Yokohama Mathematical
Journal Vol. 62, 2016

A LARGE ORBIT IN A FINITE AFFINE QUANDLE

By

Takeshi Kajiwara and Chikara Nakayama

(Received May 6, 2016; Revised September 8, 2016)

Abstract. We prove that the affine case of a conjecture by C. Hayashi that any connected finite quandle has a large orbit.

1. Results

A *quandle* is a set Q with a binary operation $*\colon Q \times Q \to Q$ satisfying the following three axioms.

(1) For any $a \in Q$, $a * a = a$.

(2) For any $b \in Q$, the map $r_b\colon Q \to Q; a \mapsto a * b$ is bijective.

(3) For any $a, b, c \in Q$, $(a * b) * c = (a * c) * (b * c)$.

The conception was first introduced by D. Joyce [2] and S. V. Matveev [4] in the context of knot theory.

A homomorphism of quandles is a map preserving the operations. Note that (3) means that the map r_b in (2) is an automorphism of Q.

Let $\mathrm{Aut}(Q)$ be the group of automorphisms of Q and $\mathrm{Inn}(Q)$ its subgroup generated by $\{r_b \,|\, b \in Q\}$. A quandle Q is said to be *connected* if $\mathrm{Inn}(Q)$ acts transitively on Q.

In the rest of this article, we only treat finite quandles. Let Q be a finite quandle. For $b \in Q$, let C_b be the cycle type of r_b as a permutation of Q defined by r_b. The multiple set of C_b for the elements b of Q is called the *profile* of Q ([3]). For a connected quandle Q, since C_b is independent of b, the profile reduces to a single cycle type $\{1, \ell_1, \ell_2, \ldots, \ell_k\}$. (Note that any r_b has a fixed point by the axiom (1).) So we denote the profile of Q just by the cycle type of r_b for any $b \in Q$.

C. Hayashi [1] conjectured the following.

Conjecture 1.1. Let Q be a connected finite quandle. Let $\{1, \ell_1, \ell_2, \ldots, \ell_k\}$ with $1 \le \ell_1 \le \ell_2 \le \cdots \le \ell_k$ be its profile. Then any ℓ_i divides ℓ_k.

2010 Mathematics Subject Classification: Primary 20N02; Secondary 20K01, 20K30
Key words and phrases: finite quandle, affine quandle, profile

Let X be a finite set X, and let $\sigma\colon X \to X$ be a bijection of order n (in the permutation group of X). An orbit of σ in X is said to be *large* if it is of cardinality n. Then the conclusion of the above conjecture is equivalent to that there is a large orbit for r_b for one (hence for all) $b \in Q$.

In this paper, we prove this conjecture in the affine case. Recall that a quandle is *affine* if there are an abelian group M and an automorphism T of M such that Q is isomorphic as a quandle to $\mathrm{Aff}\,(M,T) := (M,*)$, where $x*y = T(x)+(1-T)(y)$ $(x, y \in M)$.

Our theorem is a slight generalization of the affine case of the conjecture:

Theorem 1.2. *Let Q be an affine quandle of finite order. Then there is an element $b \in Q$ such that there is a large orbit for r_b.*

Since, in the case of $Q = \mathrm{Aff}\,(M,T)$, r_0 coincides with T (where 0 is the unit element of M), this theorem is reduced to the following group-theoretic statement.

Proposition 1.3. *Let M be a finite abelian group, and let T be a group automorphism of M. Then there is a large orbit for T.*

In the next section, we give a proof by using the elementary divisor theory.

Acknowledgments. The first author is partially supported by JSPS, Kakenhi (C) No. 24540035. The second author is partially supported by JSPS, Kakenhi (C) No. 22540011, No. 16K05093. The authors thank the referee for valuable comments.

2. Proofs

We prove Proposition 1.3, which implies Theorem 1.2 and the affine case of Conjecture 1.1, as was explained in the previous section. Let M be a finite abelian group and let T be an automorphism of M.

2.1. First we claim that it is enough to show the case where M is a p-group for some prime p. To see this, we identify M with the direct sum $\bigoplus M_p$ of its p-primary parts M_p, where p runs over the set of all primes. For each prime p, let T_p be the automorphism of M_p induced by T. Then the given automorphism T of M can be identified with the direct sum $\bigoplus T_p$ of T_p on M_p.

Assume that Proposition 1.3 is valid for M_p for every p. Then, we have a large orbit O_p for T_p in M_p for any p. Let x_p be an element of O_p for each p. We prove that the orbit through the element $(x_p)_p$ of the direct sum $\bigoplus M_p$, whose component for a prime p is x_p, is a large orbit for $\bigoplus T_p$ in $\bigoplus M_p$. Let n_p be the order of T_p. Then the order of $\bigoplus T_p$ is the least common multiple of all n_p. On the other hand, the cardinality of O_p is n_p. Hence the cardinality of the orbit through $(x_p)_p$ is also the least common multiple of all n_p. Therefore, this orbit is a large orbit. Hence Proposition 1.3 is valid for M, which completes the proof of the claim.

Thus we may assume that M is a p-group for a prime p. In the remaining part of the proof, we fix a prime p and we assume that M is a p-group.

2.2. Next we treat the case where $pM = 0$. In this case, Proposition 1.3 is a direct consequence of the elementary divisor theory as follows. But we prove a stronger statement for later use. In this case, M is regarded as an $\mathbf{F}_p[t]$-module, where t is an indeterminate acting via the given automorphism T. Hence, by the elementary divisor theory, M is isomorphic to, as an $\mathbf{F}_p[t]$-module, $\bigoplus_{i=1}^{d} \mathbf{F}_p[t]/(e_i)$, where $e_1, \ldots, e_d$ are polynomials over $\mathbf{F}_p$ satisfying $e_1 \mid e_2 \mid \cdots \mid e_d$. Here, $f \mid g$ means that f divides g. In the following, we identify M with this $\mathbf{F}_p[t]$-module. Then the order of the automorphism T of M is the order of t in the unit group of the last factor $\mathbf{F}_p[t]/(e_d)$, regarded as a commutative ring. Hence, for any element of the form $(*, *, \ldots, *, 1)$, that is, any element whose last component is 1, the orbit through it is a large orbit of T in M. Further, the union of all large orbits generates M as an abelian group because this union includes all elements of the form $(*, *, \ldots, *, t^j)$ $(j \geq 0)$, that is, the elements whose last component is a power of t. So we have just proved the following.

$(*)$ If $pM = 0$, a large orbit exists and furthermore the union of all large orbits generates M as an abelian group.

The general p-group case reduces to the case where $pM = 0$ as follows. Recall that M is a finite abelian p-group. Let $\overline{M} = M/pM$.

Lemma 2.3. *The kernel of the natural homomorphism* $\operatorname{Aut} M \to \operatorname{Aut} \overline{M}$ *is a* p*-group, where* Aut *means the group of group automorphisms.*

Proof. Let $S\colon M \to M$ be an automorphism of M which induces the identity of $\overline{M}$. We identify M with the direct sum of $\mathbf{Z}/p^{k_i}\mathbf{Z}$ $(1 \leq i \leq l, k_i > 0)$. Then, we represent S as an $l \times l$-matrix $1_l + pA$ whose (i,j)-coefficient is an element of $\operatorname{Hom}(\mathbf{Z}/p^{k_i}\mathbf{Z}, \mathbf{Z}/p^{k_j}\mathbf{Z})$ $(1 \leq i,j \leq l)$. Here 1_l is the unit matrix. Let k be the maximum of the k_i $(1 \leq i \leq l)$. Then there is an invertible matrix $1_l + p\tilde{A}$ with coefficients in $\mathbf{Z}/p^k\mathbf{Z}$ which lifts $1_l + pA$, that is, for any $1 \leq i, j \leq l$, the (i,j)-component of $1_l + p\tilde{A}$ induces the (i,j)-component of $1_l + pA$. By induction, we see $(1_l + p\tilde{A})^{p^N} \equiv 1 \bmod p^{N+1}$ for $N \geq 1$. Hence the order of $1_l + p\tilde{A}$ is a divisor of p^{k-1}, which implies that the order of S is also a power of p. $\square$

2.4. We prove the case of Proposition 1.3 where M is a general p-group. Let $\overline{T}$ be the automorphism of $\overline{M}$ induced by T. Let $n = p^a m$ be the order of T, where a is a nonnegative integer, and m is an integer prime to p. Then, by Lemma 2.3, the order of $\overline{T}$ is $p^b m$ for some $b \le a$. By $(*)$, there is a large orbit for $\overline{T}$ in $\overline{M}$. Consider all large orbits $O_1, \dots, O_l$ for $\overline{T}$ in $\overline{M}$. Take an element x_i of O_i for each i $(1 \le i \le l)$. Let $\tilde{x}_i \in M$ be an element of M whose image in $\overline{M}$ is x_i. The cardinality of the orbit $\tilde{O}_i$ through each $\tilde{x}_i$ is $p^{c_i} m$ for some c_i with $b \le c_i \le a$ because the cardinality of O_i is $p^b m$.

In order to prove that some c_i is a, we argue by contradiction. Assume that any c_i is strictly less than a, that is, any $\tilde{x}_i$ satisfies $T^{p^{a-1}m}\tilde{x}_i = \tilde{x}_i$. Then, $T^{p^{a-1}m}(x) = x$ for any element x belonging to the union U of the orbits $\tilde{O}_i$. This union U generates the abelian group M. In fact, let N be the subgroup of M generated by U. The image of U in $\overline{M}$ generates $\overline{M}$ by $(*)$. That is, we have $M = N + pM$ so that $M = N + p(N + pM) = N + p^2M = N + p^3M = \cdots = N$. (Of course, we can use here Nakayama's lemma.) Hence $T^{p^{a-1}m} = 1$, which contradicts the assumption that the order of T is $n = p^a m$. Therefore, there is an index i such that $c_i = a$, that is, the orbit $\tilde{O}_i$ is large. This completes the proof of Proposition 1.3.

Example 2.5. Let $M = \mathbf{Z}/35\mathbf{Z} = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{34}\}$, and let T be an automorphism $M \to M$ defined by $T(x) = 2x$ $(x \in M)$. Then, the order of T is 12, and the orbit through $\overline{1}$ is a large orbit $\{\overline{1}, \overline{2}, \overline{4}, \overline{8}, \overline{16}, \overline{32}, \overline{29}, \overline{23}, \overline{11}, \overline{22}, \overline{9}, \overline{18}\}$. The orbit through $\overline{3}$ is another large orbit $\{\overline{3}, \overline{6}, \overline{12}, \overline{24}, \overline{13}, \overline{26}, \overline{17}, \overline{34}, \overline{33}, \overline{31}, \overline{27}, \overline{19}\}$. The other orbits $\{\overline{0}\}$, $\{\overline{5}, \overline{10}, \overline{20}\}$, $\{\overline{15}, \overline{30}, \overline{25}\}$, $\{\overline{7}, \overline{14}, \overline{28}, \overline{21}\}$ are not large.

Let Q be a connected affine quandle Aff (M, T), that is, $Q = (M, *)$, where $x * y = 2x - y$. Then, since $r_{\overline{0}} = T$, by the above observation, the profile of Q is $\{1, 3, 3, 4, 12, 12\}$.

Example 2.6. Let $M = \mathbf{Z}/9\mathbf{Z} \oplus \mathbf{Z}/27\mathbf{Z}$, and let T be an automorphism $M \to M$ defined by $T((x, y)) = (2x + y, 2y)$ $((x, y) \in M)$. Then, the order of T is 18. There are nine large orbits, that are the orbits through $(x, \overline{1})$ for some $x \in \mathbf{Z}/9\mathbf{Z}$. The other orbits are: $\{(\overline{0}, \overline{0})\}$; the orbit through $(\overline{3}, \overline{0})$ whose cardinality is 2; the three orbits through $(x, \overline{9})$ $(x = \overline{0}, \overline{3}, \overline{6})$ each of whose cardinality is 2; three orbits through $(\overline{1}, \overline{0})$, through $(\overline{1}, \overline{9})$, and through $(\overline{2}, \overline{9})$, respectively, each of whose cardinality is 6; and the nine orbits through $(x, \overline{3})$ $(x \in \mathbf{Z}/9\mathbf{Z})$ each of whose cardinality is 6.

Let Q be a connected affine quandle Aff (M, T). Then, since $r_{(\overline{0},\overline{0})} = T$, by the above observation, the profile of Q is

$$\{1, 2, 2, 2, 2, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 18, 18, 18, 18, 18, 18, 18, 18, 18\}.$$

References

[1] Hayashi, C., Canonical forms for operation tables of finite connected quandles, *Communications in Algebra* **41** (9) (2013), 3340–3349.

[2] Joyce, D., A classifying invariant of knots, the knot quandle, *Journal of Pure and Applied Algebra*, **23** (1) (1982), 37–65.

[3] Lopes, P. and Roseman, D., On finite racks and quandles, *Communications in Algebra*, **34** (1) (2006), 371–406.

[4] Matveev, S. V., Distributive groupoids in knot theory, *Sbornik: Mathematics*, **47** (1) (1984), 73–83.

Takeshi Kajiwara
Department of Applied mathematics
Faculty of Engineering
Yokohama National University
Hodogaya-ku, Yokohama 240-8501
Japan
`kajiwara@ynu.ac.jp`

Chikara Nakayama
Department of Economics
Hitotsubashi University
2-1 Naka, Kunitachi, Tokyo 186-8601
Japan
`c.nakayama@r.hit-u.ac.jp`