J. Math. Soc. Japan
Vol. 69, No. 3 (2017) pp. 1051–1057
doi: 10.2969/jmsj/06931051

Doubly transitive groups and cyclic quandles

By Leandro Vendramin

(Received Feb. 14, 2014)
(Revised Sep. 17, 2015)

Abstract. We prove that for $n > 2$ there exists a quandle of cyclic type of size n if and only if n is a power of a prime number. This establishes a conjecture of S. Kamada, H. Tamaru and K. Wada. As a corollary, every finite quandle of cyclic type is an Alexander quandle. We also prove that finite doubly transitive quandles are of cyclic type. This establishes a conjecture of H. Tamaru.

Introduction.

Quandles are algebraic structures deeply related to the Reidemeister moves of classical knots. These structures play an important role in knot theory because they produce strong knot invariants, see for example [**4**], [**5**] and [**6**]. The applications of quandles in knot theory force us to study certain particular classes of quandles. One of these classes is the class of finite quandles of cyclic type. The idea of studying such quandles goes as far as [**13**]. Quandles of cyclic type were independently considered in [**10**] and [**17**].

In this note we present the proofs of two conjectures related to quadles of cyclic type. First we prove the following theorem, conjectured by S. Kamada, H. Tamaru and K. Wada, see [**12**, Conjecture 4.7].

Theorem 1. *Let $n \geq 3$. Then there exists a quandle of size n of cyclic type if and only if n is a power of a prime number.*

K. Wada independently proved that cyclic quandles with a prime power size are Alexander quandles [**18**]. Theorem 1 yields the following stronger result.

Corollary 2. *Let X be a finite quandle of cyclic type. Then $|X|$ is a power of a prime number and X is an Alexander simple quandle over the field with $|X|$ elements.*

Finally, using the classification of simple groups we prove the following theorem.

Theorem 3. *Every finite doubly transitive quandle is an Alexander simple quandle.*

2010 *Mathematics Subject Classification.* Primary 57M25.
Key Words and Phrases. finite quandles, two-point homogeneous quandles, quandles of cyclic type, doubly-transitive groups.
This work is supported by Conicet, UBACyT 20020110300037, ICTP, and the Alexander von Humboldt Foundation.

The theorem gains in interest if we know that doubly transitive Alexander quandles are of cyclic type. This was proved by K. Wada [**18**]. Then one immediately obtains the following corollary, which proves a conjecture of H. Tamaru, see [**17**, Conjecture 5.1].

COROLLARY 4. *Every finite doubly transitive quandle is of cyclic type.*

The principal significance of the corollary is that it advances the classification of k-transitive quandles for $k \geq 2$. On the other hand, the classification of finite indecomposable quandles is somewhat out of reach. Thus the following seems to be an interesting problem.

PROBLEM 5. *Classify finite primitive quandles.*

The paper is organized as follows. In Section 1 we set up notations and terminology, and we review some basic facts about quandles and permutation groups. Section 2 is devoted to prove Theorem 1 and Corollary 2. The proof of the theorem is based on the following observation: the inner group of a finite quandle of cyclic type is a Frobenius group. The proof of the corollary uses Theorem 1 and the classification of simple quandles of Andruskiewitsch and Graña [**2**, Section 3]. In Section 3 we prove Theorem 3. The proof depends on the classification of simple groups.

1. Preliminaries.

Recall that a *quandle* is a set X with a binary operation $\triangleright\colon X \times X \to X$ such that $x \triangleright x = x$ for all $x \in X$, the map $\varphi_x\colon X \to X$, $y \mapsto x \triangleright y$, is bijective for all $x \in X$, and $x \triangleright (y \triangleright z) = (x \triangleright y) \triangleright (x \triangleright z)$ for all $x, y, z \in X$. The *inner group* of X is the group $\operatorname{Inn}(X) = \langle \varphi_x \mid x \in X \rangle$. The quandle X is *indecomposable* (or *connected*) if $\operatorname{Inn}(X)$ acts transitively on X. From the definition of quandle one immediately obtains the following lemma.

LEMMA 6. *Let X be a quandle and $x \in X$. Then φ_x is a central element of the stabilizer of x in* $\operatorname{Inn}(X)$.

A quandle X is *primitive* if $\operatorname{Inn}(X)$ acts primitively on X. For $k \geq 1$ we say that X is *k-transitive* if $\operatorname{Inn}(X)$ acts k-transitively on X. It is worth pointing out that 1-transitive means indecomposable, and that 2-transitive (or *doubly transitive*) quandles are called two-point homogeneous in [**17**]. A similar argument to that of [**19**, Theorem 9.6] shows that doubly transitive quandles are primitive. Similarly, $(k+1)$-transitive quandles are k-transitive for all $k \geq 1$. The following result of McCarron [**15**, Proposition 5] shows that higher transitivity is a rare phenomenon: the dihedral quandle with three elements is the unique 3-transitive quandle.

LEMMA 7 (McCarron). *Let $k \in \mathbb{N}$ with $k \geq 2$ and X be a finite k-transitive quandle with at least four elements. Then $k \leq 2$.*

PROOF. Suppose that $k \geq 3$. Since X is k-transitive, it is indecomposable and nontrivial. Thus let $x, y \in X$ such that $|\{x, y, x \triangleright y\}| = 3$. By assumption, there exists

$z \in X \setminus \{x, y, x \triangleright y\}$. Since $\mathrm{Inn}(X)$ acts k-transitively on X and $k \geq 3$, there exists $f \in \mathrm{Inn}(X)$ such that $f(x) = x$, $f(y) = y$ and $f(x \triangleright y) = z$. Then $x \triangleright y = f(x) \triangleright f(y) = f(x \triangleright y) = z$, a contradiction. □

We shall also need the following lemma of [**14**]. Recall that a quandle is *simple* if it has no quotients except itself and the trivial quandle of one element [**11**].

Lemma 8 (McCarron). *Let X be a finite quandle and suppose that $\mathrm{Inn}(X)$ acts primitively on X. Then X is simple.*

Proof. Suppose that X is not simple. Then there exist a nontrivial quandle $Q \neq X$ and a surjective homomorphism of quandles $p\colon X \to Q$. Consider the equivalence relation over X given by $x \equiv y$ if and only if $p(x) = p(y)$. We claim that the orbits of this action form a system of blocks for $\mathrm{Inn}(X)$. To prove our claim let $x \in X$ and

$$\Delta_x = \{y \in X \mid p(x) = p(y)\}$$

be an equivalence class. Then $\varphi_y \cdot \Delta_x = \Delta_{\varphi_y(x)}$ for all $y \in X$ and hence $f \cdot \Delta_x = \Delta_{f(x)}$ for all $f \in \mathrm{Inn}(X)$. Thus $f \cdot \Delta_x$ is also an equivalence class and therefore $f \cdot \Delta_x \cap \Delta_x = \emptyset$ or $f \cdot \Delta_x = \Delta_x$. This implies that $\mathrm{Inn}(X)$ is not primitive. □

Following [**17**, Definition 3.5], we say that a quandle X is of *cyclic type* (or *cyclic*) if for each $x \in X$ the permutation φ_x acts on $X \setminus \{x\}$ as a cycle of length $|X| - 1$, where $|X|$ denotes the cardinality of X. Tamaru proved that quandles of cyclic type are doubly transitive [**17**, Proposition 3.6]. In particular, quandles of cyclic type are indecomposable.

Example 9 (Alexander quandles). Alexander quandles form an important family of examples. Let A be an abelian group and $g \in \mathrm{Aut}(A)$. Then A is a quandle with $x \triangleright y = (1 - g)(x) + g(y)$ for all $x, y \in A$. This is the *Alexander quandle* of type (A, g).

Example 10. Let us mention a particular case of Example 9. Let p be a prime number, $m \in \mathbb{N}$, $q = p^m$, and $\mathbb{F}_q$ be the field of q elements. For each $\alpha \in \mathbb{F}_q$ the *Alexander quandle* of type (q, α) is the quandle structure over $\mathbb{F}_q$ given by $x \triangleright y = (1 - \alpha)x + \alpha y$ for all $x, y \in \mathbb{F}_q$.

2. Proofs of Theorem 1 and Corollary 2.

Using Alexander quandles, H. Tamaru proved the existence of quandles of cyclic type with a prime number of elements, see [**17**, Section 4]. We use Tamaru's method to prove a similar result.

Recall that for any power q of a prime number, the multiplicative subgroup of $\mathbb{F}_q$ is cyclic of order $q - 1$.

Proposition 11. *Let p be a prime number, $m \in \mathbb{N}$ and $q = p^m$. Let $\alpha \in \mathbb{F}_q$ and X be an Alexander quandle of type (q, α). Then X is of cyclic type if and only if α has order $q - 1$.*

PROOF. Suppose first that X is of cyclic type. Then φ_0 acts on $X \setminus \{0\}$ as a cycle of length $q-1$. Thus

$$\varphi_0 = \left(1\ \varphi_0(1)\ \varphi_0^2(1) \cdots \varphi_0^{q-2}(1)\right)$$

and $\varphi_0^i(1) \neq \varphi_0^j(1)$ for $i, j \in \{0, \dots, q-2\}$ with $i \neq j$. Since $\varphi_0^k(1) = \alpha^k$ for all $k \in \{0, \dots, q-2\}$, the claim follows.

Conversely, suppose that α has order $q-1$. Since X has no nontrivial subquandles by [**1**, Proposition 4.1], it follows that X is indecomposable. The permutation φ_0 acts on X as the cycle $(1\,\alpha\,\alpha^2 \cdots \alpha^{q-2})$ of length $q-1$. Since X is indecomposable, this implies that X is of cyclic type by [**17**, Proposition 3.9]. □

Now we prove that the cardinality of a finite quandle of cyclic type is some power of a prime number. For that purpose, we need some basic properties of Frobenius groups. A finite group G acting on a finite set X is a *Frobenius group* if $G_x \cap G_y = 1$ for all $x, y \in X$ with $x \neq y$, where G_x and G_y denote the stabilizer (or isotropy) subgroups of x and y respectively. The *degree* of G is the cardinality of X.

It follows from the definition that the center of a Frobenius group is trivial. The following result is a consequence of [**19**, Theorem 5.1] and [**19**, Theorem 11.3(a)].

THEOREM 12. *Let G be a doubly transitive Frobenius group of degree n. Then $n = p^m$ for some prime number p and $m \in \mathbb{N}$.*

We shall also need the following two lemmas.

LEMMA 13. *Let X be a finite quandle of cyclic type, $x \in X$, and $G = \operatorname{Inn}(X)$. Then G_x is cyclic and generated by φ_x.*

PROOF. Assume that X has n elements. Then G is a subgroup of $\mathbb{S}_n$. Since

$$f \varphi_x f^{-1} = \varphi_{f(x)} = \varphi_x$$

for all $f \in G_x$, we conclude that $G_x \subseteq C_G(\varphi_x)$, where $C_G(\varphi_x)$ denotes the centralizer of φ_x in G. The permutation φ_x is a cycle of length $n-1$. Hence

$$C_G(\varphi_x) = C_{\mathbb{S}_n}(\varphi_x) \cap G = \langle \varphi_x \rangle$$

and therefore $G_x = \langle \varphi_x \rangle$. □

LEMMA 14. *Let $n \geq 3$ and X be a quandle of cyclic type of size n. Then $\operatorname{Inn}(X)$ is a Frobenius group of degree n.*

PROOF. Let $G = \operatorname{Inn}(X)$ and $x \in X$. By Lemma 13, $G_x = \langle \varphi_x \rangle$. We claim that for each $g \in G \setminus G_x$ the subgroups G_x and $gG_xg^{-1} = G_{g(x)}$ have trivial intersection. Let $h \in G_x \cap gG_xg^{-1}$ and assume that $h = g\varphi_x^k g^{-1} = \varphi_x^l$ for some $k, l \in \{0, \dots, n-2\}$ and $g \in G \setminus G_x$. Then

$$\varphi_x^l = g\varphi_x^k g^{-1} = (g\varphi_x g^{-1})^k = \varphi_{g(x)}^k.$$

Let $y \in X \setminus \{x\}$ such that $g(x) = y$. Then $\varphi_x^l = \varphi_y^k$. Since φ_y is a $(n-1)$-cycle that fixes y and $\varphi_y^k(x) = \varphi_x^l(x) = x$, we conclude that $k = 0$. From this the claim follows. □

Now we prove that for $n \geq 3$ there exists a quandle of cyclic type of size n if and only if n is a power of a prime number. This establishes [**12**, Conjecture 4.7].

Proof of Theorem 1. Assume that $n = p^m$, where p is a prime number and $m \in \mathbb{N}$. By Proposition 11, there exists a quandle of cyclic type of size n. Conversely, if X is a quandle of cyclic type and size n, then $\mathrm{Inn}(X)$ is a Frobenius group by Lemma 14. Since $\mathrm{Inn}(X)$ acts doubly transitively on X by [**17**, Proposition 3.6], Theorem 12 implies that n is a power of a prime number. □

Theorem 1, Lemma 8 and the classification of simple quandles of Andruskiewitsch and Graña [**2**, Section 3] yield Corollary 2.

Proof of Corollary 2. Let us assume that X is a cyclic quandle. By Theorem 1, the cardinality of X is some power of a prime number. Since X is doubly transitive by [**17**, Proposition 3.6], it follows that $\mathrm{Inn}(X)$ acts primitively on X. By Lemma 8, X is simple. Now [**2**, Theorem 3.9] yields the claim. □

3. Proof of Theorem 3.

Recall that a *minimal normal* subgroup of G is a normal subgroup N of G such that $N \neq 1$ and N contains no normal subgroup of G except 1 and N. The *socle* of G is the product of the minimal normal subgroups of G. The following theorem goes back to Burnside, see for example [**3**, Theorem 4.3].

Theorem 15 (Burnside). *Let G be a doubly transitive group and N be a minimal normal subgroup of G. Then N is either a regular elementary abelian group, or a nonregular nonabelian simple group.*

As a consequence of the odd analogue of Glauberman Z*-theorem, we prove that finite doubly transitive quandles are Alexander simple. The key step is a group-theoretical result kindly comunicated to us by G. Robinson, see http://mathoverflow.net/questions/184682. We refer to [**8**, Chapter 6] for more details.

Proof of Theorem 3. Let $G = \mathrm{Inn}(X)$. The quandle X is doubly transitive and hence G acts primitively on X. Then X is simple by Lemma 8 and therefore X is a conjugacy class of G and G has a trivial center by [**11**, Lemma 1].

Suppose that G is nonsolvable. Let N be the commutator subgroup of G. Since N is the unique minimal normal subgroup of G by [**11**, Lemma 2] and G is nonsolvable, it follows from Theorem 15 that N is a nonregular nonabelian simple group. Hence G is equivalent to a doubly transitive group with simple socle. Such groups are classified, see [**3**, Table 7.4]. With Lemma 7 one excludes from [**3**, Table 7.4] the groups with transitivity ≥ 3. Thus we may assume that G is a doubly transitive group with $F(G) = 1$, where $F(G)$ denotes the Fitting subgroup of G. We claim that $Z(G_x) = 1$. Suppose that $Z(G_x) \neq 1$. Let p be a prime number dividing the order of $Z(G_x)$ and let $g \in Z(G_x)$ be

an element of order p. The case where $p = 2$ follows from Glauberman Z*-theorem [**7**], so we may assume that p is odd. The permutation action of G on X is equivalent to that of G on the conjugacy class of g by conjugation. Since the action is doubly transitive and $F(G) = 1$, no conjugate of g other than itself commutes with g. By [**16**, Corollary 2], there must be a p'-subgroup T of G which is normalized, but not centralized by g. Hence for some $t \in T$, $g^{-1}t^{-1}gt$ is a nontrivial p'-element (i.e. an element of order not a multiple of p). Since $C_G(g)$ is transitive on the remaining conjugates of g, one obtains that for all $h \in G$ the order of $g^{-1}h^{-1}gh$ is not a multiple of p. By [**9**, Theorem D], $O_{p'}(G) \neq 1$, where $O_{p'}(G)$ denotes the largest normal subgroup of G which is a p'-group. Since G is doubly transitive on X, it follows that $G = O_{p'}(G)C_G(g)$. From $g \notin Z(G)$ one obtains that there exist a prime number $q \neq p$ and a q-Sylow subgroup Q of $O_{p'}(G)$ normalized but not centralized by g. A similar argument and [**9**, Theorem D] prove that $[G, g] = [O_{p'}(G), g]$ is a nontrivial q-group of G and thus $O_q(G) \neq 1$, which is a contradiction.

Since G is the inner group of a quandle, we conclude from Lemma 6 and the previous argument that G is solvable. Since X is a simple quandle and its inner group G is solvable, there exist a prime number p and $m \in \mathbb{N}$ such that X is an Alexander quandle of size p^m by [**2**, Theorem 3.9]. □

ACKNOWLEDGEMENTS. The author thanks E. Clark, S. Kamada, A. Lochmann, J. McCarron, H. Tamaru and K. Wada for several helpful comments. Special thanks go to G. Bianco for interesting conversations and to G. Robinson for the group-theoretic argument used in the proof of Theorem 3.

References

[1] N. Andruskiewitsch, F. Fantino, G. A. García and L. Vendramin, On Nichols algebras associated to simple racks, In: Groups, algebras and applications, Contemp. Math., **537**, Amer. Math. Soc., Providence, RI, 2011, 31–56.
[2] N. Andruskiewitsch and M. Graña, From racks to pointed Hopf algebras, Adv. Math., **178** (2003), 177–243.
[3] P. J. Cameron, Finite permutation groups and finite simple groups, Bull. London Math. Soc., **13** (1981), 1–22.
[4] J. S. Carter, D. Jelsovsky, S. Kamada, L. Langford and M. Saito, Quandle cohomology and state-sum invariants of knotted curves and surfaces, Trans. Amer. Math. Soc., **355** (2003), 3947–3989.
[5] W. E. Clark, M. Elhamdadi, X.-d. Hou, M. Saito and T. Yeatman, Connected quandles associated with pointed abelian groups, Pacific J. Math., **264** (2013), 31–60.
[6] W. E. Clark, M. Elhamdadi, M. Saito and T. Yeatman, Quandle colorings of knots and applications, J. Knot Theory Ramifications, **23** (2014), 1450035, 29pp.
[7] G. Glauberman, Central elements in core-free groups, J. Algebra, **4** (1966), 403–420.
[8] D. Gorenstein, Finite groups, Harper & Row Publishers, New York, 1968.
[9] R. M. Guralnick and G. R. Robinson, On extensions of the Baer-Suzuki theorem, Israel J. Math., **82** (1993), 281–297.
[10] C. Hayashi, Canonical forms for operation tables of finite connected quandles, Comm. Algebra, **41** (2013), 3340–3349.
[11] D. Joyce, Simple quandles, J. Algebra, **79** (1982), 307–318.
[12] S. Kamada, H. Tamaru and K. Wada, On classification of quandles of cyclic type, arXiv:1312.6917.
[13] P. Lopes and D. Roseman, On finite racks and quandles, Comm. Algebra, **34** (2006), 371–406.
[14] J. McCarron, Connected quandles with order equal to twice an odd prime, arXiv:1210.2150.

[15] J. McCarron, Small homogeneous quandles, In: Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation, ISSAC '12, New York, USA, 2012, ACM, 257–264.

[16] E. Shult, Some analogues of Glauberman's Z^*-theorem, Proc. Amer. Math. Soc., **17** (1966), 1186–1190.

[17] H. Tamaru, Two-point homogeneous quandles with prime cardinality, J. Math. Soc. Japan, **65** (2013), 1117–1134.

[18] K. Wada, Two-point homogeneous quandles with cardinality of prime power, Hiroshima Math. J., **45** (2015), 165–174.

[19] H. Wielandt, Finite permutation groups, (Translated from the German by R. Bercov), Academic Press, New York, 1964.

Leandro Vendramin

Departamento de Matemática, FCEN
Universidad de Buenos Aires, Pab. I
Ciudad Universitaria (1428) Buenos Aires
Argentina
E-mail: lvendramin@dm.uba.ar