.
Case 5. Next, $\mathrm{PSL}(d,q)$ acts on incident point-hyperplane pairs, with degree equal to

$$n = \frac{(q^d-1)(q^{d-1}-1)}{(q-1)^2},$$

where $d \geq 3$ and p divides $\frac{(q^d-1)}{(q-1)}$ (and G contains a graph automorphism).

Since p divides $\frac{(q^d-1)}{(q-1)}$, write

$$sp = \frac{(q^d-1)}{(q-1)},$$

where s is a positive integer. Then we have

$$2p = sp\frac{(q^{d-1}-1)}{(q-1)},$$

so that

$$2(q-1) = s(q^{d-1}-1) = s(q-1)(1+q+\cdots+q^{d-2}).$$

Dividing both sides by $q-1$, we obtain

$$2 = s(1+q+\cdots+q^{d-2}).$$

Since $s \geq 1$, it follows that

$$2 \geq 1+q+\cdots+q^{d-2},$$

which is impossible, since $d \geq 3$.

Case 6. Next, there is an action of $\mathrm{PSL}(d,q)$ on non-incident point-hyperplane pairs, where the degree is

$$n = \frac{q^{d-1}(q^d-1)}{(q-1)},$$

and where $d \geq 3$ and p divides $\frac{(q^d-1)}{(q-1)}$ (and G contains a graph automorphism).

Since p must divide $\frac{(q^d-1)}{(q-1)}$, write

$$sp = \frac{(q^d-1)}{(q-1)},$$

for some positive integer s. Then we have $2p = n = spq^{d-1}$ or

$$2 = sq^{d-1} \geq q^{d-1} \geq q^2 \geq 4,$$

a contradiction. Therefore, this case cannot occur.

Case 7. Next, the action of $\mathrm{PSL}(4,3)$ on the cosets of its subgroup of shape $\mathrm{PSp}(4,3).2$. In this case, the degree is 117 and $p = 13$.

This case does not occur, since $2p = 26 \neq 117$.

Finally, there are several actions of $\mathrm{PSL}(2,q)$, with $q \geq 4$, as follows.

Case 8. The action on cosets of a dihedral subgroup of degree

$$n = \frac{q(q \pm 1)}{2},$$

where $p = q$ if q is odd, and $p = q \pm 1$ if q is even. In this case, $G = \mathrm{PGL}(2, q)$, for $q = 7, 11$.

Suppose first that q is odd, so $p = q$. Then we get $2p = n = \frac{p(p\pm1)}{2}$, so that $4p = p(p \pm 1)$, and hence, $4 = p \pm 1$. This implies that $p = 3$ or $p = 5$.

Now suppose that q is even. Then $p = q \pm 1$, so $2p = n = \frac{qp}{2}$ and $q = 4$ giving $p = 3$ or $p = 5$. In this way, we obtain Case (5) of Proposition 18.

Case 9. The action of $\mathrm{PSL}(2, q)$ on cosets of $\mathrm{PGL}(2, \sqrt{q})$, with p a divisor of $q + 1$, where q is a square, and the degree is

$$n = \frac{\sqrt{q}(q + 1)}{f},$$

where $f = (2, q - 1)$.

Since p divides $q + 1$, there is a positive integer s for which

$$sp = q + 1.$$

Then we have

$$2p = n = \frac{sp\sqrt{q}}{f},$$

or

$$2f = s\sqrt{q}.$$

First suppose that q is even. Then $q-1$ is odd, so $f = 1$, and we get $2 = s\sqrt{q}$ or $4 = s^2q$. Since q is a square, we can write $q = v^2$, for some integer $v \geq 2$. Then we have $4 = s^2v^2 = (sv)^2$. Now, $v \geq 2$ so we have

$$4 = (sv)^2 \geq (2s)^2 \geq 4s^2,$$

so $s = 1$ and $p = q + 1$. But $2p = \sqrt{q}(q + 1)$, so $2p = p\sqrt{q}$ and hence $\sqrt{q} = 2$. This implies that $q = 4$. Thus, $p = 5$ and $n = 10$. Here, we have Case (6) in Proposition 18.

Now suppose that q is odd. Then $f = 2$ and we have

$$2p = \frac{\sqrt{q}(q + 1)}{2},$$

or

$$4p = \sqrt{q}(q + 1).$$

Again, let s be a positive integer such that $sp = q+1$. Then $4p = sp\sqrt{q}$ so that $4 = s\sqrt{q}$. Now, $q \geq 4$ since q is a square, so

$$4 = s\sqrt{q} \geq s\sqrt{4} = 2s,$$

which implies that $s \leq 2$, so $s \in \{1, 2\}$.

If $s = 1$, then $p = q + 1$ so $2p = \frac{p\sqrt{q}}{2}$ or $4 = \sqrt{q}$, and so $q = 16$. But we supposed that q was odd, so this case does not occur.

If $s = 2$, we get $4p = 2p\sqrt{q}$ so that $\sqrt{q} = 2$; that is, $q = 4$. Again, since q is odd, this case does not occur either.

Case 10. The action on cosets of A_5, where $p = q$, $q \equiv \pm 1 \pmod{10}$, and the degree is

$$n = \frac{q(q^2 - 1)}{120},$$

and $q \leq 109$.

From $2p = n$ and $p = q$, we obtain

$$2p = \frac{p(p^2 - 1)}{120},$$

from which it follows that

$$240p = p(p^2 - 1),$$

and hence, $p^2 = 241$, which has no integer solutions.

Case 11. The action on cosets of S_4, where $p = q$, $q \equiv \pm 1 \pmod 8$, and the degree is

$$n = \frac{q(q^2 - 1)}{48},$$

where $q \leq 47$.

As in the previous case, we find that $p^2 = 97$, which has no integer solutions.

Case 12. The action on cosets of A_4, where $p = q$, $q \equiv 3 \pmod 8$, and the degree is

$$n = \frac{q(q^2 - 1)}{24},$$

where $q \leq 19$.

Here, using $p = q$ and $2p = n$, we obtain $p^2 = 49$, and so $p = 7$. However, $7 \not\equiv 3 \pmod 8$, so this case does not arise either.

5.2.2. PSp.

Case 13. There is an action of the group $\mathrm{PSp}(2d, q)$ on lines (or, on totally isotropic 2-dimensional subspaces, in case $d = 2$), with p a divisor of $q^d + 1$ and d a power of 2, of degree

$$n = \frac{(q^{2d} - 1)}{(q - 1)}.$$

Writing $q^d + 1 = sp$, for some positive integer s, and using $2p = n$, we obtain

$$\begin{aligned} 2p &= \frac{(q^{2d}-1)}{(q-1)} \\ &= \frac{(q^d+1)(q^d-1)}{(q-1)} \\ &= sp\frac{(q^d-1)}{(q-1)}. \end{aligned}$$

Hence, we have

$$2 = s\frac{(q^d-1)}{(q-1)} = s(1 + q + \cdots q^{d-1}).$$

As before, this is impossible for $d \geq 2$, since $s \geq 1$.

5.2.3. Sp.
Case 14. For even q, there is an action of $\mathrm{Sp}(2d, q)$ of degree

$$n = \frac{q^d(q^d \pm 1)}{2},$$

where $p = q^d \pm 1$. If $p = q^d + 1$, then d is a power of 2. If $p = q^d - 1$, then $q = 2$ and d is prime.

First suppose that $p = q^d + 1$, so that

$$2(q^d + 1) = \frac{q^d(q^d + 1)}{2},$$

which yields

$$4 = q^d.$$

Therefore, $q = d = 2$, and so $p = 5$ and $n = 10$. This yields Case (7) of Proposition 18.

If, instead, $p = q^d - 1$, then we obtain

$$2(q^d - 1) = \frac{q^d(q^d - 1)}{2},$$

so that, again,

$$4 = q^d,$$

and so $p = 3$ and $n = 6$, and we obtain Case (7) of Proposition 18 again.

Case 15. There is an action of $\mathrm{Sp}(4,q)$, for even q, of degree

$$n = \frac{q^2(q^2+1)}{2},$$

where $p = q^2+1$.

In this case we get, from $n = 2p$,

$$2(q^2+1) = \frac{q^2(q^2+1)}{2},$$

from which it follows that $q^2 = 4$, and hence, $q = 2$ and $n = 10$. Here we have Case (7) of Proposition 18 again.

5.2.4. *PSU.*

Case 16. The group $\mathrm{PSU}(d,q)$ acts on singular 1-subspaces, for prime $d \geq 3$, with degree

$$n = \frac{(q^d+1)(q^{d-1}-1)}{(q^2-1)},$$

where p divides $\frac{(q^d+1)}{(q+1)}$.

Since p divides $\frac{(q^d+1)}{(q+1)}$, there is a positive integer s for which

$$sp = \frac{(q^d+1)}{(q+1)}.$$

Then, from $2p = n$, we obtain

$$2p = sp\frac{(q^{d-1}-1)}{(q-1)},$$

so that

$$2(q-1) = s(q^{d-1}-1) = s(q-1)(1+q+\cdots+q^{d-2}).$$

Dividing out the common factor of $q-1$, we obtain

$$2 = s(1+q+\cdots+q^{d-2}).$$

Hence, as $s \geq 1$, we obtain

$$\begin{aligned} 2 &= s(1+q+\cdots+q^{d-2}) \\ &\geq 1+q+\cdots+q^{d-2} \\ &\geq 3, \end{aligned}$$

unless $d = 2$. But we are given that $d \geq 3$, so this case cannot occur.

5.2.5. *$P\Omega$.*

Case 17. There is an action of $\mathrm{P}\Omega(2d+1,q)$ on singular 1-subspaces, with degree

$$n = \frac{(q^d-1)(q^{d-1}+1)}{(q-1)},$$

where $p = \frac{(q^d-1)}{(q-1)}$, and $d > 4$ is prime.

Using $n = 2p$, we obtain

$$2\frac{(q^d-1)}{(q-1)} = \frac{(q^d-1)(q^{d-1}+1)}{(q-1)},$$

which yields $q^{d-1}-1 = 2$, or $q^{d-1} = 3$. But $d > 4$, so this is impossible.
Case 18. There is an action of $\mathrm{P}\Omega(2d+1,q)$ on singular 1-dimensional subspaces, with degree

$$n = \frac{(q^{2d}-1)}{(q-1)},$$

where p divides q^d+1 and d is a power of 2.

Since p divides q^d+1, we can write $sp = q^d+1$, for some positive integer s. Then we have

$$2p = n = \frac{(q^{2d}-1)}{(q-1)} = \frac{(q^d+1)(q^d-1)}{(q-1)} = sp\frac{(q^d-1)}{(q-1)}.$$

Hence,

$$2 = s\frac{(q^d-1)}{(q-1)} = s(1+q+\cdots+q^{d-1}).$$

Since $s \geq 1$, we get

$$2 \geq 1+q+\cdots+q^{d-1}.$$

But, since $d \geq 2$ and $q \geq 2$, this is impossible, and we conclude that this case cannot occur.

5.2.6. Ω^+.
Case 19. There is an action of $\Omega^+(2d,2)$ on non-singular subspaces, for prime $d > 4$, where $p = 2^d-1$, with degree

$$n = 2^{d-1}(2^d-1).$$

In this case, substituting $n = 2p$, we obtain

$$2p = 2^{d-1}(2^d-1),$$

which, for $p = 2^d-1$ gives

$$2(2^d-1) = 2^{d-1}(2^d-1),$$

which yields $2 = 2^{d-1}$. Hence, $d = 2$. But we began with $d > 4$, so this case cannot occur.

5.2.7. $P\Omega^+$.

Case 20. There is an action of $\mathrm{P}\Omega^+(2d, q)$ with p a divisor of $q^d + 1$ and $d \geq 4$ a power of 2 with degree either

$$n = \frac{(q^d + 1)(q^{d-1} - 1)}{(q - 1)}$$

or

$$n = q^{d-1}(q^d + 1).$$

Suppose first that we have degree $n = q^{d-1}(q^d+1)$. Write $sp = q^d+1$, for some positive integer s. Then we have

$$2p = n = q^{d-1}(q^d + 1) = spq^{d-1},$$

or

$$2 = sq^{d-1}.$$

Thus, either $s = 1$ and $q^{d-1} = 2$ and so $q = 2$ and $d = 2$, or else $s = 2$ and we get $q^{d-1} = 1$, so $d = 1$. Thus, this case cannot occur.

Now assume that the degree n is

$$n = \frac{(q^d + 1)(q^{d-1} - 1)}{(q - 1)}.$$

Using $sp = q^d + 1$, we obtain

$$2p = sp\frac{q^{d-1} - 1)}{(q - 1)} = sp(1 + q + \cdots + q^{d-2}).$$

Hence, since $s \geq 1$, we have

$$2 \geq 1 + q + \cdots + q^{d-2}.$$

Now, since $d \geq 4$, therefore, this is impossible.

5.3. **Exceptional Socle.**

5.3.1. $Sz(q)$.

Case 21. Here, the socle is the group $Sz(q)$, with degree $q^2 + 1$ and $p \mid q^2 + 1$, $p > q$, $q = 2^{2m+1}$.

We have

$$2p = q^2 + 1 = 2^{2(2m+1)} + 1,$$

which is impossible, since $2^{2(2m+1)} + 1$ is odd, while $2p$ is even.

5.3.2. ${}^2G_2(q)$.

Case 22. In this case, we consider groups with socle the Ree group $R(q) = {}^2G_2(q)$ with degree q^2+1, $p \mid q^2+q+1$, $p > \sqrt{n}$, $q = 3^{2m+1}$.

Since p divides q^2+q+1, there is a positive integer s such that $sp = q^2+q+1$. Then we have

$$2p = n = q^2 + 1 = q + sp,$$

or

$$q = p(2-s).$$

Hence,

$$p(2-s) = 3^{2m+1}.$$

Thus, $p = 3$, so $n = 6$. But then $6 = 3^{2(2m+1)} + 1$, so $3^{2(2m+1)} = 5$, a contradiction. Therefore, this case cannot occur.

5.4. **Sporadic Socle.**

Case 23. The only sporadic simple groups that occur are the Mathieu groups, of degrees $276, 23, 253, 506, 22, 77, 66, 11, 55$ and 66, and the sporadic groups J_1 of degree 266 and the Conway group Co_2 of degree 276. Of these, only $22 = 2 \cdot 11$ is twice a prime number, which is Case (2) in Proposition 18.

This completes the proof of Proposition 18. $\square$

References

[1] N. Andruskiewitsch and M. Graña. From racks to pointed Hopf algebras. *Adv. Math.*, 178:177–243, 2003.

[2] S. R. Blackburn. Enumerating finite racks, quandles and kei, March 2012. `arXiv:1203.6504v1[math.GT]`.

[3] W. Burnside. On some properties of groups of odd order. *J. London Math. Soc.*, 33:162–185, 1901.

[4] J. S. Carter. A survey of quandle ideas, February 2010. `arXiv:1002.4429v2[math.GT]`.

[5] F. J. B. J. Clauwens. Small connected quandles, July 2011. `arXiv:1011.2456v2[math.GR]`.

[6] P. Etingof, R. Guralnick, and A. Soloviev. Indecomposable set-theoretical solutions to the quantum Yang-Baxter equation on a set with a prime number of elements. *J. Algebra*, 242(2):709–719, 2001. `arXiv:0007170v1[math.QA]`.

[7] R. Fenn and C. Rourke. Racks and links in codimension two. *J. Knot Theory Ramifications*, 1:343–406, 1992.

[8] A. Ferman, T. Nowik, and M. Teicher. On the structure and automorphism group of finite alexander quandles. Preprint, November 2008. `arXiv:0811.4211v1[math.GT]`.

[9] M. Graña. Indecomposable racks of order p^2. *Beiträge Alg. Geom.*, 45(2)::665–676, 2004.

[10] R. Henderson, T. Macedo, and S. Nelson. Symbolic computation with finite quandles. *J. Symb. Comp.*, 41:811–817, 2006. `arXiv:0508351v2[math.GT]`.

[11] B. Ho and S. Nelson. Matrices and finite quandles. *Homology, Homotopy and Applications*, 7(1):197–208, 2005. arXiv:0412417v3[math.GT].

[12] D. Holt and L. Vendramin. Finite simple groups and conjugacy classes with 2p elements. MathOverflow. http://mathoverflow.net/questions/75672 (version: 2011-09-17). Available from: http://mathoverflow.net/questions/75672, arXiv:http://mathoverflow.net/questions/75672.

[13] D. Joyce. A classifying invariant of knots, the knot quandle. *Journal of Pure and Applied Algebra*, 23(1):37–65, 1982. doi:DOI:10.1016/0022-4049(82)90077-9.

[14] S. Kamada. Knot invariants derived from quandles and racks. *Geometry and Topology Monographs*, 4:103–117, 2002.

[15] M. W. Liebeck and J. Saxl. Primitive permutation groups containing an element of large prime order. *J. London Math. Soc.*, 31:250–264, 1985.

[16] S. V. Matveev. Distributive groupoids in knot theory. *Mat. Sbornik (N.S.)*, 119(1):78–88, 1982.

[17] J. McCarron. A181769 (number of isomorphism classes of quandles of order n). http://oeis.org/A181769.

[18] J. McCarron. A181771 (number of isomorphism classes of connected quandles of order n). http://oeis.org/A181771.

[19] J. McCarron. Small homogeneous quandles. In *Proceedings ISSAC 2012*, Grenoble, France, July 2012. (to appear).

[20] N. J. Sloane and *et al*. Online encyclopedia of integer sequences. http://oeis.org.

[21] L. Vendramin. On the classification of quandles of low order, June 2011. arXiv:1105.5341v2[math.GT].

[22] L. Vendramin. On the classification of quandles of low order. *J. Knot Theory Ramifications*, 21, August 2012. doi:10.1142/S0218216512500885.

Maplesoft, 615 Kumpf Drive, Waterloo, ON, CANADA N2V 1K8
E-mail address: james@maplesoft.com