MATHEMATICS OF COMPUTATION
https://doi.org/10.1090/mcom/3409
Article electronically published on January 7, 2019

ENUMERATION OF RACKS AND QUANDLES UP TO ISOMORPHISM

PETR VOJTĚCHOVSKÝ AND SEUNG YEOP YANG

Abstract. Racks and quandles are prominent set-theoretical solutions of the Yang-Baxter equation. We enumerate racks and quandles of orders $n \leq 13$ up to isomorphism, improving upon the previously known results for $n \leq 8$ and $n \leq 9$, respectively. The enumeration is based on the classification of subgroups of small symmetric groups up to conjugation, on a representation of racks and quandles in symmetric groups due to Joyce and Blackburn, and on a number of theoretical and computational observations concerning the representation. We explicitly find representatives of isomorphism types of racks of order ≤ 11 and quandles of order ≤ 12. For the remaining orders we merely count the isomorphism types, relying in part on the enumeration of 2-reductive racks and 2-reductive quandles due to Jedlička, Pilitowska, Stanovský, and Zamojska-Dzienio.

1. Introduction

A groupoid $(X, *)$ is a *left quasigroup* if every left translation

$$L_x : X \to X, \quad y \mapsto yL_x = x * y$$

is a bijection of X. A left quasigroup is a *rack* if the left self-distributive law

$$x * (y * z) = (x * y) * (x * z)$$

holds. A rack is a *quandle* if it is idempotent, i.e., if

$$x * x = x$$

holds.

Racks and quandles form well-studied classes of set-theoretical solutions of the Yang-Baxter equation [4]. Moreover, racks and quandles appear in low-dimensional topology as invariants of oriented knots and links [12, 13]. The textbook [6] offers a friendly introduction to the theory of quandles.

In this paper we enumerate racks and quandles of order $n \leq 13$ up to isomorphism, improving upon previously known enumerations for $n \leq 8$ for racks and $n \leq 9$ for quandles. We also make all isomorphism types of racks of order $n \leq 11$ and quandles of order $n \leq 12$ available online.

Received by the editor May 22, 2018, and, in revised form, September 25, 2018.
2010 *Mathematics Subject Classification.* Primary 16T25, 20N05, 57M27.
Key words and phrases. Rack, quandle, 2-reductive rack, medial rack, Yang-Baxter equation, enumeration, isomorphism search, oriented knot, subgroups of symmetric group.
The first author was supported by a 2015 PROF grant of the University of Denver.

1.1. **Notation.** Let X be a nonempty set and let S_X be the symmetric group on X. If a group G acts on X and $x \in X$, we denote by xG the orbit of x, by G_x the stabilizer of x, and by X/G a complete set of orbit representatives. The set X/G is not uniquely determined but we will assume that one such set has been fixed whenever X and G are given.

For f, $g \in S_X$ and $G \leq S_X$, we let $g^f = f^{-1}gf$, $G^f = f^{-1}Gf$, and $f^G = \{f^g : g \in G\}$. As usual, let $C_G(H)$ and $N_G(H)$ be the centralizer and the normalizer of $H \subseteq S_X$ in G.

For a groupoid $(X, *)$ and $x \in X$, let L_x or L_x^* be the left translation by x, the latter notation being used when we need to keep track of the operation. Similarly, R_x or R_x^* will denote the right translation by x in $(X, *)$. The automorphism group of $(X, *)$ will be denoted by $\mathrm{Aut}(X, *)$.

For a left quasigroup $(X, *)$, let

$$\mathrm{Mlt}_\ell(X, *) = \langle L_x : x \in X \rangle \leq S_X,$$
$$\mathrm{Dis}(X, *) = \langle L_x^{-1} L_y : x, y \in X \rangle \leq \mathrm{Mlt}_\ell(X, *)$$

be the *left multiplication group* and the *displacement group* of $(X, *)$, respectively.[1] Note that racks can be equivalently defined as groupoids $(X, *)$ satisfying $\mathrm{Mlt}_\ell(X, *) \leq \mathrm{Aut}(X, *)$.

A rack $(X, *)$ is said to be 2-*reductive* if

$$(x * u) * v = (y * u) * v \tag{1.1}$$

holds for every x, y, u, $v \in X$. A rack that is not 2-reductive will be called *non-2-reductive*.

It is not difficult to see that the following conditions are equivalent for a rack $(X, *)$:

- $(X, *)$ is 2-reductive, that is, the identity (1.1) holds,
- $(X, *)$ satisfies the identity $(x * u) * v = u * v$,
- $\mathrm{Mlt}_\ell(X, *)$ is commutative.

A rack $(X, *)$ is *medial* if it satisfies the medial law

$$(x * u) * (v * y) = (x * v) * (u * y).$$

One can show (see for instance [10, Proposition 2.4]) that a rack $(X, *)$ is medial if and only if $\mathrm{Dis}(X, *)$ is commutative. In particular, every 2-reductive rack is medial.

A medial rack $(X, *)$ is 2-reductive if and only if it satisfies the identity $(x*y)*y = y * y$. Therefore, a medial quandle $(X, *)$ is 2-reductive if and only if it satisfies the identity $(x * y) * y = y$. This last identity is used in [11] as a definition of 2-reductivity in the context of medial quandles.

1.2. **Asymptotic growth.** The asymptotic growth of racks and quandles is known. Due to the nature of the estimate, it does not matter whether the algebras in question are counted up to isomorphism or absolutely on a fixed set.

Denote by $r(n)$ (resp., $q(n)$) the number of racks (resp., quandles) of order n up to isomorphism. Blackburn [2] proved that there are constants $c_1 = 1/4$ and

[1] In rack and quandle literature, the left multiplication group $\mathrm{Mlt}_\ell(X, *)$ of a rack $(X, *)$ is often denoted by $\mathrm{Inn}(X, *)$ and is called the *inner automorphism group* of $(X, *)$, a terminology that is in conflict with older conventions for quasigroups and loops [3].

$c_2 = (1/6)\log_2(24) + (1/2)\log_2(3)$ such that for every $\varepsilon > 0$ and for all sufficiently large orders n we have

$$2^{c_1 n^2 - \varepsilon} \leq q(n) \leq r(n) \leq 2^{c_2 n^2 + \varepsilon}.$$

The lower bound is obtained by exhibiting a large class of racks with $\mathrm{Mlt}_\ell(X, *)$ isomorphic to an elementary abelian 2-group, while the upper bound is based on an estimate for the number of subgroups of symmetric groups and on a relatively straightforward analysis of partitions of n. In the same paper, Blackburn also developed a representation of racks and quandles in symmetric groups that deserves to be better known and that we recall in Section 3.

Ashford and Riordan [1] improved Blackburn's upper bound and showed that for every $\varepsilon > 0$ and for all sufficiently large orders n we have

$$2^{n^2/4 - \varepsilon} \leq q(n) \leq r(n) \leq 2^{n^2/4 + \varepsilon}.$$

The main idea for their upper bound is harder to convey. Roughly speaking, a small amount of global information partitions the class of all racks defined on $\{1, \ldots, n\}$ into relatively small subsets, and the racks in each of those subsets can then be fully determined by an additional small set of parameters.

1.3. **Exact enumeration.** The exact values of $r(n)$ and $q(n)$ are known only for very small values of n.

A brute-force approach (constructing one row of the multiplication table at a time and checking whether the resulting partial groupoid is a partial rack) is feasible for $n \leq 7$ or so. Henderson, Macedo, and Nelson determined $q(n)$ for $n \leq 8$ [8]. McCarron reported the values $r(n)$ for $n \leq 8$ and $q(n)$ for $n \leq 9$ in the Online Encyclopedia of Integer Sequences [14]. Elhamdadi, Macquarrie, and Restrepo [5] also calculated the values $q(n)$ for $n \leq 9$ while investigating automorphism groups of quandles.

Jedlička, Pilitowska, Stanovský, and Zamojska-Dzienio [11] developed a theory of so-called affine meshes in order to construct and enumerate medial and 2-reductive quandles of small orders. This allowed them to count medial quandles of order $n \leq 13$ and 2-reductive quandles of order $n \leq 16$ up to isomorphism.

A quandle is said to be *connected* if its left multiplication group acts transitively on the underlying set. All connected quandles of order less than 36 (resp., 48) were obtained by Vendramin [15] (resp., in [10]). A library of connected quandles of order less than 48 is available in `Rig`, a `GAP` [7] package developed by Vendramin.

1.4. **Summary of results.** Our enumerative results are summarized in Tables 1 and 2. In Table 1, $r(n)$ (resp., $r_{\mathrm{med}}(n)$, $r_{\text{2-red}}(n)$ and $r_{\text{non-2-red}}(n)$) is the number of racks (resp., medial racks, 2-reductive racks, and non-2-reductive racks) of order n up to isomorphism. Obviously, $r(n) = r_{\text{2-red}}(n) + r_{\text{non-2-red}}(n)$, but we report all three numbers for the convenience of the reader, to better indicate which results are new, and for future reference. The notation in Table 2 is analogous but for quandles instead of racks.

New results are reported in shaded cells. If a number in the tables is in roman font, representatives of isomorphism types can be downloaded from the website of the first author. If a number in the tables is in italics, representatives of isomorphism types are not available. The numbers that are both in unshaded cells and it italics are either taken from [11] or they were provided to us by Jedlička in personal communication. For instance, we constructed 3163262 representatives of

TABLE 1. The number of racks $r(n)$, medial racks $r_{\text{med}}(n)$, 2-reductive racks $r_{\text{2-red}}(n)$, and non-2-reductive racks $r_{\text{non-2-red}}(n)$ of order n up to isomorphism.

n	1	2	3	4	5	6	7
$r(n)$	1	2	6	19	74	353	2080
$r_{\text{med}}(n)$	1	2	6	18	68	329	1965
$r_{\text{2-red}}(n)$	1	2	5	17	65	323	1960
$r_{\text{non-2-red}}(n)$	0	0	1	2	9	30	120
n	8	9	10	11	12	13	14
$r(n)$	16023	159526	2093244	36265070	*836395102*	*25794670618*	?
$r_{\text{med}}(n)$	15455	155902	2064870	35982366	*832699635*	*25731050872*	?
$r_{\text{2-red}}(n)$	15421	155889	2064688	35982357	*832698007*	*25731050861*	*1067863092309*
$r_{\text{non-2-red}}(n)$	602	3637	28556	282713	3697095	63619757	?

TABLE 2. The number of quandles $q(n)$, medial quandles $q_{\text{med}}(n)$, 2-reductive quandles $q_{\text{2-red}}(n)$, and non-2-reductive quandles $q_{\text{non-2-red}}(n)$ of order n up to isomorphism.

n	1	2	3	4	5	6	7
$q(n)$	1	1	3	7	22	73	298
$q_{\text{med}}(n)$	1	1	3	6	18	58	251
$q_{\text{2-red}}(n)$	1	1	2	5	15	55	246
$q_{\text{non-2-red}}(n)$	0	0	1	2	7	18	52
n	8	9	10	11	12	13	14
$q(n)$	1581	11079	102771	1275419	21101335	*469250886*	?
$q_{\text{med}}(n)$	1410	10311	98577	1246488	20837439	*466087635*	?
$q_{\text{2-red}}(n)$	1398	10301	98532	1246479	20837171	*466087624*	*13943041873*
$q_{\text{non-2-red}}(n)$	183	778	4239	28940	264164	3163262	?

isomorphism types of non-2-reductive quandles of order 13, the number 466087624 of 2-reductive quandles of order 13 is taken from [11], resulting in the 469250886 quandles of order 13 up to isomorphism.

1.5. **Commented outline of the paper.** In Section 2 we show that a classification of left quasigroups up to isomorphism defined on X can be accomplished by independent classifications of left quasigroups with a given left multiplication group $G \leq S_X$. Crucially, it suffices to consider subgroups G of S_X up to conjugation in S_X, rather than all subgroups of S_X.

The first step of our algorithm therefore consists of a determination of subgroups of the symmetric group S_n up to conjugation. This is a nontrivial task. Fortunately, `GAP` [7] can determine these subgroups for $n \leq 12$ in a matter of minutes and for $n = 13$ in a matter of a few hours. The results are summarized in Table 3. The state of the art results in this area are due to Holt [9] who counted (but did not list) subgroups of S_n for $n \leq 18$, both absolutely and up to conjugation in S_n. To illustrate Holt's results, there are 7598016157515302757 subgroups of S_{18} partitioned into 7274651 conjugacy classes.

TABLE 3. The number $a(n)$ of subgroups of the symmetric group S_n up to conjugacy in S_n, and the number $b(n)$ of nonabelian subgroups of S_n up to conjugacy.

n	1	2	3	4	5	6	7	8	9	10	11	12	13
$a(n)$	1	2	4	11	19	56	96	296	554	1593	3094	10723	20832
$b(n)$	0	0	1	4	10	36	70	235	472	1413	2858	10129	20070

In Section 3 we prove that there is a one-to-one correspondence between racks (resp., quandles) defined on X and so-called rack envelopes (resp., quandle envelopes) defined on X. A *rack envelope* (resp., *quandle envelope*) is a tuple

$$(G, (\lambda_x : x \in X/G))$$

such that $G \leq S_X$, $\lambda_x \in C_G(G_x)$ (resp., $\lambda_x \in Z(G_x)$) for every $x \in X/G$, and $\langle \bigcup_{x \in X/G} \lambda_x^G \rangle = G$. If the last condition is dropped, we speak of rack and quandle folders. It does not seem to be easy to determine without an explicit check if a given folder is in fact an envelope, greatly complicating our enumeration.

The main idea behind rack and quandle envelopes is due to Blackburn [2, Section 2] who attributed it in part to Joyce. A special case of quandle envelopes for connected quandles was described in [10], where the "envelope" terminology for quandles originated. Although we have independently rediscovered Blackburn's representation of racks and quandles while working on this project, the full credit for the results of Subsection 3.1 should go to Blackburn [2].

The isomorphism problem for rack and quandle envelopes is solved in Subsection 3.2 in terms of an explicit group action (3.2) of the normalizer $N_{S_X}(G)$. The same group also acts on rack and quandle folders, where the orbits of the action are easier to understand (see Section 5).

For any $G \leq S_X$ the set of rack/quandle folders $(G, (\lambda_x : x \in X/G))$ is nonempty, containing at least the trivial folder with $\lambda_x = 1$ for every $x \in X/G$. Call $G \leq S_X$ *rack/quandle admissible* if the set of rack/quandle envelopes over G is also nonempty. Equivalently, $G \leq S_X$ is rack/quandle admissible if and only if there is a rack/quandle $(X, *)$ such that $\mathrm{Mlt}_\ell(X, *) = G$. We touch upon the question "Which subgroups $G \leq S_X$ are rack/quandle admissible?" in Subsection 3.3 but further investigation would be of considerable interest.

Our algorithm is presented in Section 4, first in a simplified form in Subsection 4.1 and then with essential improvements. For racks, given a subgroup G of S_n, the algorithm returns orbit representatives of the action (3.2) of the normalizer $N_{S_n}(G)$ on the parameter space

$$\mathrm{Fol}_r(G) = \prod_{x \in X/G} C_G(G_x)$$

consisting of rack folders, disqualifying those folders that are not envelopes. For quandles, we use quandle folders

$$\mathrm{Fol}_q(G) = \prod_{x \in X/G} Z(G_x)$$

as the parameter space.

The main obstacle in the algorithm is the fact that the parameter spaces can be quite large. For instance, there exists a subgroup G of S_{12} isomorphic to an elementary abelian 2-group for which $\mathrm{Fol}_q(G)$ has over one billion elements. The default orbit-stabilizer theorem of `GAP` cannot cope with spaces this large since it first attempts to convert the action into a permutation action. Nevertheless, it is possible to determine the orbits by employing careful indexing of the space of rack/quandle folders, using one bit of memory for every folder. This is described in Subsection 4.2.

We can further take advantage of the indexing (and other improvements) to minimize storage space for the library of racks and quandles. For instance, the library of 36265070 racks of order 11 is stored in a compressed file of approximately 5.7 megabytes, with each rack requiring only 1.25 bits of storage on average. More details are given in the actual library.

The action (3.2) is of local character in the following sense. If $f \in N_{S_X}(G)$ and

$$(\kappa_x : x \in X/G) = (\lambda_x : x \in X/G)f,$$

a given κ_x can be calculated once a single λ_z is known, namely the λ_z with z in the same orbit of G as xf^{-1}. This observation is exploited in Subsection 4.3, where we show how to precalculate the action to crucially speed up the algorithm.

The algorithm is powerful enough to construct all isomorphism types of racks of order $n \leq 8$ and quandles of order $n \leq 9$ in a matter of seconds, verifying the counts reported in [14]. It takes about a day to determine isomorphism types of racks of order 11 and about three days to determine isomorphism types of quandles of order 12.

The algorithm spends most of its running time dealing with elementary abelian 2-groups contained in S_n and it is finally overwhelmed while trying to determine $r(12)$ and/or $q(13)$. Fortunately, as far as counting of racks and quandles is concerned, all abelian subgroups of S_n can be excluded from the search since they yield precisely 2-reductive racks and 2-reductive quandles, which can be counted more efficiently by the methods of [11] using a different representation and Burnside's Lemma. As we have already mentioned, Jedlička provided us with the numbers $r_{\text{2-red}}(n)$ and $q_{\text{2-red}}(n)$ for $n \leq 14$. (We have independently verified $r_{\text{2-red}}(n)$ for $n \leq 11$ and $q_{\text{2-red}}(n)$ for $n \leq 12$.)

To determine $r(12)$, $r(13)$, and $q(13)$, we therefore consider only nonabelian subgroups of symmetric groups and obtain $r_{\text{non-2-red}}(12)$, $r_{\text{non-2-red}}(13)$, and $q_{\text{non-2-red}}(13)$ together with the corresponding representatives of isomorphism types. Memory management remains important even in the nonabelian case. For instance, there is a nonabelian subgroup G of S_{13} for which $\mathrm{Fol}_r(G)$ has over two billion elements. It took about two weeks of computing time to determine the most difficult case, $r_{\text{non-2-red}}(13)$, and thus $r(13)$.

To determine $r_{\text{med}}(n)$, we explicitly construct all non-2-reductive racks $(X, *)$ of order n and count only those with $\mathrm{Dis}(X, *)$ abelian. We add this count to $r_{\text{2-red}}(n)$ since every 2-reductive rack is medial. We proceed similarly for medial quandles.

In Section 5 we show how to efficiently count the orbits of $N_{S_X}(G)$ on the space of rack or quandle folders. The problem that we really need to solve, namely efficiently counting orbits of $N_{S_X}(G)$ on the space of rack or quandle envelopes, remains open.

Recall that if a finite group F acts on a set Y and $\mathrm{Fix}(Y,f)=\{y\in Y : yf=y\}$ is the set of f-invariant elements of Y, then Burnside's Lemma states that

$$|Y/F|=\frac{1}{|F|}\sum_{f\in F}|\mathrm{Fix}(Y,f)|.$$

In our setting we let $F=N_{S_X}(G)$ and $Y=\mathrm{Fol}_r(G)$, the quandle case being similar. For every $f\in N_{S_X}(G)$ we then construct a certain $|X/G|$-partite digraph $\Gamma_r(G,f)$ that encodes the action of $\langle f\rangle$ on Y. We describe the structure of $\Gamma_r(G,f)$ in detail and prove that the elements of $\mathrm{Fix}(Y,f)$ are in one-to-one correspondence with unions of certain short directed cycles of $\Gamma_r(G,f)$. These short cycles can be easily counted as long as X is not too large.

The paper concludes with several open problems.

2. Isomorphisms and conjugation for left quasigroups

For a subgroup G of S_X let $\mathcal{L}(G)$ be the set of all left quasigroups defined on X whose left multiplication group is equal to G.

The following result is likely well known and it applies to the special cases of racks and quandles.

Proposition 2.1. *Let X be a set, and let $(X,*)$ and $(X,\circ)$ be left quasigroups. Then:*

(i) *A bijection $f\in S_X$ is an isomorphism $f:(X,*)\to(X,\circ)$ if and only if $L^\circ_{xf}=(L^*_x)^f$ for every $x\in X$.*
(ii) *If $f:(X,*)\to(X,\circ)$ is an isomorphism, then $\mathrm{Mlt}_\ell(X,\circ)=(\mathrm{Mlt}_\ell(X,*))^f$.*
(iii) *If G, H are subgroups of S_X that are not conjugate, then no left quasigroup in $\mathcal{L}(G)$ is isomorphic to a left quasigroup in $\mathcal{L}(H)$.*
(iv) *If G, H are conjugate subgroups of S_X, then $\mathcal{L}(G)$ and $\mathcal{L}(H)$ contain the same isomorphism types of left quasigroups.*

Proof. (i) We have $xf\circ yf=(x*y)f$ for every x, $y\in X$ if and only if $yL^\circ_{xf}=xf\circ y=(x*yf^{-1})f=yf^{-1}L^*_xf=y(L^*_x)^f$ for every x, $y\in X$.

(ii) Using (i), we have $\mathrm{Mlt}_\ell(X,\circ)=\langle L^\circ_x : x\in X\rangle=\langle (L^*_{xf^{-1}})^f : x\in X\rangle=\langle L^*_{xf^{-1}} : x\in X\rangle^f=\langle L^*_x : x\in X\rangle^f=(\mathrm{Mlt}_\ell(X,*))^f$. Part (iii) now follows, too.

For (iv), suppose that $H=G^f$ for some $f\in S_X$ and let $(X,*)\in\mathcal{L}(G)$. Then $f:(X,*)\to(X,\circ)$ is an isomorphism, where $(X,\circ)$ is defined by $x\circ y=(xf^{-1}*yf^{-1})f$. Since $\mathrm{Mlt}_\ell(X,\circ)=(\mathrm{Mlt}_\ell(X,*))^f=G^f=H$ by (ii), we have $(X,\circ)\in\mathcal{L}(H)$. This shows $\mathcal{L}(G)\subseteq\mathcal{L}(H)$ and the other inclusion is proved analogously. □

Consequently, to classify left quasigroups defined on X up to isomorphism, it suffices to:

- calculate subgroups of S_X up to conjugacy,
- for each such subgroup, G, determine the isomorphism types in $\mathcal{L}(G)$,
- return the (necessarily disjoint) union of the isomorphism types.

Proposition 2.1 immediately implies the following corollary.

Corollary 2.2. *Let $(X,*)$ and $(X,\circ)$ be left quasigroups such that $\mathrm{Mlt}_\ell(X,*)=\mathrm{Mlt}_\ell(X,\circ)=G$. Then every isomorphism $f:(X,*)\to(X,\circ)$ satisfies $f\in N_{S_X}(G)$.*

3. Rack and quandle envelopes up to isomorphism

In this section we obtain a one-to-one correspondence between racks and quandles defined on X and certain configurations in S_X, called rack and quandle envelopes. We also solve the isomorphism problem for envelopes.

3.1. **Rack and quandle envelopes.** For a rack $(X,*)$ with $\mathrm{Mlt}_\ell(X,*)=G$ let

$$\mathbf{E}(X,*)=(G,(L_x : x\in X/G)).$$

Lemma 3.1. *Let $(X,*)$ be a rack and $G=\mathrm{Mlt}_\ell(X,*)$. Then $(X,*)$ is determined by $\mathbf{E}(X,*)$. Moreover, $L_x\in C_G(G_x)$ for every $x\in X$ and $G=\langle\bigcup_{x\in X/G} L_x^G\rangle$. If $(X,*)$ is a quandle, then $L_x\in Z(G_x)$ for every $x\in X$.*

Proof. If $x\in X/G$ and $y\in xG$ are given, let $g\in G$ be such that $xg=y$. Since $g\in G=\mathrm{Mlt}_\ell(X,*)\leq \mathrm{Aut}(X,*)$, we have $(L_x)^g=L_{xg}=L_y$. Hence $(X,*)$ is determined by $\mathbf{E}(X,*)$. Moreover, $L_x\in C_G(G_x)$ since for any $g\in G_x$ we have $(L_x)^g=L_{xg}=L_x$. Finally, $G=\mathrm{Mlt}_\ell(X,*)=\langle L_x : x\in X\rangle=\langle (L_x)^g : x\in X/G,\ g\in G\rangle=\langle\bigcup_{x\in X/G} L_x^G\rangle$. If $(X,*)$ is a quandle, we have also $L_x\in G_x$ (since $x*x=x$) and thus $L_x\in Z(G_x)$. □

Definition 3.2. Let $G\leq S_X$. Then $(G,(\lambda_x : x\in X/G))$ is a *rack folder* (resp., *quandle folder*) if $\lambda_x\in C_G(G_x)$ (resp., $\lambda_x\in Z(G_x)$) for every $x\in X/G$. A rack folder (resp., quandle folder) is a *rack envelope* (resp., *quandle envelope*) if $\langle\bigcup_{x\in X/G}\lambda_x^G\rangle=G$.

Given $G\leq S_X$ and $\Lambda=(\lambda_x\in G : x\in X/G)$, we attempt to define a groupoid

$$\mathbf{R}(G,\Lambda)=(X,*)$$

by setting

$$L_y=(\lambda_x)^{g_y},$$

where $x\in X/G$, $y\in xG$, and g_y is any element of G such that $xg_y=y$.

Proposition 3.3. *Let $G\leq S_X$, $\Lambda=(\lambda_x\in G : x\in X/G)$, and $(X,*)=\mathbf{R}(G,\Lambda)$. Then:*

(i) *$(X,*)$ is well-defined if and only if (G,Λ) is a rack folder, in which case $(X,*)$ is a rack satisfying $L_x=\lambda_x$ for every $x\in X/G$ and $\mathrm{Mlt}_\ell(X,*)=\langle\bigcup_{x\in X/G}\lambda_x^G\rangle\leq G$.*

(ii) *$(X,*)$ is a well-defined quandle if and only if (G,Λ) is a quandle folder.*

Proof. (i) Suppose that $(X,*)$ is well-defined and let $x\in X/G$. For every $g_x\in G_x$ we have $\lambda_x^{g_x}=L_x=\lambda_x$, where the latter equality follows by taking $g_x=1$. Thus $\lambda_x\in C_G(G_x)$. Conversely, suppose that $\lambda_x\in C_G(G_x)$ holds for every $x\in X/G$ and let g, $h\in G$ be such that $xg=xh$. Since $gh^{-1}\in G_x$, we have $\lambda_x^{gh^{-1}}=\lambda_x$, that is, $\lambda_x^g=\lambda_x^h$, and $(X,*)$ is well-defined.

Now suppose that $(X,*)$ is well-defined, necessarily a left quasigroup. We claim that $(X,*)$ is a rack. Fix u, v, $w\in X$ and let $x\in X/G$, $g_v\in G$ be such that $xg_v=v$. Since $g_vL_u\in G$ satisfies $xg_vL_u=vL_u=u*v$, we have $L_{u*v}=\lambda_x^{g_vL_u}=(\lambda_x^{g_v})^{L_u}=L_v^{L_u}$ and hence

$$(u*v)*(u*w)=wL_uL_{u*v}=wL_uL_v^{L_u}=wL_vL_u=u*(v*w).$$

We certainly have $\mathrm{Mlt}_\ell(X,*)=\langle\bigcup_{x\in X/G}L_x^G\rangle=\langle\bigcup_{x\in X/G}\lambda_x^G\rangle\leq G$.

(ii) If $(X,*)$ is a well-defined quandle, then (G,Λ) is a rack folder by (i) and for every $x \in X/G$ we have $x\lambda_x = x$, that is, $\lambda_x \in C_G(G_x) \cap G_x = Z(G_x)$. Conversely, if (G,Λ) is a quandle folder, then it is a rack folder, $(X,*)$ is a rack by (i), and for every $x \in X/G$, $y \in xG$, and $g_y \in G$ such that $xg_y = y$ we have $yL_y = y\lambda_x^{g_y} = yg_y^{-1}\lambda_x g_y = x\lambda_x g_y = xg_y = y$, where we have used $\lambda_x \in G_x$ in the penultimate step. □

Theorem 3.4 (Correspondence between racks/quandles and rack/quandle envelopes)**.** *Let X be a nonempty set and $G \le S_X$. There is a one-to-one correspondence between racks/quandles $(X,*)$ satisfying $\mathrm{Mlt}_\ell(X,*) = G$ and rack/quandle envelopes (G,Λ). Given a rack/quandle $(X,*)$ with $\mathrm{Mlt}_\ell(X,*) = G$, the corresponding rack/quandle envelope is $\mathbf{E}(X,*)$. Given a rack/quandle envelope (G,Λ), the corresponding rack/quandle is $\mathbf{R}(G,\Lambda)$.*

Proof. Suppose that $(X,*)$ is a rack/quandle with $\mathrm{Mlt}_\ell(X,*) = G$. By Lemma 3.1, $\mathbf{E}(X,*) = (G,(L_x^* : x \in X/G))$ is a rack/quandle envelope and $G = \langle \bigcup_{x\in X/G} (L_x^*)^G \rangle$. By Proposition 3.3, $(X,\circ) = \mathbf{R}(\mathbf{E}(X,*))$ is a rack/quandle satisfying $L_x^\circ = L_x^*$ for every $x \in X/G$ and $\mathrm{Mlt}_\ell(X,\circ) = \langle \bigcup_{x\in X/G} (L_x^*)^G \rangle = G$. Lemma 3.1 then implies that $(X,*) = (X,\circ)$.

Conversely, suppose that $\Lambda = (\lambda_x : x \in X/G)$ and (G,Λ) is a rack/quandle envelope. By Proposition 3.3, $(X,*) = \mathbf{R}(G,\Lambda)$ is a rack/quandle satisfying $L_x^* = \lambda_x$ for every $x \in X/G$ and $\mathrm{Mlt}_\ell(X,*) = \langle \bigcup_{x\in X/G} \lambda_x^G \rangle = G$, where the last equality holds because (G,Λ) is an envelope. Finally, we have $\mathbf{E}(\mathbf{R}(G,\Lambda)) = \mathbf{E}(X,*) = (G,(L_x^* : x \in X/G)) = (G,\Lambda)$. □

Note that we do not claim that there is a one-to-one correspondence between rack (or quandle) folders (G,Λ) and racks (or quandles) $(X,*)$ satisfying $\mathrm{Mlt}_\ell(X,*) \le G$. Indeed, if (G,Λ) is a rack folder, then there might exist several racks $(X,*)$ such that $L_x^* = \lambda_x$ for every $x \in X/G$ and $\mathrm{Mlt}_\ell(X,*) \le G$. (Let $G = S_X$, $X/G = \{x_0\}$, and $\lambda_{x_0} = 1$. Then (G,Λ) is a rack folder and any rack $(X,*)$ satisfying $L_{x_0}^* = 1$ does the job.) Conversely, if $(X,*)$ is a rack such that $\mathrm{Mlt}_\ell(X,*) \le G$, it might not be the case that $L_x^* \in C_G(G_x)$ for every $x \in X/G$. (Consider a rack with some $L_x^* \ne 1$ but take $G = S_X$ with $|X|$ large enough so that $C_G(G_x) = 1$.)

3.2. **Envelopes up to isomorphism.** We present a solution to the isomorphism problem for rack and quandle envelopes. Thanks to Proposition 2.1, it suffices to consider the case when the two corresponding racks have the same left multiplication groups.

Proposition 3.5. *Let $(G,(\lambda_x : x \in X/G))$ and $(G,(\kappa_x : x \in X/G))$ be rack/quandle envelopes. For every $x \in X/G$ and $y \in xG$ let $g_y \in G$ be such that $xg_y = y$. Then the corresponding racks/quandles are isomorphic if and only if there is $f \in N_{S_X}(G)$ such that*

$$\kappa_x = ((\lambda_{yg_y^{-1}})^{g_y})^f \tag{3.1}$$

for every $x \in X/G$, where $y = xf^{-1}$.

Proof. Let $(X,*)$ and $(X,\circ)$ be the racks/quandles corresponding to $(G,(\lambda_x : x \in X/G))$ and $(G,(\kappa_x : x \in X/G))$, respectively. By Corollary 2.2, $(X,*)$ is isomorphic to $(X,\circ)$ if and only if there is an isomorphism $f : (X,*) \to (X,\circ)$ such that $f \in N_{S_X}(G)$. By Proposition 2.1, f is an isomorphism if and only if $L_{xf}^\circ = (L_x^*)^f$

for every $x \in X$, or, equivalently, $L_x^\circ = (L^*_{xf^{-1}})^f$ for every $x \in X$. In fact, since $(X, \circ)$ is determined by G and the left translations L_x° with $x \in X/G$ (see Lemma 3.1), the last condition can be equivalently restated as $L_x^\circ = (L^*_{xf^{-1}})^f$ for every $x \in X/G$.

Let $x \in X/G$. We certainly have $\kappa_x = L_x^\circ$. Now, $y = xf^{-1}$ is not necessarily in X/G, but yg_y^{-1} is an element of X/G (possibly distinct from x), so

$$(L^*_{xf^{-1}})^f = (L_y^*)^f = ((L^*_{yg_y^{-1}})^{g_y})^f = ((\lambda_{yg_y^{-1}})^{g_y})^f,$$

finishing the proof. □

For $G \leq S_X$, let

$$\mathrm{Fol}_r(G), \quad \mathrm{Fol}_q(G), \quad \mathrm{Env}_r(G), \quad \mathrm{Env}_q(G)$$

be, respectively, the sets of all rack folders, quandle folders, rack envelopes, and quandle envelopes on X of the form (G, Λ). Given $f \in N_{S_X}(G)$ and an element $(\lambda_x : x \in X/G)$ of one of the above spaces, we define

$$(\lambda_x : x \in X/G)f = (\kappa_x : x \in X/G), \tag{3.2}$$

where for every $x \in X/G$ the bijection κ_x is obtained by (3.1).

Theorem 3.6 (Rack/quandle envelopes up to isomorphism)**.** *Let X be a nonempty set, $G \leq S_X$, and $F = N_{S_X}(G)$. Then:*

(i) *The group F acts on each of $\mathrm{Fol}_r(G)$, $\mathrm{Fol}_q(G)$, $\mathrm{Env}_r(G)$, and $\mathrm{Env}_q(G)$ via (3.2).*

(ii) *The orbits of F on $\mathrm{Env}_r(G)$ (resp., $\mathrm{Env}_q(G)$) are in one-to-one correspondence with isomorphism types of racks (resp., quandles) defined on X with left multiplication groups equal to G.*

(iii) *If an orbit of F on $\mathrm{Fol}_r(G)$ (resp., $\mathrm{Fol}_q(G)$) contains an element of $\mathrm{Env}_r(G)$ (resp., $\mathrm{Env}_q(G)$), then the entire orbit is a subset of $\mathrm{Env}_r(G)$ (resp., $\mathrm{Env}_q(G)$).*

Proof. Proposition 3.5 settles part (ii) and also part (i) for the case of rack and quandle envelopes. Does F act on rack/quandle folders? Suppose that (G, Λ) is a rack/quandle folder and let $(X, *) = \mathbf{R}(G, \Lambda)$. Let $f \in F$ and let $(X, \circ)$ be such that $f : (X, *) \to (X, \circ)$ is an isomorphism. Using the same notation as in the proof of Proposition 3.5, we have $L_x^\circ = (L^*_{xf^{-1}})^f = ((\lambda_{yg_y^{-1}})^{g_y})^f$, which means that $(\lambda_x : x \in X/G)f = (L_x^\circ : x \in X/G)$. By Proposition 3.3, $(G, (L_x^\circ : x \in X/G))$ is a rack/quandle folder. This proves (i). Part (iii) follows. □

3.3. **Remarks on rack and quandle admissibility.** A subgroup $G \leq S_X$ is said to be *rack admissible* (resp., *quandle admissible*) if there is a rack (resp., quandle) $(X, *)$ such that $\mathrm{Mlt}_\ell(X, *) = G$. Note that it is necessary to keep track of the way G acts on X, not just of the isomorphism type of G.

Proposition 3.7. *Let $G \leq S_X$. If G is rack admissible, then $\bigcup_{x \in X/G} (C_G(G_x))^G$ generates G. If G is quandle admissible, then $\bigcup_{x \in X/G} Z(G_x)^G$ generates G.*

Proof. If G is rack admissible, then by Theorem 3.4 there is a rack envelope $(G, (\lambda_x : x \in G/X))$. Since $\lambda_x \in C_G(G_x)$ for every $x \in X/G$, we have $G = \langle \bigcup_{x \in X/G} \lambda_x^G \rangle \leq \langle \bigcup_{x \in X/G} (C_G(G_x))^G \rangle \leq G$. The quandle case is similar. □

The necessary condition of Proposition 3.7 disqualifies many "large" subgroups of S_X from the search for racks and quandles. Certainly S_X itself is disqualified.

Corollary 3.8. *Let $|X| \geq 4$. Then S_X as a subgroup of itself is not rack admissible.*

Proof. The group $G = S_X$ acts transitively on X. For $x \in X$, G_x is isomorphic to $S_{X\setminus\{x\}}$. Since $|X| \geq 4$, we have $C_G(G_x) \cong C_{S_X}(S_{X\setminus\{x\}}) = 1$ and hence $(C_G(G_x))^G = 1$ does not generate G. □

It is well known that every rack (resp., quandle) of order n embeds into a rack (resp., quandle) of order $n+1$, proving that both r and q are nondecreasing functions. We give a short argument based on envelopes. It is certainly possible to give an elementary proof on the level of multiplication tables.

Proposition 3.9. *Let X be a set and z an element not contained in X. Every rack/quandle on X embeds into a rack/quandle on $X \cup \{z\}$.*

Proof. Let $\overline{X} = X \cup \{z\}$. For $\sigma \in S_X$ define $\overline{\sigma} \in S_{\overline{X}}$ by $x\overline{\sigma} = x$ if $x \in X$ and $z\overline{\sigma} = z$. Let $(G, (\lambda_x : x \in X/G))$ be a rack envelope. The orbits of $\overline{G}$ are the same as those of G, except for the additional singleton orbit $\{z\}$. For $x \in X/G$ let $\kappa_x = \overline{\lambda_x}$ and observe that $\kappa_x \in C_{\overline{G}}(\overline{G}_x)$ because $\lambda_x \in C_G(G_x)$. Let κ_z be the identity on $\overline{X} = X \cup \{z\}$, clearly satisfying $\kappa_z \in C_{\overline{G}}(\overline{G}_z)$. Then $(\overline{G}, (\kappa_x : x \in \overline{X}/\overline{G}))$ is a rack envelope. The quandle case is similar. □

4. The algorithm

4.1. **A basic algorithm.** It follows from Proposition 2.1, Theorem 3.4, and Theorem 3.6 that the algorithm in Figure 1 returns a complete set of isomorphism types of racks of order n (more precisely, rack envelopes on $X = \{1, \dots, n\}$).

```
01  X ← {1, ..., n}
02  𝒢 ← subgroups of S_X up to conjugation in S_X
03  for G in 𝒢 do
04      if MightBeRackAdmissible(G, X) then
05          Y ← Fol_r(G) = ∏_{x∈X/G} C_G(G_x)
06          O ← orbit representatives of the action
                of N_{S_X}(G) on Y given by (3.2)
07          R_G ← {(G, (λ_x : x ∈ X/G)) ∈ O : ⟨⋃_{x∈X/G} λ_x^G⟩ = G}
08      else
09          R_G ← ∅
10      end if
11  end for
12  return ⋃_{G∈𝒢} R_G
```

FIGURE 1. A basic algorithm for enumeration of racks and quandles up to isomorphism.

The function `MightBeRackAdmissible`(G, X) in line 04 returns `true` iff $\langle \bigcup_{x\in X/G} (C_G(G_x))^G \rangle = G$; cf. Proposition 3.7. Note that `true` might be returned even if $G \leq S_X$ is in fact not rack admissible.

Theorem 3.6(iii) guarantees that it is safe to discard the entire orbit of (G, Λ) in line 07 if (G, Λ) is not a rack envelope.

For quandles, it suffices to modify the algorithm as follows:

- replace the function `MightBeRackAdmissible`(G, X) in line 04 with the function `MightBeQuandleAdmissible`(G, X), which returns `true` iff $\langle \bigcup_{x \in X/G} Z(G_x)^G \rangle = G$, and
- populate the variable Y in line 05 with $\mathrm{Fol}_q(G) = \prod_{x \in X/G} Z(G_x)$.

We remark that the algorithm will struggle when $N_{S_X}(G)$ is large, which tends to happen when G is either very small or very large. The extreme case $G = 1$ (which yields $N_{S_X}(G) = S_X$) can be handled separately since then the set $\mathrm{Fol}_r(G)$ is a singleton. Large subgroups of S_X are typically disqualified by failing the necessary condition of Proposition 3.7.

4.2. **Indexing.** In some computational packages it is possible to define the action (3.2) on the domain Y and then call standard methods for orbit representatives. We encounter two difficulties. The space Y can be too large (more than a billion elements for some $G \leq S_{12}$) to be stored in memory. Even if Y can be stored in memory, the default methods to convert the action into a permutation action on $\{1, \ldots, |Y|\}$ and the algorithm might run out of memory then. In this subsection we will show how to make the algorithm work on larger domains than the default methods would allow. A similar approach to indexing and actions on large domains is implemented in `GAP`; cf. methods `PositionCanonical` and `OrbitStabilizerAlgorithm`.

Let $G \leq S_X$. We will efficiently index the space $Y = \prod_{x \in X/G} C_G(G_x)$ of rack folders, the case of quandle folders being similar. (However, it is not easy to index elements of the subset of rack envelopes or quandle envelopes.) Let $<$ be a lexicographical order on Y inherited from a linear order on S_X. Let $p(C_G(G_x), \lambda_x)$ be the position of λ_x in $C_G(G_x)$ with respect to $<$. Then $\Lambda = (\lambda_x : x \in X/G) \in Y$ can be identified with the numerical vector $(p(C_G(G_x), \lambda_x) : x \in X/G)$, which can in turn be identified with an element of the interval $\{1, \ldots, |Y|\}$, for instance by using a hybrid-base expansion. It is then easy to implement the conversion functions `Element`(Y, i) (that returns the ith element of Y) and `Position`(Y, Λ) (that returns the position of Λ in Y).

Given $G \leq S_X$ and $Y = \mathrm{Fol}_r(G)$, the algorithm in Figure 2 returns the desired orbit representatives of the action of $N_{S_X}(G)$ on Y; it can be used to replace lines 06 and 07 of the algorithm in Figure 1. Note that thanks to the indexing functions described above we do not need to keep Y in memory, only the much smaller subsets $C_G(G_x)$ and a binary vector of length $|Y|$.

The test in line 06:05 ensures that folders (G, Λ) that are not envelopes will not be returned. Note that the value of p in line 06:09 can never be less than i.

4.3. **Precalculating the action of $N_{S_X}(G)$.** It is time consuming to calculate Λf in line 06:09, inside the innermost cycle of the algorithm. In this subsection we will show how the algorithm can be substantially improved by precalculating the action of $N_{S_X}(G)$ on the space Y. We will take advantage of the fact that the action (3.2) can be localized, i.e., when

$$(\kappa_x : x \in X/G) = (\lambda_x : x \in X/G) f,$$

```
06:01  V ← binary array of length |Y| with all values initialized to true
06:02  for i in {1,...,|Y|} do
06:03      if V[i] = true then
06:04          Λ = (λ_x : x ∈ X/G) ← Element(Y, i)
06:05          if ⟨⋃_{x∈X/G} λ_x^G⟩ ≠ G then
06:06              V[i] ← false
06:07          end if
06:08          for f in N_{S_X}(G) do
06:09              p ← Position(Y, Λf)
06:10              if p > i then
06:11                  V[p] ← false
06:12              end if
06:13          end for
06:14      end if
06:15  end for
06:16  R_G ← {(G, Element(Y, i)) : 1 ≤ i ≤ |Y|, V[i] = true}
06:17  return R_G
```

FIGURE 2. An algorithm for orbit representatives of $N_{S_X}(G)$ on $Y = \mathrm{Fol}_r(G)$.

```
06:09:01  for x ∈ X/G do
06:09:02      y ← xf^{-1}
06:09:03      z ← the unique element of (X/G) ∩ yG
06:09:04      p_x ← I(f, x, λ_z)
06:09:05  end for
06:09:06  p ← the index of (p_x : x ∈ X/G) as an element of {1,...,|Y|}
```

FIGURE 3. Code for the position of $(\lambda_x : x \in X/G)f$ in $\mathrm{Fol}_r(G)$ with precalculated action.

the value of κ_x depends only on $y = xf^{-1}$, g_y, and $\lambda_{yg_y^{-1}}$, rather than on the entire folder $(\lambda_x : x \in X/G)$.

Suppose that $G \leq S_X$ is given. Given $f \in N_{S_X}(G)$ and $x \in X/G$, let $y = xf^{-1}$ and $z \in (X/G) \cap yG$, and for every $\lambda_z \in C_G(G_z)$ let us precalculate

$$I(f, x, \lambda_z) = p(C_G(G_x), ((\lambda_z)^{g_y})^f).$$

Line 06:09 can then be replaced with the code in Figure 3.

We have now finished describing the main features of the algorithm by which we have obtained the isomorphism types of racks (resp., quandles) of orders ≤ 11 (resp., ≤ 12). We have explained in the Introduction how the cases $r(12)$, $r(13)$, and $q(13)$ were handled.

5. Counting orbits of the action on rack and quandle folders

In this section we visualize the action (3.2) of $N_{S_X}(G)$ on $\mathrm{Fol}_r(G)$ and count its orbits, the case of quandle folders being similar. Unfortunately, this approach does not solve the orbit counting problem on the space of rack and quandle envelopes.

Let $G \leq S_X$, $F = N_{S_X}(G)$, and $f \in F$. Construct a digraph (possibly with loops) $\Gamma_r(G, f)$ as follows. The vertex set of $\Gamma_r(G, f)$ is the disjoint union of the sets $C_G(G_x)$ for $x \in X/G$. (The sets $C_G(G_x)$ are not disjoint as subsets of S_X, but we will treat them as being formally disjoint for the digraph construction.) Given not necessarily distinct x, $z \in X/G$, $\kappa_x \in C_G(G_x)$, and $\lambda_z \in C_G(G_z)$, we declare $\lambda_z \to \kappa_x$ to be a directed edge of $\Gamma_r(G, f)$ if and only if with $y = xf^{-1}$ we have $z = yg_y^{-1}$ and $\kappa_x = ((\lambda_z)^{g_y})^f$.

The digraph $\Gamma_r(G, f)$ can be seen as a visualization of the action of $\langle f \rangle$ on $\mathrm{Fol}_r(G)$. The elements $(\lambda_x : x \in X/G)$ of $\mathrm{Fol}_r(G)$ correspond precisely to selections of vertices of $\Gamma_r(G, f)$, one in each vertex set $C_G(G_x)$. When $(\kappa_x : x \in X/G) = (\lambda_x : x \in X/G)f$, then the tuple $(\kappa_x : x \in X/G)$ is obtained from $(\lambda_x : x \in X/G)$ by moving away from every λ_x along the (unique) directed edge starting at λ_x.

Before we describe some properties of $\Gamma_r(G, f)$, let us observe that $f \in N_{S_X}(G)$ induces a permutation of X/G. Indeed, suppose that x, $y \in G$ belong to the same orbit of G, so $x = yg$ for some $g \in G$. Then $xff^{-1}gf = xgf = yf$ and $f^{-1}gf \in G$ show that xf, yf belong to the same orbit of G.

Proposition 5.1. *Let X be a finite set, $G \leq S_X$, $f \in N_{S_X}(G)$, and $\Gamma = \Gamma_r(G, f)$. Let $\bar{f}$ be the permutation of X/G induced by f. Then:*

(i) *Γ is an $|X/G|$-partite digraph with parts $\{C_G(G_x) : x \in X/G\}$.*
(ii) *For x, $z \in X/G$, there exists an edge from $C_G(G_z)$ to $C_G(G_x)$ if and only if $\bar{f}$ maps zG to xG.*
(iii) *The digraph induced by Γ on X/G by collapsing every vertex set $C_G(G_x)$ into a single vertex is a disjoint union of directed cycles, namely the cycle decomposition of $\bar{f}$.*
(iv) *Every vertex of Γ has indegree equal to 1 and outdegree equal to 1, so Γ is a union of disjoint directed cycles.*

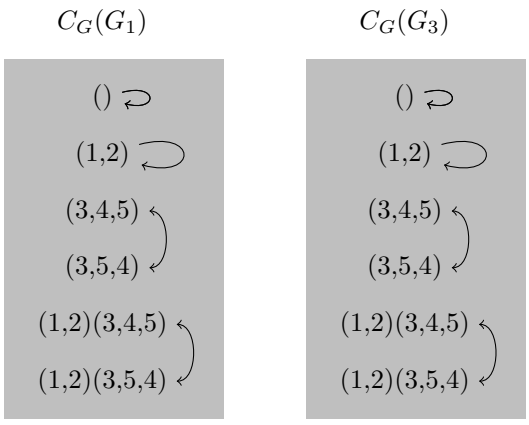
Proof. Part (i) follows from the definition of Γ. For (ii), note that the identity permutation 1 is present in every $C_G(G_x)$ and if $y = xf^{-1}$, $z = yg_y^{-1}$, $\kappa_x = 1$, and $\lambda_z = 1$, then $\kappa_x = ((\lambda_z)^{g_y})^f$. Part (iii) follows.

For (iv), suppose that $\lambda_z \to \kappa_x$ and $\mu_z \to \kappa_x$ are edges and let $y = xf^{-1}$ as usual. Then $((\lambda_z)^{g_y})^f = \kappa_x = ((\mu_z)^{g_y})^f$ and therefore $\lambda_z = \mu_z$. Dually, if $\lambda_z \to \kappa_x$ and $\lambda_z \to \nu_x$ are edges, then $\kappa_x = ((\lambda_z)^{g_y})^f = \nu_x$. Since the indegree and outdegree of every vertex is equal to 1, Γ is a disjoint union of directed cycles. □

Let us illustrate the digraph construction with two small examples.

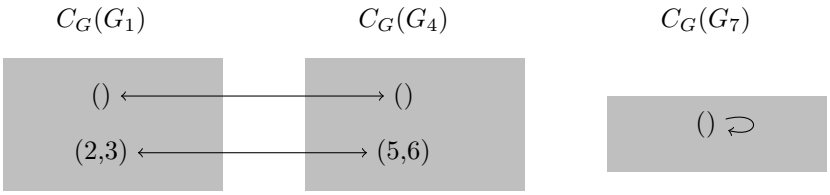
Example 5.2. Let $X = \{1, \ldots, 5\}$ and let $G = \langle (1, 2)(3, 4, 5) \rangle \cong C_6$ be a subgroup of S_X. Then G has orbits $\{1, 2\}$, $\{3, 4, 5\}$ and we can take $X/G = \{1, 3\}$. We have $C_G(G_1) = C_G(G_3) = G$ and $F = N_{S_5}(G) = \langle G, (4, 5) \rangle$. Consider $f = (1, 2)(4, 5) \in F$. The permutation $\bar{f}$ on X/G induced by f is trivial and the directed graph

$\Gamma_r(G, f)$ is as follows:



For instance, there is a directed edge $(3,4,5) \to (3,5,4)$ in the vertex set $C_G(G_1)$ because with $x = 1$, $y = xf^{-1} = 2$, and $g_y = (1,2)$ we have $((3,4,5)^{g_y})^f = (3,4,5)^f = (3,5,4)$. (Since G is abelian here, the conjugations by the g_ys can be omitted.)

Example 5.3. Let $X = \{1, \dots, 7\}$ and let $G = \langle (1,2), (1,2,3), (4,5), (4,5,6) \rangle \cong S_3 \times S_3$ be a subgroup of S_X. Then G has orbits $\{1,2,3\}$, $\{4,5,6\}$, $\{7\}$ and we can take $X/G = \{1,4,7\}$. We have $C_G(G_1) = \langle (2,3) \rangle$, $C_G(G_4) = \langle (5,6) \rangle$, $C_G(G_7) = 1$, and $F = N_{S_7}(G) = \langle G, (1,4)(2,5)(3,6) \rangle$. Consider $f = (1,5)(2,4)(3,6) \in F$. The permutation of X/G induced by f is given by $(1,4)(7)$ and the directed graph $\Gamma_r(G, f)$ is as follows:



This must be the case because the cycle structure of permutations is preserved by conjugation. To give a detailed calculation in one case, there is an edge from $(5,6)$ in $C_G(G_4)$ to $(2,3)$ in $C_G(G_1)$ since with $x = 1$, $y = xf^{-1} = 5$, and $g_y = (4,5)$ we have $((5,6)^{g_y})^f = (2,3)$.

Note that a directed cycle of $\Gamma_r(G, f)$ can visit a given vertex set $C_G(G_x)$ more than once before closing upon itself. For instance, in Example 5.2, there is a cycle that starts in $C_G(G_1)$ at $(3,4,5)$, returns to $C_G(G_1)$ at $(3,5,4)$, and only then closes itself. Call a cycle of $\Gamma_r(G, f)$ *short* if it intersects every vertex set $C_G(G_x)$ at most once.

Theorem 5.4. *Let X be a finite set, $G \leq S_X$, $Y = \mathrm{Fol}_r(G)$, $F = N_{S_X}(G)$, and consider the action* (3.2) *of F on Y.*

For $f \in F$, let $\bar{f}$ be the permutation of X/G induced by f, $\mathrm{Cyc}(\bar{f})$ a complete set of cycle representatives of $\bar{f}$, and $c(\bar{f}, x)$ the cycle of $\bar{f}$ containing $x \in \mathrm{Cyc}(\bar{f})$. Then there is a one-to-one correspondence between the fixed points $\mathrm{Fix}(Y, f)$ of the

action of $\langle f\rangle$ on Y and the tuples $(c_x : x \in \mathrm{Cyc}(\bar{f}))$, where c_x is a short directed cycle of $\Gamma_r(G,f)$ with vertices in $\bigcup_{y\in c(\bar{f},x)} C_G(G_y)$.

Therefore, the number of orbits of F on Y is given by

$$|Y/F| = \frac{1}{|F|}\sum_{f\in F}|\mathrm{Fix}(Y,f)| = \frac{1}{|F|}\sum_{f\in F}\prod_{x\in\mathrm{Cyc}(\bar{f})}\gamma_r(G,f,x),$$

where $\gamma_r(G,f,x)$ is the number of short directed cycles of $\Gamma_r(G,f)$ with vertices in $\bigcup_{y\in c(\bar{f},x)} C_G(G_y)$.

Proof. Let $f \in N_{S_X}(G)$ and let $\Lambda = (\lambda_x : x \in X/G)$ be a rack folder realized as a selection of vertices of the digraph $\Gamma = \Gamma_r(G,f)$, one vertex in each part $C_G(G_x)$. Then $\Lambda f = \Lambda$ if and only if all edges of Γ starting in Λ also terminate in Λ, or, in other words, if and only if Λ is a disjoint union of short directed cycles. We are done by Burnside's Lemma. □

Note that while $\mathrm{Fol}_r(G)$ is of size $\prod_{x\in X/G}|C_G(G_x)|$ and therefore possibly quite large, the vertex set of every $\Gamma_r(G,f)$ is only of size $\sum_{x\in X/G}|C_G(G_x)|$ so it is relatively easy to construct $\Gamma_r(G,f)$ explicitly. Due to the structure of $\Gamma_r(G,f)$, it is not difficult to count its short directed cycles. Indeed, since the outdegree and indegree of every vertex is equal to 1, it suffices to trace the cycles starting at vertices of $\bigcup_{x\in\mathrm{Cyc}(\bar{f})} C_G(G_x)$ and keep only the short cycles. Of course, we can also determine the number of short cycles from suitable powers of the adjacency matrix of $\Gamma_r(G,f)$.

6. Open problems

We were not able to determine the numbers $r(14)$ and $q(14)$. Note that it suffices to find $r_{\text{non-2-red}}(14)$ and $q_{\text{non-2-red}}(14)$ since $r_{2\text{-red}}(14)$ and $q_{2\text{-red}}(14)$ are known; cf. Tables 1 and 2. The main obstacle in the enumeration is the size of the spaces of rack folders and quandle folders for certain nonabelian permutation groups. For larger orders, it will not be feasible to consider all subgroups of S_n up to conjugacy.

Problem 6.1. Determine the number of isomorphism types of racks and quandles of order 14.

It is to be expected that $r(14)$ and $q(14)$ will only slightly exceed $r_{2\text{-red}}(14)$ and $q_{2\text{-red}}(14)$, respectively. However, the asymptotic proportion of 2-reductive racks and 2-reductive quandles is less predictable.

Problem 6.2. What are the limits $\lim_{n\to\infty}\frac{r_{2\text{-red}}(n)}{r(n)}$ and $\lim_{n\to\infty}\frac{q_{2\text{-red}}(n)}{q(n)}$, if they exist?

Let us now look at the structure of $\mathrm{Mlt}_\ell(X,*)$ for racks and quandles. Blackburn [2] proved that for every group G there is a quandle $(X,*)$ on some set X such that $\mathrm{Mlt}_\ell(X,*)$ is isomorphic to G. But not every permutation group is rack/quandle admissible. In view of the results in Section 3, a subgroup $G \le S_X$ is rack admissible (resp., quandle admissible) if and only if there are $(\lambda_x \in C_G(G_x) : x \in X/G)$ (resp., $(\lambda_x \in Z(G_x) : x \in X/G)$) such that $\langle\bigcup_{x\in X/G}\lambda_x^G\rangle = G$.

Problem 6.3. Describe a large or algebraically significant class of subgroups G of S_X that are not rack/quandle admissible, that is, for which there is no rack/quandle $(X,*)$ such that $\mathrm{Mlt}_\ell(X,*) = G$.

To shed some light on Problems 6.2 and 6.3, we offer the following observations about left multiplication groups of quandles of order 10. These and similar facts can be verified using the library of racks and quandles available on the web page of the first author.

There are 102771 quandles of order 10 and their left multiplication groups form a set of 471 nonequivalent permutation groups. The number of quandles associated with a given permutation group varies greatly. There are 63 permutation groups with a unique quandle, 84 with two quandles and 22 with three quandles. On the other side of the spectrum, there are five permutation groups that account for 20084, 17336, 12033, 6359 and 6284 quandles, respectively. Up to isomorphism, these groups are $C_3 \times C_2^3$, C_2^4, $C_3 \times C_2^2$, $C_3^2 \times C_2$, and $C_4 \times C_2^2$, respectively. The most prolific group has generators $(2,5,3)(7,9)(8,10)$, $(8,10)$, and $(4,6)(7,9)$.

There is a unique nonsolvable group among the 471 permutation groups, namely a copy of S_5 generated by $(1,4,6,3,2)(5,8,7,10,9)$ and $(3,8)(5,9)(6,10)$. There are two quandles associated with this group. Furthermore, there are 247 nonnilpotent groups with 3383 associated quandles, 320 nonabelian groups with 4239 associated quandles, and 59 elementary abelian 2-groups with 35091 associated quandles.

Problem 6.4. Let $G \leq S_X$. Show how Burnside's Lemma can be effectively used to count the orbits of the action of $N_{S_X}(G)$ on $\mathrm{Env}_r(G)$ or $\mathrm{Env}_q(G)$.

Finally, our computational data support the following conjecture.

Conjecture 6.5. *Let p be a prime. Then $r_{\mathrm{med}}(p) - r_{2\text{-red}}(p) = p-2$ and $q_{\mathrm{med}}(p) - q_{2\text{-red}}(p) = p-2$. In particular, every medial rack of order p that is not 2-reductive is a quandle.*

Acknowledgments

We thank Alexander Hulpke for the reference [9], Přemysl Jedlička for the numbers of 2-reductive racks of small orders, Victoria Lebed for the references [1] and [2], David Stanovský for useful discussions about Burnside's Lemma in the context of affine meshes, Glen Whitney for a clarification about 2-reductivity in racks, and anonymous referees for useful comments. The calculations took place at the High Performance Computing Cluster of the University of Denver.

References

[1] M. Ashford and O. Riordan, *Counting racks of order n*, Electron. J. Combin. **24** (2017), no. 2, Paper 2.32, 20. MR3665565

[2] S. R. Blackburn, *Enumerating finite racks, quandles and kei*, Electron. J. Combin. **20** (2013), no. 3, Paper 43, 9. MR3118951

[3] R. H. Bruck, *A Survey of Binary Systems*, Ergebnisse der Mathematik und ihrer Grenzgebiete. Neue Folge, Heft 20. Reihe: Gruppentheorie, Springer Verlag, Berlin-Göttingen-Heidelberg, 1958. MR0093552

[4] V. G. Drinfel′d, *On some unsolved problems in quantum group theory*, Quantum Groups (Leningrad, 1990), Lecture Notes in Math., vol. 1510, Springer, Berlin, 1992, pp. 1–8, DOI 10.1007/BFb0101175. MR1183474

[5] M. Elhamdadi, J. Macquarrie, and R. Restrepo, *Automorphism groups of quandles*, J. Algebra Appl. **11** (2012), no. 1, 1250008, 9, DOI 10.1142/S0219498812500089. MR2900878

[6] M. Elhamdadi and S. Nelson, *Quandles—An Introduction to the Algebra of Knots*, Student Mathematical Library, vol. 74, American Mathematical Society, Providence, RI, 2015. MR3379534

[7] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.6.3; 2013. `http://www.gap-system.org`.

[8] R. Henderson, T. Macedo, and S. Nelson, *Symbolic computation with finite quandles*, J. Symbolic Comput. **41** (2006), no. 7, 811–817, DOI 10.1016/j.jsc.2006.03.002. MR2232202
[9] D. F. Holt, *Enumerating subgroups of the symmetric group*, Computational Group Theory and the Theory of Groups, II, Contemp. Math., vol. 511, Amer. Math. Soc., Providence, RI, 2010, pp. 33–37, DOI 10.1090/conm/511/10041. MR2655292
[10] A. Hulpke, D. Stanovský, and P. Vojtěchovský, *Connected quandles and transitive groups*, J. Pure Appl. Algebra **220** (2016), no. 2, 735–758, DOI 10.1016/j.jpaa.2015.07.014. MR3399387
[11] P. Jedlička, A. Pilitowska, D. Stanovský, and A. Zamojska-Dzienio, *The structure of medial quandles*, J. Algebra **443** (2015), 300–334, DOI 10.1016/j.jalgebra.2015.04.046. MR3400403
[12] D. Joyce, *A classifying invariant of knots, the knot quandle*, J. Pure Appl. Algebra **23** (1982), no. 1, 37–65, DOI 10.1016/0022-4049(82)90077-9. MR638121
[13] S. V. Matveev, *Distributive groupoids in knot theory*, Math. USSR - Sbornik **47/1** (1984), 73–83.
[14] The Online Encyclopedia of Integer Sequences, `https://oeis.org/A181769` and `https://oeis.org/A181770`.
[15] L. Vendramin, *On the classification of quandles of low order*, J. Knot Theory Ramifications **21** (2012), no. 9, 1250088, 10, DOI 10.1142/S0218216512500885. MR2926571

Department of Mathematics, University of Denver, 2390 S York St, Denver, Colorado, 80208
Email address: `petr@math.du.edu`

Department of Mathematics, Kyungpook National University, Daegu, 41566, Republic of Korea
Email address: `seungyeop.yang@knu.ac.kr`