On Finite Racks and Quandles

Pedro Lopes
Departamento de Matemática
Instituto Superior Técnico
Av. Rovisco Pais
1049-001 Lisboa
Portugal
pelopes@math.ist.utl.pt

Dennis Roseman
Mathematics Department
The University of Iowa
MacLean Hall
Iowa City, IA 52242
USA
roseman@math.uiowa.edu

August 30, 2004

Abstract

We revisit finite racks and quandles using a perspective based on permutations which can aid in the understanding of the structure. As a consequence we recover old results and prove new ones. We also present and analyze several examples.

1 Introduction

The algebraic structure known as quandle was introduced independently by Joyce and Matveev ([10] and [14]) in order to obtain invariants of knotted circles i.e., invariants of embeddings of the circle in three space ([12]). Given any knotted circle, the idea is to associate a quandle to it - the knot quandle. As was later remarked by Fenn and Rourke ([9]) this procedure generalizes to higher dimensions, in particular to embeddings of closed surfaces in four space - the so-called knotted surfaces ([17], [4]). Given the similarities of these two procedures we will next describe how to associate the knot quandle to the embedding in both cases i.e., embeddings of circles in three space and embeddings of closed surfaces in four space. Consider the embedding under study. Upon convenient projection of it on a plane (3-hyperplane, resp.), the crossing points (lines of self-intersection, resp.) split the projection into arcs (regions, resp.).

A presentation of the knot quandle is obtained by regarding the arcs (regions, resp.) as generators and by reading specific relations at the crossings (lines of self-intersection, resp.). Thanks to the defining axioms of quandles this association is essentially insensitive to the Reidemeister moves (Roseman moves, resp.) thus making the knot quandle an invariant for knotted circles (for knotted surfaces, resp.). Moreover, in the case of knots, the knot quandle is a classifying invariant modulo orientation of the ambient space. Given that the knot quandle is an invariant modulo orientation of the ambient space, we will take a knot to be a representative of each of these equivalence classes; in particular, the trefoil knot and its mirror image correspond to the same knot.

As in the case of group presentations, these quandle presentations by themselves are difficult to work with. On the other hand, the naïve approach of counting homomorphisms from the knot quandle to specified target quandles (counting colorings of the knot quandle by specified labelling quandles, [9], [5], [13]) has proved to be extremely effective. As a matter of fact, with only ten labelling quandles all but less than 3% of the pairs of prime knots of up to ten crossings are told apart by counting colorings ([8]). A relevant success is also obtained when trying to tell apart knotted surfaces via counting colorings ([2]).

There is a related algebraic structure known as rack of which the quandles are particular cases. Racks are invariants of framed knots ([9]). Moreover, racks are invariants of knotted surfaces ([18]).

Notwithstanding the success of these applications of quandles and/or racks to knot theory, there are simple questions that remain unanswered. Here are some of them. Are there knots which are not distinguished by counting colorings? If any two knots are distinguished by counting colorings, given an integer $c > 2$, find an integer $n_c > 2$ such that all prime knots of crossing number less than or equal to c are distinguished via counting colorings with labelling quandles of order less than or equal to n_c. Can the class of labelling quandles be further restricted to finite Alexander quandles? Or even to finite linear Alexander quandles?

We believe that in order to answer these and other related questions more has to be known about the structure of racks and quandles. In this paper we focus on racks and quandles as sequences of permutations. In Section 2 we describe the passage into regarding racks and quandles as sequences of permutations and give basic examples of racks from this point of view. We rewrite the axioms and prove easily basic properties in Section 3. In Sections 4 and 5 we use elementary facts about permutations to derive invariants of racks and quandles. In Section 6 we briefly discuss indecomposability and transitivity of racks and quandles. In Section 7 we introduce Δ-orbits which will be useful in the proofs in Section 8 where we identify the racks that realize given profiles. Throughout the text we present and discuss several examples of racks and quandles.

2 Preliminaries

A **rack** ([10], [14], [3], [12], [9], [6], [1], for instance) is an algebraic structure whose binary operation, denoted $*$, is right-invertible and self-distributive. Denoting X the underlying set, right-invertibility states that for any i, j in X, there is a unique x in X satisfying the equation $x * j = i$. Hence, for any j in X, the assignment

$$\begin{aligned} \mu_j : \quad X &\longrightarrow X \\ x &\longmapsto x * j \end{aligned}$$

is a permutation of X; it is surjective because there is a solution to each equation referred to above and it is injective because that solution is unique, see Section 3 for details. We will then regard a rack of order n as a finite sequence of n permutations from S_n (the group of permutations of n objects) one for each element of X, in the sense just discussed. In particular, the j-th column of the multiplication table of the rack under study is the image of the permutation corresponding to j, for each j in X. Since there is a second axiom in the definition of rack, it turns out that not any sequence of n permutations from S_n gives rise to a rack. In fact, this second axiom, self-distributivity, amounts to saying that the μ_j's preserve the $*$ operation i.e., $\mu_j(i * i') = \mu_j(i) * \mu_j(i')$ and since the μ_j's are bijections then this amounts to saying that each μ_j defines an automorphism on the rack under study. We will next illustrate these ideas with examples. Our main reference for notation and facts about permutations will be [19].

2.1 Preliminary Examples

Example 2.1 *For integer n greater than 2, the* **dihedral rack** *of order n, denoted R_n, is the set formed by the first n positive integers, $\{1, 2, \ldots, n\}$, equipped with the operation $i * j := 2j - i$, mod n.*

The multiplication table for R_3 is displayed in Table 2.1. The permutation corresponding to 1 is then

R_3	1	2	3
1	1	3	2
2	3	2	1
3	2	1	3

Table 2.1: R_3 Multiplication Table

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (1)(23)$$

where (1)(23) is the permutation expressed as products of disjoint cycles, which is the way permutations will be written, henceforth; note also that () denotes the identity permutation. Analogously, $\mu_2 = (13)$, and $\mu_3 = (12)$, omitting 1-cycles. The sequence of permutations of R_3 is then $\big((23), (13), (12)\big)$. In this way, $1 * 1 = \mu_1(1) = 1$, $1 * 2 = \mu_2(1) = 3$, $\mu_j(i) = i * j = 2j - i$, mod 3, for any i, and $j \in \{1, 2, 3\}$ thereby

T_3	1	2	3
1	1	1	1
2	2	2	2
3	3	3	3

Table 2.2: T_3 Multiplication Table

C_3	1	2	3
1	2	2	2
2	3	3	3
3	1	1	1

Table 2.3: C_3 Multiplication Table

recovering the rack operation on $\{1,2,3\}$. For general n, the i-th term of the sequence of permutations of R_n is, for any i in $\{1,2,\ldots,n\}$, the product of transpositions,

$$\mu_i = \prod_{j=1}^{[\frac{n-1}{2}]} (\ i+j \quad i-j\ ) \qquad \texttt{mod n}$$

Example 2.2 *T_n is the* **trivial rack** *of order n. The underlying set is the set of the n first positive integers $\{1,2,\ldots,n\}$ and $i*j := i$ for any i, $j \in \{1,2,\ldots,n\}$.*

For $n=3$ its multiplication table is displayed in Table 2.2; the sequence of permutations is then $\big((),(),()\big)$, where $()$ stands for the identity permutation. For general n, the i-th term of the sequence of permutations is, for any i in $\{1,2,\ldots,n\}$

$$\mu_i = (\ )$$

Example 2.3 *C_n is the* **cyclic rack** *of order n. Its underlying set is $\{1,2,\ldots,n\}$ and $i*j := i+1$ mod n, for any i, and $j \in \{1,2,\ldots,n\}$.*

For $n = 3$ its multiplication table is displayed in Table 2.3; the sequence of permutations is then $\big((1\ 2\ 3),(1\ 2\ 3),(1\ 2\ 3)\big)$. For general n, the i-th term of the sequence of permutations is, for any i in $\{1,2,\ldots,n\}$

$$\mu_i = (\ 1\ 2\ 3\ \cdots\ n\ )$$

3 Racks as Sequences of Permutations

We begin with

Def. 3.1 *A* **rack** *is a set, X, equipped with a binary operation, denoted $*$, such that:*

- *for all i, and $j \in X$ there exists a unique $x \in X$ such that $x*j = i$ holds;*
- *for all i, j, and $k \in X$, $(i*j)*k = (i*k)*(j*k)$*

We refer to the first axiom as "right-invertibility" and to the second as "self-distributivity".

Def. 3.2 *A* **quandle** *is a rack, such that, for any $i \in X$, $i*i = i$.*

This will be called the "quandle condition".

Def. 3.3 *A* **prack** *is a rack which is not a quandle.*

In this note, we will be dealing with finite racks or quandles. Without loss of generality, the underlying set of such an algebraic structure of order n, and any set of finite cardinality n, will be taken to be the set of the first n positive integers, $\{1, 2, \dots, n\}$, unless where explicitly stated.

Def. 3.4 *A rack of finite order n is called a k-**prack** (for some k in $\{0, 1, 2, \dots, n\}$) if there are exactly k distinct elements $i_1, i_2, \dots, i_k$ in $\{1, 2, \dots, n\}$ such that $i_j * i_j \neq i_j$.*

Roughly speaking, a k-prack is a rack which violates k times the quandle condition. A 0-prack is a quandle. In the introduction, the trivial racks and the dihedral racks are examples of quandles. The cyclic racks are examples of pracks; for each n, the cyclic rack of order n is an n-prack.

Thm. 3.1 *Let X be a finite set of cardinality n. Suppose a permutation $\mu_i \in S_n$ (the group of permutations of the n symbols $1, 2, \dots, n$) is assigned to each i in X. Then the expression*

$$i * j := \mu_j(i)$$

for all i, $j \in \{1, 2, \dots, n\}$, yields a rack structure in X if and only if

$$\mu_{\mu_j(i)} = \mu_j \mu_i \mu_j^{-1}$$

for all i, $j \in \{1, 2, \dots, n\}$.

Proof: Suppose $(X, *)$ is a rack. Then $(i*j)*k = (i*k)*(j*k)$ is equivalent to $\mu_k\big(\mu_j(i)\big) = \mu_{\mu_k(j)}\big(\mu_k(i)\big)$ which is equivalent to $\mu_{\mu_k(j)} = \mu_k \mu_j \mu_k^{-1}$. This proves the result in one direction. Now for the converse. Self-distributivity is clear from the calculations above. Suppose i, j, and $k \in \{1, 2, \dots, n\}$. Then $k = i * j := \mu_j(i)$ is equivalent to $\mu_j^{-1}(k) = i$. So, for any k, $j \in \{1, 2, \dots, n\}$ there is a unique solution to the equation $k = x * j$. The result follows. ■

Def. 3.5 *Let $R = (X, *)$ be a finite rack of order n. We call **sequence of permutations of** R the sequence of permutations $(\mu_1, \dots, \mu_n)$ given by $\mu_j(i) := i * j$, for all i, $j \in X$.*

In this way, Theorem 3.1 describes the conditions the permutations of the sequence of permutations of a rack have to satisfy. These permutations generate the **operator group** ([10], [9]). We note

Cor. 3.1 *Let $(\mu_1, \dots, \mu_n)$ denote the sequence of permutations of a rack R of finite order n. Then R is a quandle if and only if $\mu_i(i) = i$, for all i.*

Proof: Since $R = (X, *)$ is a rack then it is a quandle if and only if $i = i * i = \mu_i(i)$, for all i. ■

The right-invertibility axiom of a rack allows for the definition of a second binary operation on the rack.

Def. 3.6 *Let $R = (X, *)$ be a rack. For any i, $j \in X$, let $i \,\bar{*}\, j$ denote the unique solution to the equation $x * j = i$. $\bar{*}$ is said to be the dual operation to $*$. X equipped with this binary operation is called the **dual** of R.*

In the proof of Theorem 3.1 we came up with a formula for this unique solution provided we had the original rack represented by its sequence of permutations. This will help to prove that

Cor. 3.2 *The dual of a rack (resp., quandle) is a rack (resp., quandle).*

Proof: Let $R = (X, *)$ be a finite rack with sequence of permutations $(\mu_1, \dots, \mu_n)$. As seen above, the dual operation is given by $i \,\bar{*}\, j = \mu_j^{-1}(i)$. So if the dual of R is also a rack, its sequence of permutations has to be $(\mu_1^{-1}, \dots, \mu_n^{-1})$. Since R is a rack then, for all i, j, $\mu_{\mu_i(j)} = \mu_i \mu_j \mu_i^{-1}$ which, by taking inverses, is equivalent to $\mu_{\mu_i(j)}^{-1} = \mu_i \mu_j^{-1} \mu_i^{-1}$ which can be rewritten as $\mu_i^{-1} \mu_{\mu_i(j)}^{-1} \mu_i = \mu_j^{-1}$. Since, for any i, μ_i is a bijection, then we can put $j' = \mu_i(j)$ so that $j = \mu_i^{-1}(j')$ and so, for all j' and i, $\mu_i^{-1} \mu_{j'}^{-1} \mu_i = \mu_{\mu_i^{-1}(j')}^{-1}$. Finally, if R is a quandle then, for any i, $\mu_i(i) = i$ which is equivalent to saying that $\mu_i^{-1}(i) = i$, for all i. The result follows. ■

Cor. 3.3 *The $*$ and $\bar{*}$ operations are distributive with respect to each other i.e., for all i, j and k,*

$$(i * j) \bar{*} k = (i \bar{*} k) * (j \bar{*} k) \qquad and \qquad (i \bar{*} j) * k = (i * k) \bar{*} (j * k)$$

Proof: We will just prove that $(i*j)\bar{*}k = (i\bar{*}k)*(j\bar{*}k)$. This is equivalent to $\mu_k^{-1}\mu_j(i) = \mu_{\mu^{-1}(j)}\mu^{-1}\mu_k(i)$ which is equivalent to $\mu_k^{-1}\mu_j^{-1}\mu_k = \mu^{-1}_{\mu_k^{-1}(j)}$ which is the statement that the $\bar{*}$ is self-distributive. ■

Prop. 3.1 *Let R be a finite rack of order n. There exists a positive integer l such that, for any j in $\{1, 2, \ldots, n\}$, $\mu_j^l = ()$, where $()$ stands for the identity permutation.*

Proof: Write the μ_i's as products of disjoint cycles and let Σ stand for the set of all these cycles, except 1-cycles. Then l can be taken to be the least common multiplier of the lengths of the cycles in Σ. ■

For the purpose of the discussion in this section we will fix two racks, R and R', of finite order n but otherwise arbitrary. The operations will be denoted $*$ and $*'$, respectively. The sequences of their permutations will be denoted $(\mu_1, \ldots, \mu_n) \subset S_n$, and $(\mu_1', \ldots, \mu_n') \subset S_n$, respectively.

Def. 3.7 *A* **rack homomorphism** *between two racks, R and R', is a map, α, between the underlying sets, such that $\alpha(i * j) = \alpha(i) *' \alpha(j)$, for all i, and j. If α is a bijection then it is a* **rack isomorphism**.

Clearly, if two racks are isomorphic they have to have the same order. Moreover,

Prop. 3.2 *If a k-prack, R, is isomorphic to a k'-prack, R', then $k = k'$.*

Proof: Assume to the contrary and let $k < k'$. Let α be the isomorphism from the k'-prack to the k-prack. Let $i_1, \ldots, i_{k'}$ be all elements of the k'-prack which violate the "quandle condition". Then $\alpha(i_j) *' \alpha(i_j) \neq \alpha(i_j)$ hence the image cannot be a k-prack.■

Furthermore,

Thm. 3.2 *α is a rack isomorphism of R with R' if and only if:*

$$\mu'_{\alpha(j)} = \alpha\mu_j\alpha^{-1}$$

for each $j \in \{1, 2, \ldots, n\}$.

Proof: For any i, and $j \in X$, $\alpha(i * j) = \alpha(i) *' \alpha(j)$, which, in terms of the sequences of permutations is $\alpha(\mu_j(i)) = \mu'_{\alpha(j)}(\alpha(i))$, and since α is a bijection:

$$\mu'_{\alpha(j)} = \alpha\mu_j\alpha^{-1}$$

and conversely. ■

In this way a rack isomorphism α, being a permutation from S_n, gives rise to an action on S_n by conjugation

$$\alpha \longmapsto \hat{\alpha} : \begin{array}{l} S_n \longrightarrow S_n \\ \mu \longmapsto \alpha\mu\alpha^{-1} \end{array}$$

which induces a bijection between the sequences of permutations of the two racks, according to:

$$\mu'_{\alpha(j)} = \alpha\mu_j\alpha^{-1}$$

4 Invariants of Racks - Basics

Theorem 3.2 gives necessary conditions on two sequences of permutations in order for the corresponding racks to be isomorphic. Before looking at some examples, here is a

Def. 4.1 *Let $\nu \in S_n$ be a permutation whose decomposition into disjoint cycles is (modulo ordering of the cycles),*

$$\nu = (i_1^1, \ldots, i_{n_1}^1)(i_1^2, \ldots, i_{n_2}^2)\ldots(i_1^k, \ldots, i_{n_k}^k)$$

We call the list of the lengths of the cycles, $\{n_1, \ldots, n_k\}$, the **pattern** *of ν.*

Racks	Profile	Sequences of Permutations
R	$(\{1, 1, 1, 1\}, \{1, 1, 1, 1\}, \{1, 1, 2\}, \{1, 1, 2\})$	((), (), (1 2)(3)(4), (1 2)(3)(4))
S		((), (), (1)(2)(3 4), (1)(2)(3 4))
T	$(\{1, 3\}, \{1, 3\}, \{1, 3\}, \{1, 3\})$	((1 2 3)(4), (1 2 3)(4), (1 2 3)(4), (1 2 3)(4))
U		((1 2 3)(4), (1 2 3)(4), (1 2 3)(4), (1 3 2)(4))
V		((1)(2 3 4), (1 4 3)(2), (1 2 4)(3), (1 3 2)(4))

Table 4.1: Racks and Their Profiles

with the following understanding,

Def. 4.2 *A list is a set with (possible) repeats.*

The notation for list will be the same as for sets i.e., the elements will be involved by curled braces. It will be clear either from context or by explicit mention which object we mean.

Consider the following five racks of order four given by their sequences of permutations where the permutations are broken down into products of disjoint cycles.

$$R: \quad \big((), (), (12)(3)(4), (12)(3)(4)\big)$$

$$S: \quad \big((), (), (1)(2)(34), (1)(2)(34)\big)$$

$$T: \quad \big((123)(4), (123)(4), (123)(4), (123)(4)\big)$$

$$U: \quad \big((123)(4), (123)(4), (123)(4), (132)(4)\big)$$

$$V: \quad \big((1)(234), (2)(143), (3)(124), (4)(132)\big)$$

Clearly, none of the first two is isomorphic to any of the last three racks since conjugation preserves the pattern of the permutations. In this way, we define a first invariant of rack isomorphism.

Def. 4.3 *Let R be a rack with sequence of permutations $(\mu_1, \dots, \mu_n) \subset S_n$. Let $\{k_1^i, \dots, k_{m_i}^i\}$ be the pattern of μ_i for each $i \in \{1, \dots, n\}$. We call the sequence of patterns $\big(\{k_1^1, \dots, k_{m_1}^1\}, \dots, \{k_1^n, \dots, k_{m_n}^n\}\big)$ the* **profile** *of R.*

Prop. 4.1 *The profile is an invariant under rack isomorphism.*

Proof: From Theorem 3.2 and remark right after it, any rack isomorphism establishes a one-to-one correspondence between the sequences of permutations of the racks under study via conjugation by a fixed permutation. Since conjugation preserves the pattern the result follows. ■

We can now subdivide these five racks, R, S, T, U, and V, into two classes according to profile (see Table 4.1). Note that, for the first profile, $\big(\{1, 1, 1, 1\}, \{1, 1, 1, 1\}, \{1, 1, 2\}, \{1, 1, 2\}\big)$, there are two distinct patterns, $\{1, 1, 1, 1\}$ and $\{1, 1, 2\}$, each of them realized in just one way with multiplicity two, for each rack (see Table 4.2). As for the second profile, $\big(\{1, 3\}, \{1, 3\}, \{1, 3\}, \{1, 3\}\big)$, there is only one distinct pattern which is realized in different ways for each of the different racks, T, U, and V (see Table 4.3). Now T cannot be isomorphic either to U or to V because the isomorphism would send the four equal permutations into another four equal permutations and neither U nor V have such a sequence of permutations. Analogously U cannot be isomorphic to the other two and V cannot be isomorphic to the other two.

In this way we give the following

Racks	Profile	Distinct Patterns	...realized as...
R	$(\{1, 1, 1, 1\}, \{1, 1, 1, 1\}, \{1, 1, 2\}, \{1, 1, 2\})$	$\{1, 1, 1, 1\}$	(), ()
		$\{1, 1, 2\}$	(1 2)(3)(4), (1 2)(3)(4)
S		$\{1, 1, 1, 1\}$	(), ()
		$\{1, 1, 2\}$	(1)(2)(3 4), (1)(2)(3 4)

Table 4.2: How the profile is realized for R and S

Racks	Profile	Distinct Patterns	...realized as...
T	$(\{1, 3\}, \{1, 3\}, \{1, 3\}, \{1, 3\})$	$\{1, 3\}$	(1 2 3)(4), (1 2 3)(4), (1 2 3)(4), (1 2 3)(4)
U		$\{1, 3\}$	(1 2 3)(4), (1 2 3)(4), (1 2 3)(4)
			(1 3 2)(4)
V		$\{1, 3\}$	(1)(2 3 4)
			(1 4 3)(2)
			(1 2 4)(3)
			(1 3 2)(4)

Table 4.3: How the profile is realized for T, U and V

Def. 4.4 *Suppose R is a rack of finite order n with sequence of permutations $(\mu_1, \ldots, \mu_n) \subset S_n$ and profile $\left(\{n_1^1, \ldots, n_{k_1}^1\}, \ldots, \{n_1^n, \ldots, n_{n_{k_n}}^n\}\right)$.*

Assume further that the sequence of **distinct** *patterns is $\left(\{n_1^1, \ldots, n_{n_1}^1\}, \ldots, \{n_1^m, \ldots, n_{n_m}^m\}\right)$ with $m \leq n$, with r^i repeats for the i-th distinct pattern, corresponding to r_1^i identical permutations, ρ_1^i, ..., $r_{j_i}^i$ identical permutations, $\rho_{j_i}^i$, such that $r_1^i + \cdots + r_{j_i}^i = r^i$ and $\rho_k^i \neq \rho_l^i$ for $k \neq l$.*

For each of the distinct patterns, say $\{n_1^i, \ldots, n_{n_i}^i\}$ consider the ordered pair $\left(\{n_1^i, \ldots, n_{n_i}^i\}, \{r_1^i, \ldots, r_{n_i}^i\}\right)$, whose first term is this pattern and whose second term is the list of multiplicities corresponding to this pattern, $\{r_1^i, \ldots, r_{n_i}^i\}$.

We call the sequence of these ordered pairs, one ordered pair per distinct pattern,

$$\left(\left(\{n_1^1, \ldots, n_{n_1}^1\}, \{r_1^1, \ldots, r_{j_1}^1\}\right), \ldots, \left(\{n_1^m, \ldots, n_{n_m}^m\}, \{r_1^m, \ldots, r_{j_m}^m\}\right)\right)$$

the **detail** *of R.*

Def. 4.5 *Keeping the notation of the previous definition, we call the sequence*

$$\left(\left(\{n_1^1, \ldots, n_{n_1}^1\}, \{(r_1^1, \rho_1^1), \ldots, (r_{j_1}^1, \rho_{j_1}^1\}\right), \ldots, \left(\{n_1^m, \ldots, n_{n_m}^m\}, \{(r_1^m, \rho_1^m), \ldots, (r_{j_m}^m, \rho_{j_m}^m)\}\right)\right)$$

the **absolute detail** *of R.*

Prop. 4.2 *The detail is an invariant under rack isomorphism.*

Proof: Omitted since it is similar to the proof of the previous proposition. ■

We can now break down the profile $\left(\{1,3\}, \{1,3\}, \{1,3\}, \{1,3\}\right)$ into three distinct details (see Table 4.4).

Cor. 4.1 *Isomorphic racks have the same detail. Racks with the same detail have the same profile.*

Proof: Clear from the discussion above. ■

The converses are not true. Specifically, we saw that racks T, U, and V have the same profile but different details, and R and S although they have the same detail, they are not isomorphic, since R is a quandle and S is a 2-prack.

Rack	Detail	Absolute Detail
T	$\big((\{1, 3\}, \{4\})\big)$	$\big((\{1, 3\}, \{(4, (1\ 2\ 3)(4))\})\big)$
U	$((\{1, 3\}, \{1, 3\}))$	$\big((\{1, 3\}, \{(1, (1\ 3\ 2)(4)), (3, (1\ 2\ 3)(4))\})\big)$
V	$\big((\{1, 3\}, \{1, 1, 1, 1\})\big)$	$\big((\{1, 3\}, \{(1, (1)(2\ 3\ 4)), (1, (1\ 4\ 3)(2)), (1, (1\ 2\ 4)(3)), (1, (1\ 3\ 2)(4))\})\big)$

Table 4.4: Profile $\{(1,3),(1,3),(1,3),(1,3)\}$ has different details

5 Invariants of Racks - More Examples

From the considerations of the previous Section we can extract a sequence of instructions for a partial classification of racks for each order n. Upon selection of the order n, all racks of that order are generated, each one being specified by its sequence of permutations. Then they are sorted according to their profiles. Then within each profile, they are sorted according to their detail. Then, within each detail, they are sorted according to being a k-prack for each k in $\{0,1,2,\ldots,n\}$. Of course, we still end up with a number of different but isomorphic racks. That is why we now introduce some more invariants of racks by discussing examples.

The Laurent polynomials have a natural structure of quandle given by setting $a*b := Ta + (1-T)b$ for any a, $b \in \mathbb{Z}[T,T^{-1}]$. This is an infinite quandle. In order to obtain finite quandles, we take the coefficients of the polynomials from $\mathbb{Z}_n$ and take the polynomials from the quotient of $\mathbb{Z}_n[T,T^{-1}]$ by some principal ideal, being careful in the choice of n and ideal so that the right-invertibility axiom holds. These are the so-called finite Alexander quandles, denoted $\mathbb{Z}_n[T,T^{-1}]/(h(T))$, where $(h(T))$ is the principal ideal generated by polynomial h. For each n greater than 2, the dihedral quandle R_n is isomorphic with the finite Alexander quandle $\mathbb{Z}_n[T,T^{-1}]/(T+1)$ ([10], [15]).

It is known that, for any prime order $p \geq 3$, there are $p-2$ non-trivial quandles pairwise non-isomorphic, which are isomorphic with the linear Alexander quandles of order p i.e., $\mathbb{Z}_p[T,T^{-1}]/(T-m)$ where m is from $\{2,3,\ldots,p-1\}$ and $a*b = Ta + (1-T)b$ in the indicated quotient ([15]). We will now concentrate on how to tell these racks apart for $p=5$ using the techniques developed in the previous Section. There are three non-trivial linear Alexander quandles of order 5, $\mathbb{Z}_5[T,T^{-1}]/(T-2)$, $\mathbb{Z}_5[T,T^{-1}]/(T-3)$, and $\mathbb{Z}_5[T,T^{-1}]/(T-4)$. The sequences of permutations are, respectively:

$$\mu_1 = (1)(2354), \quad \mu_2 = (2)(1534), \quad \mu_3 = (3)(1452), \quad \mu_4 = (4)(1325), \quad \mu_5 = (5)(1243)$$

(see multiplication table in Table 5.1 where, for instance $2*1=3$) ,

	1	2	3	4	5
1	1	5	4	3	2
2	3	2	1	5	4
3	5	4	3	2	1
4	2	1	5	4	3
5	4	3	2	1	5

Table 5.1: $\mathbb{Z}_5[T,T^{-1}]/(T-2)$ Multiplication Table

$$\mu_1 = (1)(2453), \quad \mu_2 = (2)(1435), \quad \mu_3 = (3)(1254), \quad \mu_4 = (4)(1523), \quad \mu_5 = (5)(1342)$$

(see multiplication table in Table 5.2) , and,

$$\mu_1 = (1)(25)(34), \quad \mu_2 = (2)(13)(45), \quad \mu_3 = (3)(15)(24), \quad \mu_4 = (4)(12)(35), \quad \mu_5 = (5)(14)(23)$$

(see multiplication table in Table 5.3).

	1	2	3	4	5
1	1	4	2	5	3
2	4	2	5	3	1
3	2	5	3	1	4
4	5	3	1	4	2
5	3	1	4	2	5

Table 5.2: $\mathbb{Z}_5[T,T^{-1}]/(T-3)$ Multiplication Table

	1	2	3	4	5
1	1	3	5	2	4
2	5	2	4	1	3
3	4	1	3	5	2
4	3	5	2	4	1
5	2	4	1	3	5

Table 5.3: $\mathbb{Z}_5[T,T^{-1}]/(T-4)$ Multiplication Table

Now $\mathbb{Z}_5[T,T^{-1}]/(T-4)$ is not isomorphic with $\mathbb{Z}_5[T,T^{-1}]/(T-3)$ nor with $\mathbb{Z}_5[T,T^{-1}]/(T-2)$ by inspection of profiles. As for $\mathbb{Z}_5[T,T^{-1}]/(T-3)$ and $\mathbb{Z}_5[T,T^{-1}]/(T-2)$, they have the same detail. Inspection of their multiplication tables shows that that of $\mathbb{Z}_5[T,T^{-1}]/(T-3)$ is symmetric with respect to the diagonal whereas that of $\mathbb{Z}_5[T,T^{-1}]/(T-2)$ is not. Clearly, an isomorphism would preserve this symmetry hence $\mathbb{Z}_5[T,T^{-1}]/(T-2)$ and $\mathbb{Z}_5[T,T^{-1}]/(T-3)$ are not isomorphic. We further remark that these two quandles form an example of a rack which is not isomorphic to its dual. In fact, the sequence of permutations, $(\nu_1, \nu_2, \nu_3, \nu_4, \nu_5)$, of the dual of $\mathbb{Z}_5[T,T^{-1}]/(T-3)$ is, omitting 1-cycles,

$$\nu_1 = (2453)^{-1} = (3542), \quad \nu_2 = (1435)^{-1} = (5341), \quad \nu_3 = (1254)^{-1} = (4521),$$
$$\nu_4 = (1523)^{-1} = (3251), \quad \nu_5 = (1342)^{-1} = (2431)$$

which is the sequence of permutations of $\mathbb{Z}_5[T,T^{-1}]/(T-2)$. Since these two racks are not isomorphic the remark follows.

We will now develop the notion of symmetry. Let $R = (X, *)$ and $(\mu_1, \ldots, \mu_n)$ have the usual meanings.

Def. 5.1 *Given a rack, R, we call* **opposite** *of R, notation $R^o = (X, *^o)$, the algebraic structure whose underlying set is again $X = \{1, 2, \ldots, n\}$ and whose binary operation is given by:*

$$i *^o j := j * i = \mu_i(j)$$

for any i, and j in $\{1, 2, \ldots, n\}$.

Def. 5.2 *Keeping the notation above, a rack is called* **symmetric** *if for any i, and j in $\{1, 2, \ldots, n\}$, $i *^o j = i * j$.*

Prop. 5.1 *Symmetry is an invariant under rack isomorphism.*

Proof: Let α denote the isomorphism. Then $\alpha(i) *'^o \alpha(j) = \alpha(j) *' \alpha(i) = \alpha(j * i) = \alpha(i *^o j) = \alpha(i * j) = \alpha(i) *' \alpha(j)$. ■

When is the opposite of a rack (resp., quandle) a rack (resp. quandle)? Clearly,

Prop. 5.2 *If $R = (X, *)$ is a quandle, then all elements in R^o satisfy the quandle condition i.e., $i *^o i = i$ for all i.*

Proof: Omitted. ■

What about right-invertibility?

Prop. 5.3 *Let $R = (X, *)$ be a finite rack. $*^o$ is right-invertible if and only if, for any i, and j in $\{1, 2, \ldots, n\}$, there exists a unique x in $\{1, 2, \ldots, n\}$ such that $i * x = j$.*

Proof: If R^o is right-invertible then, for any i, and j in $\{1, 2, \ldots, n\}$, there exists a unique x in $\{1, 2, \ldots, n\}$ such that $j = x *^o i = i * x$ and vice-versa. ■

The racks that satisfy the condition on Proposition 5.3 are both left- and right-invertible. An algebraic structure whose binary operation is both left- and right-invertible is called a quasi-group ([16]). Clearly, $\mathbb{Z}_5[T, T^{-1}]/(T-3)$ is a quasi-group since being symmetric, its opposite is again a quandle. Furthermore, dihedral quandles of any odd order, say $2m+1$, are quasi-groups since for any i, and j in $\{1, 2, \ldots, 2m+1\}$ the equation $i * x = j$ is equivalent to $2x = i + j$, which, upon multiplication on both sides by $m + 1$, yields the unique $x = (m+1)(i+j)$. Straightforward calculations show also that for each prime order p the non-trivial (linear) Alexander quandles are quasi-groups. We will now give a partial answer to the question of when the opposite of a quandle is again a quandle. We start out by noting that

Prop. 5.4 *If $(X, *)$ is an Alexander quandle, then its opposite is self-distributive.*

Proof: What we have to prove is that $(i *^o j) *^o k = (i *^o k) *^o (j *^o k)$, that is, $k * (j * i) = (k * j) * (k * i)$, that is, $Tk + (1-T)\big(Tj + (1-T)i\big) = T\big(Tk + (1-T)j\big) + (1-T)\big(Tk + (1-T)i\big)$ and this is now a straightforward calculation. ■

In this way, Propositions 5.2 and 5.4 show that the opposite of any Alexander quandle satisfies the quandle axiom and the self-distributivity axiom. From the remarks made right before Proposition 5.4 we can say that for any odd order, say $2m+1$, the opposite of the dihedral quandle R_{2m+1} is again a quandle; and that the opposite of any non trivial linear Alexander quandle of any prime order is again a quandle.

We will now give an example of a quandle whose opposite is not self-distributive. In Table 5.4 we see the multiplication table of a quandle such that its opposite is not right-invertible. This is the octahedron quandle ([1]). Omitting 1-cycles, its sequence of permutations is

	1	2	3	4	5	6
1	1	5	2	3	4	1
2	3	2	6	2	1	5
3	4	1	3	6	3	2
4	5	4	1	4	6	3
5	2	6	5	1	5	4
6	6	3	4	5	2	6

Table 5.4: Octahedron Quandle Multiplication Table

$$\mu_1 = (2345), \quad \mu_2 = (1563), \quad \mu_3 = (1264), \quad \mu_4 = (1365), \quad \mu_5 = (1462), \quad \mu_6 = (2543)$$

We remark that, for the octahedron quandle, we have $1 * (2 * 3) = 1 * 6 = 1$ whereas $(1 * 2) * (1 * 3) = 5 * 2 = 6$, thus the opposite of the octahedron quandle is not self-distributive. Hence, the octahedron quandle is not an Alexander quandle.

In Proposition 5.3 we dealt with this property of having just one element connecting any two elements of the rack. This prompted us into the following. Let $R = (X, *)$ be a finite rack. For any i, and j in $\{1, 2, \ldots, n\}$ set:

$$N_{i,j} := \{m \in \mathbb{Z}_0^+ \mid \exists\, k_1, \ldots, k_m \in \{1, 2, \ldots, n\},\ \epsilon_1, \ldots, \epsilon_m \in \{\pm 1\} \,:\, j = (\cdots((i *^{\epsilon_1} k_1) *^{\epsilon_2} k_2) \cdots) *^{\epsilon_m} k_m\}$$

(where $*^{+1} := *$ and $*^{-1} := \bar{*}$). If $N_{i,j} \neq \emptyset$ set $m_{i,j} := \min N_{i,j}$, otherwise $m_{i,j} := 0$.

Def. 5.3 *Keeping the notation above, we say a rack is c-**connected** if, for all i, and j in $\{1, 2, \ldots, n\}$, $m(i, j) \neq \emptyset$ and*

$$c = \max\{m(i, j) \mid i, j \in \{1, 2, \ldots, n\}\}$$

*Otherwise, if there are i, and j in $\{1, 2, \ldots, n\}$, such that $m(i, j) = \emptyset$, then we say the rack is **not connected**.*

In this way, the octahedron quandle is 2-connected.

Prop. 5.5 *Keeping the notation above, if a rack of finite order n is c-connected for $c > 0$, then $c \leq n$.*

Proof: Omitted. ■

We will now prove that c-connectedness is an invariant of racks under isomorphism after introducing the relevant object for this proof.

Def. 5.4 *Let $R = (X, *)$ be a finite rack. For each i in $\{1, 2, \ldots, n\}$ we call the set:*

$$\mathcal{O}_i := \{(\cdots((i *^{\epsilon_1} k_1) *^{\epsilon_2} k_2) \cdots) *^{\epsilon_m} k_m \mid m \in \mathbb{Z}_0^+,\, k_1, \ldots, k_m \in \{1, \ldots, n\},\, \epsilon_1, \ldots \epsilon_m \in \{\pm 1\}\}$$

the **orbit of** i.

Prop. 5.6 *Let α be a rack isomorphism between racks R and R'. For any i, let $\mathcal{O}_i$ and $\mathcal{O}'_i$ denote the orbit of i in R and R', respectively. Then α restricted to $\mathcal{O}_i$ is a bijection of $\mathcal{O}_i$ with $\mathcal{O}'_{\alpha(i)}$. Furthermore, α induces a bijection from the set of orbits of R to the set of orbits of R'.*

Proof: We just remark that

$$\alpha\Big(\mathcal{O}_i\Big) = \alpha\Big(\{(\cdots((i *^{\epsilon_1} k_1) *^{\epsilon_2} k_2) \cdots) *^{\epsilon_m} k_m \mid m \in \mathbb{Z}_0^+,\, k_1, \ldots, k_m \in \{1, \ldots, n\},\, \epsilon_1, \ldots \epsilon_m \in \{\pm 1\}\}\Big) =$$
$$= \{(\cdots((\alpha(i) {*'}^{\epsilon_1} \alpha(k_1)) {*'}^{\epsilon_2} \alpha(k_2)) \cdots) {*'}^{\epsilon_m} \alpha(k_m) \mid m \in \mathbb{Z}_0^+,\, k_1, \ldots, k_m \in \{1, \ldots, n\},\, \epsilon_1, \ldots \epsilon_m \in \{\pm 1\}\}$$

■

Prop. 5.7 *c-connectedness is an invariant under rack isomorphism.*

Proof: Clear from proof of previous proposition. ■

Prop. 5.8 *Let R be a finite rack and pick any i. Then, $\mathcal{O}_i$ is a subrack of R.*

Proof: We will just note that $\mathcal{O}_i$ is closed under the $*$ and $\bar{*}$ operations. Consider the elements $(\cdots((j *^{\epsilon_1} k_1) *^{\epsilon_2} k_2) \cdots) *^{\epsilon_m} k_m$ and $(\cdots((j' *^{\epsilon'_1} k'_1) *^{\epsilon'_2} k'_2) \cdots) *^{\epsilon'_{m'}} k'_{m'}$ in $\mathcal{O}_i$. Then

$$(\cdots((j *^{\epsilon_1} k_1) *^{\epsilon_2} k_2) \cdots) *^{\epsilon_m} k_m *^{\epsilon} (\cdots((j' *^{\epsilon'_1} k'_1) *^{\epsilon'_2} k'_2) \cdots) *^{\epsilon'_{m'}} k'_{m'} = (\cdots((j *^{\epsilon''_1} k''_1) *^{\epsilon''_2} k''_2) \cdots) *^{\epsilon''_{m''}} k''_{m''}$$

since in the left-hand side of the equality, j is the leftmost element. Then $\mathcal{O}_i$ is closed under the $*$ and $\bar{*}$ operations. ■

6 Indecomposability vs. Transitivity

In this Section we briefly discuss indecomposability and transitivity of racks and quandles.

Def. 6.1 *([1]) A* **decomposition** *of a rack $R = (X, *)$ is a disjoint union $X = X_1 \sqcup X_2$ such that $(X_1, *)$ and $(X_2, *)$ are subracks of $R = (X, *)$ (in particular, X_1 and X_2 are both non-empty). R is* **decomposable** *if it admits a decomposition and* **indecomposable** *otherwise.*

Def. 6.2 *([20]) A rack $R = (X, *)$ is said* **transitive** *if it is c-connected for some $c > 0$.*

Prop. 6.1 *A finite rack is indecomposable if and only if it is transitive.*

Proof: See [1]. ■

Notice, moreover, that each of the two subracks in the definition of decomposability above satisfy the following

Def. 6.3 *A subrack $(X_o, *)$ of a rack $R = (X, *)$ is said* **stable** *if, for any i_o in X_o and for any j in X, $i_o * j \in X_o$.*

(see [1] for a proof). We remark, however, that a rack may be transitive and still contain subracks. These subracks will not be stable, in general. Consider, for instance, R_9. It is a transitive rack - see remarks after Proposition 5.3. On the other hand, it contains three copies of R_3 namely, $R_3^1 = \{1, 4, 7\}$, $R_3^2 = \{2, 5, 8\}$, $R_3^3 = \{3, 6, 9\}$, see Table 6.1. Mind the unusual ordering of the underlying set and the boldface in order to bring out the three subracks. Moreover, these subracks are not stable: for instance, $1 * 2 = 3$ and $1 \in R_3^1$ whereas $3 \notin R_3^1$.

	1	4	7	2	5	8	3	6	9
1	**1**	**7**	**4**	3	9	6	5	2	8
4	**7**	**4**	**1**	9	6	3	2	8	5
7	**4**	**1**	**7**	6	3	9	8	5	2
2	9	6	3	**2**	**8**	**5**	4	1	7
5	6	3	9	**8**	**5**	**2**	1	7	4
8	3	9	6	**5**	**2**	**8**	7	4	1
3	8	5	2	1	7	4	**3**	**9**	**6**
6	5	2	8	7	4	1	**9**	**6**	**3**
9	2	8	5	4	1	7	**6**	**3**	**9**

Table 6.1: R_9 Multiplication Table

7 Orbits and Δ-Orbits

In this section we begin by describing an algorithm for obtaining the orbits of a rack, given its sequence of permutations. This algorithm is prompted by the following Proposition.

Prop. 7.1 *Let R be a finite rack of order n with sequence of permutations $(\mu_1, \ldots, \mu_n)$ and assume the permutations are already broken down into products of disjoint cycles. Let Σ denote the set of all these disjoint cycles and suppose $\Sigma = \Sigma_1 \bigsqcup \Sigma_2$ such that cycles from Σ_1 only move elements from X_1 and cycles from Σ_2 only move elements from X_2 where X_1 and X_2 are disjoint subsets of $\{1, 2, \ldots, n\}$ the underlying set of R. Then R is decomposable.*

Proof: Pick x_i in X_i. Then, for any j in X, $\mu_j(x_i) \in X_i$, for each cycle in the permutations either moves an element of X_1 or (exclusively) an element of X_2. ■

We now describe the algorithm for obtaining the orbits of a rack given its sequence of permutations:

Fix a finite rack $R = (X, *)$ with sequence of permutations $(\mu_1, \ldots, \mu_n)$ and assume the permutations are already broken down into products of disjoint cycles. Let Σ be the set of all cycles used in expressing the μ_i's as products of disjoint cycles, except 1-cycles. Σ is a finite set. If Σ is the empty set, then each μ_i is the product of 1-cycles i.e.,

$$\mu_i = (1)(2)(3)\cdots(n) = ()$$

and so R is the trivial rack of order n, T_n. Otherwise, assume $\Sigma = \{\sigma_1, \ldots, \sigma_m\}$ for some positive integer m, where

$$\sigma_k = (i_1^k \cdots i_{m_k}^k) \qquad 1 \leq k \leq m \qquad 1 < m_k \leq n$$

and $i_j^k \in \{1, \ldots, n\}$. Set $s^k = \{i_1^k, i_2^k, \ldots, i_{m_k}^k\}$, for each k. So, the s^k is the set of the elements which are moved by σ_k. If $X \setminus \bigcup_{k=1}^m s^k$ is not empty, let $\{o_1, \ldots, o_l\} = X \setminus \bigcup_{k=1}^m s^k$. Then each o_i is a (one element) orbit. Now for the remaining orbits.

Let $E_1^1 = \{i \mid s^1 \cap s^i \neq \emptyset\}$ and let $F_1^1 = \{i \mid s^1 \cap s^i = \emptyset\}$.

Set

$$\mathcal{O}_1^1 := \bigcup_{i \in E_1^1} s^i$$

If $E_1^1 = \{1\}$, then set $\mathcal{O}_1 = \mathcal{O}_1^1$. Otherwise set $j_1^1 = \min\left(E_1^1 \setminus \{1\}\right)$. Then let $E_2^1 = \{i \in F_1^1 | s^{j_1} \cap s^i \neq \emptyset\}$, and $F_2^1 = \{i \in F_1^1 \mid s^{j_1^1} \cap s^i = \emptyset\}$.

Set

$$\mathcal{O}_1^2 := \mathcal{O}_1^1 \cup \bigcup_{i \in E_2^1} s^i$$

If $E_2^1 = \{j_1^1\}$, then set $\mathcal{O}_1 = \mathcal{O}_1^2$. Otherwise set $j_2^1 = \min\big(E_2^1 \setminus \{j_1^1\}\big)$. Then let $E_3^1 = \{i \in F_2^1 \,|\, s^{j_2^1} \cap s^i \neq \emptyset\}$, and $F_3^1 = \{i \in F_2^1 \mid s^{j_2^1} \cap s^i = \emptyset\}$.

Set

$$\mathcal{O}_1^3 := \mathcal{O}_1^2 \cup \bigcup_{i \in E_3^1} s^i$$

Since we are dealing with a finite rack, there has to be a positive integer k such that $E_k^1 = \{j_{k-1}^1\}$. Then, set

$$\mathcal{O}_1 = \mathcal{O}_1^k$$

and set $j_0^2 := \min F_{k-1}^1$. This will be the beginning of the construction of the second orbit. Let $E_1^2 = \{i \in F_{k-1}^1 \mid s^{j_0^2} \cap s^i \neq \emptyset\}$ and let $F_1^2 = \{i \in F_{k-1}^1 \mid s^{j_0^2} \cap s^i = \emptyset\}$. Then set

$$\mathcal{O}_2^1 := \bigcup_{i \in E_1^2} s^i$$

If $E_1^2 = \{j_0^2\}$, then set $\mathcal{O}_2 = \mathcal{O}_2^1$. Otherwise set $j_1^2 = \min\big(E_1^2 \setminus \{j_0^2\}\big)$, and proceed as for the previous orbit. Since we are dealing with a finite rack the process has to stop at some step yielding, say, N orbits, $\mathcal{O}_1, \ldots, \mathcal{O}_N$ with more than one element.

The next results address the relations between profile and orbits of racks.

Prop. 7.2 *Let $R = (X, *)$ be a finite rack of order n. The permutations corresponding to the elements of a given orbit have all the same pattern.*

Proof: Let $\mathcal{O}_{i_0}$ denote the orbit of i_0. Then for any $i \in \mathcal{O}_{i_0}$, we have $i = (\cdots((i_0 * i_1) * i_2) \cdots) * i_m$. Then

$$\begin{aligned} \mu_i &= \mu_{(\cdots((i_0*i_1)*i_2)\cdots)*i_m} = \mu_{\mu_{i_m}(\cdots((i_0*i_1)*i_2)\cdots)} = \mu_{i_m}\mu_{((\cdots((i_0*i_1)*i_2)\cdots))}\mu_{i_m}^{-1} = \cdots = \\ &= \mu_{i_m}\cdots\mu_{i_1}\mu_{i_0}\mu_{i_1}^{-1}\cdots\mu_{i_m}^{-1} \end{aligned}$$

Since the permutation corresponding to any i in $\mathcal{O}_{i_0}$ is conjugate to the permutation corresponding to i_0 then they have the same pattern. The result follows. ■

Cor. 7.1 *Let $R = (X, *)$ be an indecomposable finite rack of order n. Then its permutations have all the same pattern. In particular, the profile is a constant sequence and the detail is a singleton.*

Proof: Since an indecomposable rack is transitive, the result follows from the proof of the previous proposition. ■

Def. 7.1 *Let $R = (X, *)$ be a finite rack of order n. For each i in $\{1, 2, \ldots, n\}$ consider the sequence (i_k) defined in the following way. $i_1 = i$, and, for any $k \geq 1$, $i_{k+1} = i_k * i_k$. We call the set of its terms the* **Δ-orbit of** *i, or simply the Δ_i* **orbit**. *The length of the Δ-orbit is the number of elements in it.*

We remark that the Δ-orbits can be defined for infinite racks, but, if we are dealing with finite racks, then the Δ_i orbits are finite sets. Furthermore, for quandles, Δ-orbits are singletons.

Prop. 7.3 *Let $R = (X, *)$ be a finite rack of order n. For an arbitrary i in $\{1, 2, \ldots, n\}$, consider the sequence introduced in Definition 7.1. This sequence is periodic and the length of Δ_i is its period. Moreover, for any $k \geq 1$, $i_{k+1} = \mu_i^k(i)$.*

Proof: We start out by proving the last claim, for any $k \geq 1$, $i_{k+1} = \mu_i^k(i)$. We have $i_2 = i * i = \mu_i(i) = \mu_i^1(i)$. Suppose there is a positive integer r such that $i_{r+1} = \mu_i^r(i)$. Then,

$$\begin{aligned} i_{r+2} &= i_{r+1} * i_{r+1} = \mu_{i_{r+1}}(i_{r+1}) = \mu_{\mu_i^r(i)}(\mu_i^r(i)) = \mu_{\mu_i(\mu_i^{r-1}(i))}(\mu_i^r(i)) = \\ &= \mu_i\mu_{\mu_i^{r-1}(i)}\mu_i^{-1}(\mu_i^r(i)) = \cdots = \mu_i^r\mu_i\mu_i^{-r}(\mu_i^r(i)) = \mu_i^{r+1}(i) \end{aligned}$$

thus proving the claim.

Since R is finite, there is a positive integer m such that $i_m * i_m$ is in $\{i_k \mid 1 \leq k \leq m\}$. Suppose $i_m * i_m = i_l$ with l not equal to 1. Then $i_{l+1} = i_l * i_l$, $\ldots$ $, i_m = i_{m-1} * i_{m-1}$, $i_l = i_m * i_m$ $\ldots$, and so on, keeping on repeating the subsequence $(i_l, \ldots, i_m)$. So for any $k \geq m-1$,

$$i = i_1 \neq i_{k+1} * i_{k+1} = \mu_{i_{k+1}}(i_{k+1}) = \mu_{\mu_i^k(i)}(\mu_i^k(i)) = \mu_i^k \mu_i \mu_i^{-k}(\mu_i^k(i)) = \mu_i^{k+1}(i)$$

Via Proposition 3.1 we know that there are infinitely many positive integers r such that μ_i^r is the identity permutation which clearly contradicts the preceding calculations. Hence $l = 1$ i.e., the sequence $i = i_1$ and $i_{k+1} = i_k * i_k$ for any $k \geq 1$, is periodic and the length of the Δ_i orbit is its period. ■

Prop. 7.4 *Let $R = (X, *)$ be a finite rack of order n. The permutations corresponding to the elements of a given Δ-orbit are all equal. Furthermore, for any i in $\{1, 2, \ldots, n\}$, $\mu_i = (i_1\ i_2 \ldots i_m)\pi$, where m is the length of the Δ-orbit, $(i_1, i_2, \ldots, i_m)$ is the sequence introduced in Definition 7.1, and π is a permutation of the remaining elements i.e., $\{1, 2, \ldots, n\} \setminus \{i_1, i_2, \ldots, i_m\}$*

Proof: Fix an arbitrary i in $\{1, 2, \ldots, n\}$ and consider the sequence (i_k) introduced in Definition 7.1. We have $\mu_{i_2} = \mu_{i*i} = \mu_{\mu_i(i)} = \mu_i \mu_i \mu_i^{-1} = \mu_i$. Suppose $\mu_{i_k} = \mu_i$. Then $\mu_{i_{k+1}} = \mu_{i_k * i_k} = \mu_{\mu_{i_k}(i_k)} = \mu_{i_k} \mu_{i_k} \mu_{i_k}^{-1} = \mu_{i_k} = \mu_i$ which establishes the first claim in the statement. For the second claim, we know from the previous Proposition that $i_{k+1} = \mu_i^k(i)$, for all $k \geq 1$. Then, either $m = 1$ and $\mu_i(i) = i$ or $m > 1$ and i is moved to $\mu_i(i)$ which is moved to $\mu_i^2(i)$ and so on and so forth until i is reached again. The proof is complete. ■

Prop. 7.5 *Let $R = (X, *)$ be a finite rack of order n. Suppose there are elements i and j in X such that $\Delta_i \cap \Delta_j$ is non-empty. Then $\Delta_i = \Delta_j$.*

Proof: Let $\Delta_i = \{i_m | m \in \mathbb{Z}^+\}$ and $\Delta_j = \{j_m | m \in \mathbb{Z}^+\}$ where the i_k and j_k have the same meaning as before. Since R is a finite rack, these sequences are periodic. Since their intersection is not empty then there exist k and k' in $\mathbb{Z}^+$ such that $i_k = j_{k'}$. Then, by induction, if there exists p such that $i_{k+p} = j_{k'+p}$, then $i_{k+p} * i_{k+p} = j_{k'+p} * j_{k'+p}$ i.e., $i_{k+p+1} = j_{k'+p+1}$ and since the (i_m) and (j_m) sequences are periodic, the result follows. ■

Prop. 7.6 *Let α be a rack isomorphism between racks R and R'. For any i, let Δ_i and Δ'_i denote the Δ-orbit of i in R and R', respectively. Then α restricted to Δ_i is a bijection of Δ_i with $\Delta'_{\alpha(i)}$. Furthermore, α induces a bijection from the set of Δ-orbits of R to the set of Δ-orbits of R'.*

Proof: Let $\Delta_i = \{i_k \mid k \in \mathbb{Z}^+\}$, where the sequence (i_k) has the same meaning as in Definition 7.1. Then

$$\alpha(\Delta_i) = \alpha\Big(\{i_k \mid k \in \mathbb{Z}^+\}\Big) = \{\alpha(i_k) \mid k \in \mathbb{Z}^+\} = \Delta_{\alpha(i)}$$

noting that $\alpha(i_1) = \alpha(i)$ and, for any k, $\alpha(i_{k+1}) = \alpha(i_k * i_k) = \alpha(i_k) *' \alpha(i_k)$. ■

Prop. 7.7 *Let R be a finite rack of order n and pick i in $\{1, 2, \ldots, n\}$. Then Δ_i, the Δ-orbit of i, is a subrack of R.*

Proof: We will just show that Δ_i is closed under the $*$ operation. Pick any two elements in Δ_i, $i_{k'}$ and i_k. Due to the periodicity of the sequence (i_n) then $i_{k'} = i_{k+p}$, for a given p. We will prove by induction on p that $i_{k'} * i_k (= i_{k+p} * i_k) = i_{k+p} * i_{k+p}$, thereby proving it is an element of Δ_i. For $p = 1$ we have, $i_{k+1} * i_k = \big(i_k * i_k\big) * i_k = \big(i_k * i_k\big) * \big(i_k * i_k\big) = i_{k+1} * i_{k+1}$. Now assume that for some p it is true that $i_{k+p} * i_k = i_{k+p} * i_{k+p}$. Then, $i_{k+p+1} * i_k = \big(i_{k+p} * i_{k+p}\big) * i_k = \big(i_{k+p} * i_k\big) * \big(i_{k+p} * i_k\big) = \big(i_{k+p} * i_{k+p}\big) * \big(i_{k+p} * i_{k+p}\big) = i_{k+p+1} * i_{k+p+1}$, an element of Δ_i. ■

8 Racks Given Their Profiles

In this section we express the possible representatives of the equivalence classes of racks given specific profiles. As usual, let $R = (X, *)$ be a rack of order n and $(\mu_1, \ldots, \mu_n)$ be its sequence of permutations.

Thm. 8.1 *Suppose one of the permutations of a finite rack of order n is a cycle of length n. Then, the sequence of permutations of this rack is constant. Moreover there is only one such rack of this order (up to isomorphism). This rack can be taken to be the C_n rack i.e., the cyclic rack of order n.*

Proof: Let $\mu_i = (i_1\ i_2\ \cdots\ i_n)$ where, without loss of generality, we take $i_1 = i$. Then, by Proposition 7.4, $\{1, 2, \dots, n\}$ is the Δ_i-orbit which contains all elements of the rack. Again by Proposition 7.4, $\mu_j = (i_1\ i_2\ \cdots\ i_n)$, for all j in $\{1, 2, \dots, n\}$.

Now consider the assignment $\alpha(i_k) = k$, for all k in $\{1, 2, \dots, n\}$. This is a rack isomorphism from the rack under study to the cyclic rack of order n, C_n, which finishes the proof. ■

We next address the case of a prack of order n with constant profile $(\{m, n-m\}, \dots, \{m, n-m\})$. For clarity, we split this study into Theorem 8.2, concerning $m = 1$, Corollary 8.1, concerning $1 < m < n-m$, and Corollary 8.2, concerning $m = n-m$. We recall that the Euler φ-function is, for each positive integer n, the number of positive integers relatively prime to, and less than n.

Thm. 8.2 *Any prack of order $n > 2$ with constant profile*

$$(\{1, n-1\}, \dots, \{1, n-1\})$$

is decomposable and is isomorphic to a prack given by the following sequence of permutations:

$$\begin{aligned} \mu_1 = \mu_2 = \quad \cdots \quad &= \mu_{n-1} = (1\ 2\ \cdots\ n-1)(n), \\ \mu_n &= (1\ 2\ \cdots\ n-1)^k(n) \end{aligned}$$

where k is relatively prime to $n-1$.

Moreover, there are exactly $\varphi(n-1)$ such pracks up to isomorphism, one per each k relatively prime to $n-1$ $(1 \leq k < n-1)$.

Proof: Since each permutation fixes one element, then there has to be one which does not fix its own index, for otherwise the rack would be a quandle. So suppose $\mu_i(j) = j$. If necessary using the rack isomorphism $\alpha = (i\ 1)(j\ n)$ we may assume $\mu_1(n) = n$. Let $i_1 = 1$ and let the sequence (i_k) be as in Definition 7.1. Then by Proposition 7.4, $\mu_1 = \mu_2 = \cdots = \mu_{n-1} = (i_1\ i_2\ \cdots\ i_{n-1})(n)$. Moreover, $\mu_n(n) = n$ for otherwise suppose $\mu_n(n) = i_n \neq n$. Then $\mu_1 = \mu_{i_n} = \mu_{\mu_n(n)} = \mu_n \mu_n \mu_n^{-1} = \mu_n$ and so $\mu_n(n) = \mu_1(n) = n$. In particular, this prack is decomposable by Proposition 7.1. Using, if necessary, the isomorphism $\alpha(i_k) = k$, for $1 \leq k \leq n-1$, the first $n-1$ permutations of the sequence of permutations become all equal to $\mu_k = (1\ 2\ \cdots\ n-1)(n)$, for $1 \leq k \leq n-1$. For this prack the conditions $\mu_{\mu_j(i)} = \mu_j \mu_i \mu_j^{-1}$ are equivalent to saying that μ_n commutes with $(1\ 2\ \cdots\ n-1)(n)$ which is equivalent to saying that the $(n-1)$-cycle in μ_n is in the centralizer of $(1\ 2\ \cdots\ n-1)$ in S_{n-1}. The centralizer of an r-cycle in S_r is the cyclic group generated by that cycle. Thus, in the current situation we want to pick a power $(1\ 2 \dots n-1)^k$ which is an $(n-1)$-cycle which amounts to picking the k relatively prime to $n-1$. Hence the prack under study can only be isomorphic to a prack given by a sequence of permutations as in the statement and there will be at most $\varphi(n-1)$ pracks up to isomorphism with the indicated profile. We will next show that there are exactly $\varphi(n-1)$ such pracks by showing that any two such pracks with different k's are not isomorphic.

Suppose two such pracks are isomorphic. Specifically, assume that rack R with permutations $\mu_1 = \cdots = \mu_{n-1} = (1\ 2\ \cdots\ n-1)(n)$, $\mu_n = (1\ 2\ \cdots\ n-1)^k(n)$ is isomorphic with rack R' with permutations $\mu'_1 = \cdots = \mu'_{n-1} = (1\ 2\ \cdots\ n-1)(n)$, $\mu'_n = (1\ 2\ \cdots\ n-1)^{k'}(n)$, via an isomorphism α (with distinct integers $1 \leq k, k' < n-1$ both relatively prime to $n-1$). Since, by Proposition 7.6, isomorphisms map Δ-orbits to Δ-orbits of the same length, then $\alpha(n) = n$, and $\alpha(\{1, 2, \dots, n-1\}) = \{1, 2, \dots, n-1\}$. Hence, for any i in $\{1, 2, \dots, n-1\}$,

$$(1\ 2\ \cdots\ n-1)(n) = \mu'_{\alpha(i)} = \alpha \mu_i \alpha^{-1} = \alpha (1\ 2\ \cdots\ n-1)(n) \alpha^{-1}$$

i.e., α is in the centralizer of $(1\ 2\ \cdots\ n-1)(n)$ in S_n. Since $\alpha = \sigma \cdot (n)$ for some σ in S_{n-1} then σ is in the centralizer of $(1\ 2\ \cdots\ n-1)$ in S_{n-1}. Thus, $\sigma = (1\ 2\ \cdots\ n-1)^l$ for some l in $\{1, 2, \dots, n-1\}$. Finally,

$$\begin{aligned} (1\ 2\ \cdots\ n-1)^{k'}(n) = \mu'_n = \mu'_{\alpha(n)} = \alpha \mu_n \alpha^{-1} &= (1\ 2\ \cdots\ n-1)^l(n)(1\ 2\ \cdots\ n-1)^k(n)(1\ 2\ \cdots\ n-1)^{-l}(n) = \\ &= (1\ 2\ \cdots\ n-1)^k(n) \end{aligned}$$

Hence $k = k'$ and the result follows. ■

We remark there are indecomposable quandles of order n of constant profile $\{(1, n-1), \ldots, (1, n-1)\}$ - see, for instance, the quandles $\mathbb{Z}_5[T, T^{-1}]/(T-2)$ and $\mathbb{Z}_5[T, T^{-1}]/(T-3)$ in Section 5.

Cor. 8.1 *Any prack of order $n > 3$ with constant profile*

$$(\{m, n-m\}, \ldots, \{m, n-m\})$$

(where $1 < m < n-m$) is decomposable and is isomorphic to a prack given by the following sequence of permutations:

$$\begin{aligned} \mu_1 = \mu_2 = \quad \ldots \quad &= \mu_m = (1\ 2\ \cdots\ m)(m+1\ \cdots\ n)^l, \\ \mu_{m+1} = \mu_{m+2} = \quad \ldots \quad &= \mu_n = (1\ 2\ \cdots\ m)^k(m+1\ \cdots\ n) \end{aligned}$$

where k is relatively prime to m and l is relatively prime to $n-m$.

There are exactly $\varphi(m) \cdot \varphi(n-m)$ such pracks up to isomorphism, one prack per each ordered pair (k, l) where k is relatively prime to m and l is relatively prime to $n-m$ ($1 \leq k < m$, $1 \leq l < n-m$).

Proof: $\mu_1(1) \neq 1$ for there is no cycle of length one. Let $i_1 = 1$ and let the sequence (i_k) be as in Definition 7.1. Then by Proposition 7.4, $\mu_{i_1} = \mu_{i_2} = \cdots = \mu_{i_m} = (i_1\ i_2\ \cdots\ i_m)\pi$, where π is a permutation of $\{1, 2, \ldots, n\} \setminus \{i_1, i_2, \ldots, i_m\}$. Pick any j in $\{1, 2, \ldots, n\} \setminus \{i_1, i_2, \ldots, i_m\}$. Again, $\mu_j(j) \neq j$ for there is no cycle of length one. Let $j_1 = j$ and (j_k) be as in Definition 7.1. Arguing as above, $\mu_{j_1} = \mu_{j_2} = \cdots = \mu_{j_m} = (j_1\ j_2\ \cdots\ j_{n-m})\rho$, where ρ is a permutation of $\{i_1, i_2, \ldots, i_m\}$. Let α be the isomorphism such that $\alpha(i_k) = k$ and $\alpha(j_k) = m+k$. In this way the permutations are now (keeping the notation μ for the permutations in the image of the isomorphism) $\mu_1 = \mu_2 = \cdots = \mu_m = (1\ 2\ \cdots\ m)\delta$ and $\mu_{m+1} = \mu_{m+2} = \cdots = \mu_n = \gamma(m{+}1\ m{+}2\ \cdots\ n)$, where δ is a permutation of $\{m{+}1, m{+}2, \ldots, n\}$ and γ is a permutation of $\{1, 2, \ldots, m\}$. The self-distributivity axiom amounts to saying that $\mu_{\mu_i(j)} = \mu_i \mu_j \mu_i^{-1}$. In this way, for i, j in $\{1, 2, \ldots, m\}$, or i, j in $\{m+1, m+2, \ldots, n\}$ they yield trivial expressions. If i is from $\{1, 2, \ldots, m\}$ and j is from $\{m+1, m+2, \ldots, n\}$ we obtain, since $\delta(j)$ is in $\{m+1, m+2, \ldots, n\}$,

$$\begin{aligned} \gamma(m+1\ m+2\ \ldots\ n) = \mu_{\delta(j)} = \mu_{\mu(i)} &= (1\ 2\ \ldots\ m)\delta \cdot \gamma(m+1\ m+2\ \cdots\ n) \cdot \delta^{-1}(m\ \cdots\ 2\ 1) = \\ &= (1\ 2\ \cdots\ m)\gamma(m\ \cdots\ 2\ 1) \cdot \delta(m+1\ m+2\ \cdots\ n) \cdot \delta^{-1} \end{aligned}$$

so $\gamma = (1\ 2\ \ldots\ m)\gamma(m\ \cdots\ 2\ 1)$ and $(m+1\ m+2\ \ldots\ n) = \delta(m+1\ m+2\ \cdots\ n) \cdot \delta^{-1}$ i.e., γ is in the centralizer of $(1\ 2\ \ldots\ m)$ in the symmetry group of $\{1, 2, \ldots, m\}$, and δ is in the centralizer of $(m+1\ m+2\ \cdots\ n)$ in the symmetry group of $\{m+1, m+2, \ldots, n\}$. Thus, $\gamma = (1\ 2\ \ldots\ m)^k$, for some k relatively prime to m, and $\delta = (m+1\ m+2\ \cdots\ n)^l$, for some l relatively prime to $n-m$, since γ (resp., δ) has to be an m-cycle (resp., $(n-m)$-cycle). We arrive at the same conclusion if i is from $\{m+1, m+2, \ldots, n\}$ and j is from $\{1, 2, \ldots, m\}$. In particular, this rack is indecomposable by Proposition 7.1.

Now suppose two such racks are isomorphic. Specifically, assume that rack R with permutations $\mu_1 = \cdots = \mu_m = (1\ 2\ \cdots\ m)(m+1\ 2\ \cdots\ n)^l$, $\mu_{m+1} = \cdots = \mu_n = (1\ 2\ \cdots\ m)^k(m+1\ 2\ \cdots\ n)$ is isomorphic with rack R' with permutations $\mu'_1 = \cdots = \mu'_m = (1\ 2\ \cdots\ m)(m+1\ 2\ \cdots\ n)^{l'}$, $\mu'_{m+1} = \cdots = \mu'_n = (1\ 2\ \cdots\ m)^{k'}(m+1\ 2\ \cdots\ n)$, via an isomorphism α (with distinct pairs (k, l), and (k', l') further satisfying the conditions in the statement). Since, by Proposition 7.6, isomorphisms map Δ-orbits to Δ-orbits of the same length, then $\alpha(\{1, 2, \ldots, m\}) = \{1, 2, \ldots, m\}$, and $\alpha(\{m+1, \ldots, n\}) = \{m+1, \ldots, n\}$. Hence, $\alpha = \delta\gamma$, where δ is in $S_{\{1,2,\ldots,m\}}$ and γ is in $S_{\{m+1,\ldots,n\}}$. Then, for each i in $\{1, 2, \ldots, m\}$, there is an i' in $\{1, 2, \ldots, m\}$ such that $\alpha(i) = i'$; and, for each j in $\{m+1, \ldots, n\}$, there is a j' in $\{m+1, \ldots, n\}$ such that $\alpha(j) = j'$. So

$$(1\ 2\ \cdots\ m)(m+1\ 2\ \cdots\ n)^{l'} = \mu'_{\alpha(i)} = \alpha\mu_i\alpha^{-1} = \delta\gamma(1\ 2\ \cdots\ m)(m+1\ \cdots\ n)^l\delta^{-1}\gamma^{-1}$$

and

$$(1\ 2\ \cdots\ m)^{k'}(m+1\ 2\ \cdots\ n) = \mu'_{\alpha(j)} = \alpha\mu_j\alpha^{-1} = \delta\gamma(1\ 2\ \cdots\ m)^k(m+1\ \cdots\ n)\delta^{-1}\gamma^{-1}$$

whence δ is in the centralizer of $(1\ 2\ \cdots\ m)$ in $S_{\{1,2,\ldots,m\}}$, γ is in the centralizer of $(m+1\ \cdots\ n)$ in $S_{\{m+1,\ldots,n\}}$; and $l = l'$, and $k = k'$ i.e, the racks are isomorphic. In particular, there are $\varphi(m) \cdot \varphi(n-m)$ pracks up to isomorphism with the indicated profile. This concludes the proof. ■

Cor. 8.2 *Any prack of order $n > 3$ with constant profile*

$$(\{m, m\}, \ldots, \{m, m\})$$

(where $m > 1$ and $n = m + m$) is decomposable and is isomorphic to a prack given by the following sequence of permutations:

$$\mu_1 = \mu_2 = \quad \ldots \quad = \mu_m = (1\ 2\ \cdots\ m)(m+1\ \cdots\ n)^l,$$
$$\mu_{m+1} = \mu_{m+2} = \quad \ldots \quad = \mu_n = (1\ 2\ \cdots\ m)^k(m+1\ \cdots\ n)$$

where k and l are both relatively prime to m.

There are exactly $\frac{1}{2}(1 + \varphi(m)) \cdot \varphi(m)$ such pracks up to isomorphism, one per each ordered pair (k, l) where k and l are both relatively prime to m, and $1 \leq l \leq k < m$.

Proof: We omit the proof here, since it is a slight variation to the proof to the previous Corollary. We just note that, since the Δ-orbits have the same length, then different choices of k and l may give rise to isomorphic pracks. This is taken care of, in the statement, by requiring $k \geq l$. ■

We now address the case of pracks of constant profile such that the corresponding permutations have more than two cycles. Theorem 8.3 and Corollary 8.3 concern pracks of constant profile with r cycles of length one and one cycle of length greater than one. Theorem 8.4 concerns a prack of constant profile with three cycles of distinct lengths, all greater than one.

Thm. 8.3 *Given integers $n > 3$ and $f > 2$ such that $f < n$, the sequence of permutations,*

$$\mu_1 = \mu_2 = \cdots = \mu_{n-f} = (1\ 2\ \cdots\ n-f)(n-f+1)(n-f+2)\cdots(n-1)(n)$$
$$\mu_j = (1\ 2\ \ldots\ n-f)^{k_j}(n-f+1)(n-f+2)\cdots(n-1)(n), \quad j \in \{n-f+1, \ldots, n\}$$

where the k_j's are relatively prime to $n - f$, stands for a decomposable prack of order n with profile:

$$(\{1, 1, \ldots, 1, n-f\}, \ldots, \{1, 1, \ldots, 1, n-f\})$$

Let $P_i(f)$ be the number of partitions of f into i summands, $C_i^{\varphi(n-f)}$ be the number of subsets of i elements from a set of $\varphi(n-f)$ elements, and $m := \min\{f, \varphi(n-f)\}$. There are exactly

$$\sum_{i=1}^{m} C_i^{\varphi(n-f)} P_i(f)$$

pracks with such sequence of permutations up to isomorphism, one per finite sequence $\{k_j\}_{j=n-f+1}^{n}$, modulo permutation of the k_j's (k_j's relatively prime to, and less than, $n - f$).

Before proving the Theorem we state:

Cor. 8.3 *Consider the profile in the statement of Theorem 8.3:*

$$(\{1, 1, \ldots, 1, n-f\}, \ldots, \{1, 1, \ldots, 1, n-f\})$$

If $2 < f < n - f$ there are exactly $\sum_{i=1}^{m} C_i^{\varphi(n-f)} P_i(f)$ pracks of order n with such a profile, up to isomorphism. These pracks are the ones indicated in the Theorem.

If $f = n - f$, there are exactly $1 + \sum_{i=1}^{m} C_i^{\varphi(n-f)} P_i(f)$ pracks of order n with such a profile, up to isomorphism. These pracks are the ones indicated in the Theorem plus the decomposable prack given by the following sequence of permutations:

$$\mu_1 = \mu_2 = \cdots = \mu_{n-f} = (1\ 2\ \cdots\ n-f)(n-f+1)(n-f+2)\cdots(n-1)(n)$$
$$\mu_{n-f+1} = \mu_{n-f+1} = \cdots = \mu_n = (1)(2)\cdots(n-f)(n-f+1\ n-f+2\ \cdots\ n-1\ n)$$

Proof (Theorem 8.3): Since we are dealing with a prack, there has to be a permutation which moves its own index. It follows that the permutations corresponding to the Δ-orbit of this element are all equal. Thus without loss of generality we may assume, arguing as in similar cases above,

$$\mu_1 = \mu_2 = \cdots = \mu_{n-f} = (1\ 2\ \cdots\ n-f)(n-f+1)(n-f+2)\cdots(n-1)(n)$$

We now assume that the remaining permutations fix the same elements as the former ones do. In this way,

$$\mu_j = \sigma_j(n-f+1)(n-f+2)\cdots(n-1)(n)$$

for j in $\{n-f+1,\ldots,n\}$, where σ_j is an $(n-f)$-cycle in $S_{\{1,\ldots,n-f\}}$. Using the distributivity axiom, σ_j has to be in the centralizer of $(1\ 2\ \cdots\ n-f)$ in $S_{\{1,\ldots,n-f\}}$. Hence,

$$\mu_j = (1\ 2\ \cdots\ n-f)^{k_j}(n-f+1)(n-f+2)\cdots(n-1)(n)$$

with k_j relatively prime to $n-f$, for each $j \in \{n-f+1,\ldots n\}$. Clearly, this prack is decomposable by Proposition 7.1.

Suppose two such racks are isomorphic. Specifically, assume that

$$\begin{aligned}
&\mu_1 = \mu_2 = \cdots = \mu_{n-f} = (1\ 2\ \cdots\ n-f)(n-f+1)(n-f+2)\cdots(n-1)(n)\\
&\mu_j = (1\ 2\ \ldots\ n-f)^{k_j}(n-f+1)(n-f+2)\cdots(n-1)(n), \quad j \in \{n-f+1,\ldots,n\}
\end{aligned}$$

and

$$\begin{aligned}
&\mu'_1 = \mu'_2 = \cdots = \mu'_{n-f} = (1\ 2\ \cdots\ n-f)(n-f+1)(n-f+2)\cdots(n-1)(n)\\
&\mu'_j = (1\ 2\ \ldots\ n-f)^{k'_j}(n-f+1)(n-f+2)\cdots(n-1)(n), \quad j \in \{n-f+1,\ldots,n\}
\end{aligned}$$

(where $\{k_j\}_{j=n-f+1}^{n}$ and $\{k'_j\}_{j=n-f+1}^{n}$ are sequences of numbers relatively prime to, and less than $n-f$) are isomorphic via isomorphism α. Since rack isomorphisms map Δ-orbits into Δ-orbits of the same length then $\alpha(\{1,2,\ldots,n-f\}) = \{1,2,\ldots,n-f\}$ and $\alpha(\{n-f+1,\ldots,n\}) = \{n-f+1,\ldots,n\}$ and so $\alpha = \gamma\delta$ with $\gamma \in S_{\{1,2,\ldots,n-f\}}$ and $\delta \in S_{\{n-f+1,\ldots,n\}}$. In particular, for any i in $\{1,2,\ldots,n-f\}$, there exists i' in $\{1,2,\ldots,n-f\}$ such that $\alpha(i) = i'$. Then

$$\begin{aligned}
(1\ 2\ \cdots\ n-f)(n-f+1)(n-f+2)\cdots(n-1)(n) &= \mu'_{i'} = \mu'_{\alpha(i)} = \alpha\mu_i\alpha^{-1} =\\
&= \gamma\delta(1\ 2\ \cdots\ n-f)(n-f+1)(n-f+2)\cdots((n-1)(n)\gamma^{-1}\delta^{-1}
\end{aligned}$$

and so $(1\ 2\ \cdots\ n-f)\gamma = \gamma(1\ 2\ \cdots\ n-f)$ i.e., $\gamma = (1\ 2\ \cdots\ n-f)^g$, for some positive integer g. Furthermore, since for any j in $\{n-f+1, n-f+2,\ldots,n-1,n\}$ there is a j' in $\{n-f+1, n-f+2,\ldots,n-1,n\}$ such that $\alpha(j) = j'$, then

$$\begin{aligned}
(1\ 2\ \cdots\ n-f)^{k'_{j'}}(n-f+1)(n-f+2)\cdots(n-1)(n) &= \mu'_{j'} = \mu'_{\alpha(j)} = \alpha\mu_j\alpha^{-1} =\\
&= \gamma\delta(1\ 2\ \cdots\ n-f)^{k_j}(n-f+1)(n-f+2)\cdots((n-1)(n)\gamma^{-1}\delta^{-1}
\end{aligned}$$

and so

$$\begin{aligned}
(1\ 2\ \cdots\ n-f)^{k'_{\alpha(j)}} &= (1\ 2\ \cdots\ n-f)^{k'_{j'}} = (1\ 2\ \cdots\ n-f)^g(1\ 2\ \cdots\ n-f)^{k_j}(1\ 2\ \cdots\ n-f)^{-g} =\\
&= (1\ 2\ \cdots\ n-f)^{k_j}
\end{aligned}$$

i.e., $k'_{\alpha(j)} = k_j$ for any j in $\{n-f+1, n-f+2,\ldots,n-1,n\}$. Hence, any permutation of the terms of a sequence of numbers relatively prime to and less than $n-f$, $\{k_j\}_{j=n-f+1}^{n}$, gives rise to isomorphic racks, as constructed above.

Let us now count how many isomorphism classes there are. Let us consider them according to how many different numbers there are in the $\{k_j\}_{j=n-f+1}^{n}$ sequence. If there is just one number, then there are $\varphi(n-f)$ possibilities, one per number relatively prime to and less than $n-f$. If there are two numbers, say k and k', then we may have f_1 repeats of k and f_2 repeats of k' such that $f_1 + f_2 = f$.

Since we are not allowing permutations of the terms of the sequence then this is the same as the number of partitions of f using only two summands, $P_2(f)$. Also the number of different possibilities of picking two numbers out of a set of $\varphi(n-f)$ is $C_2^{\varphi(n-f)}$. So the contribution for the total number of isomorphic classes from using just two different numbers in the indicated sequence is $C_2^{\varphi(n-f)} \cdot P_2(f)$. We believe it is now clear that when using i distinct numbers the contribution is $C_i^{\varphi(n-f)} \cdot P_i(f)$ and that the last i should be the first of $\varphi(n-f)$ or f to be reached. Hence the total number of isomorphism classes is $\sum_{i=1}^{m} C_i^{\varphi(n-f)} P_i(f)$ where $m := \min\{f, \varphi(n-f)\}$. ■

Proof (Corollary 8.3): Again we assume that the first $n-f$ permutations are

$$\mu_1 = \mu_2 = \cdots = \mu_{n-f} = (1\ 2\ \cdots\ n-f)(n-f+1)(n-f+2)\ldots(n-1)(n)$$

We now assume one of the remaining permutations fixes the index of one of the former permutations i.e., there is $j \in \{n-f+1, \ldots, n\}$ and $i \in \{1, \ldots, n-f\}$ such that $\mu_j(i) = i$. Then $\mu_i = \mu_{\mu_i(j)} = \mu_i \mu_j \mu_i^{-1}$ i.e., $\mu_i \mu_j = \mu_j \mu_i$. Hence, mod $n-f$, we have

$$\mu_j(i+1) = \mu_j \mu_i(i) = \mu_i \mu_j(i) = \mu_i(i) = i+1$$

Suppose there is s such that $\mu_j(i+s) = i+s$, mod $n-f$. Then, mod $n-f$

$$\mu_j(i+s+1) = \mu_j \mu_i(i+s) = \mu_i \mu_j(i+s) = \mu_i(i+s) = i+s+1$$

If the increment is $n-f$ we recover $\mu_j(i) = i$; then μ_j fixes all elements from $\{1, \ldots, n-f\}$. If $f < n-f$ this is impossible. Assume $n-f = f$. Then μ_j moves any element from $\{n-f+1, \ldots, n\}$ so it moves its own index. Then, without loss of generality, we may assume, invoking Proposition 7.4

$$\mu_{n-f+1} = \cdots = \mu_n = (1)\cdots(n-f)(n-f+1\ n-f+2\ \ldots\ n-1\ n)$$

This prack is decomposable by Proposition 7.1. It also has two distinct Δ-orbits. Then it is not isomorphic with any of the pracks in the Theorem since these have only one Δ-orbit. This finishes the proof. ■

Thm. 8.4 *Any prack of finite order $m_1 + m_2 + m_3$ $(1 < m_1 < m_2 < m_3)$ with constant profile*

$$(\{m_1, m_2, m_3\}, \ldots, \{m_1, m_2, m_3\})$$

is decomposable and is isomorphic to a prack given by the following sequence of permutations,

$$\begin{aligned}
\mu_1 = \cdots = \mu_{m_1} &= (1\ \cdots\ m_1)(m_1+1\ \cdots\ m_1+m_2)^{k_2^1}(m_1+m_2+1\ \cdots\ m_1+m_2+m_3)^{k_3^1} \\
\mu_{m_1+1} = \cdots = \mu_{m_1+m_2} &= (1\ \cdots\ m_1)^{k_1^2}(m_1+1\ \cdots\ m_1+m_2)(m_1+m_2+1\ \cdots\ m_1+m_2+m_3)^{k_3^2} \\
\mu_{m_1+m_2+1} = \cdots = \mu_{m_1+m_2+m_3} &= (1\ \cdots\ m_1)^{k_1^3}(m_1+1\ \cdots\ m_1+m_2)^{k_2^3}(m_1+m_2+1\ \cdots\ m_1+m_2+m_3)
\end{aligned}$$

where k_1^2, k_1^3 are relatively prime to m_1, k_2^1, k_2^3 are relatively prime to m_2, and k_3^1, k_3^2 are relatively prime to m_3.

There are exactly $\big(\varphi(m_1)\big)^2 \cdot \big(\varphi(m_2)\big)^2 \cdot \big(\varphi(m_3)\big)^2$ such pracks up to isomorphism, one sequence per each $((k_1^2, k_1^3), (k_2^1, k_2^3), (k_3^1, k_3^2))$, where k_1^2, k_1^3 are relatively prime to and less than m_1, k_2^1, k_2^3 are relatively prime to and less than m_2, and k_3^1, k_3^2 are relatively prime to and less than m_3.

Proof: No element is fixed by any of the permutations and each of these is the product of three disjoint cycles, so we can assume, without loss of generality, that

$$\begin{aligned}
\mu_1 = \cdots = \mu_{m_1} &= (1\ \cdots\ m_1)\pi_{2,3} \\
\mu_{m_1+1} = \cdots = \mu_{m_1+m_2} &= (m_1+1\ \cdots\ m_1+m_2)\pi_{1,3} \\
\mu_{m_1+m_2+1} = \cdots = \mu_{m_1+m_2+m_3} &= (m_1+m_2+1\ \cdots\ m_1+m_2+m_3)\pi_{1,2}
\end{aligned}$$

where the $\pi_{i,j}$ are from $S_{M_i \cup M_j}$, they are products of an m_i-cycle by an m_j-cycle, and $M_1 = \{1, \ldots, m_1\}$, $M_2 = \{m_1+1, \ldots, m_1+m_2\}$, and $M_3 = \{m_1+m_2+1, \ldots, m_1+m_2+m_3\}$.

Let j be in M_1. Since $|M_3| = m_3 > m_2 = |M_2|$, there has to be i_3 in M_3 such that $\pi_{2,3}(i_3)$ is in M_3. In this way,

$$(m_1 + m_2 + 1 \ \cdots \ m_1 + m_2 + m_3)\pi_{1,2} = \mu_{\pi_{2,3}(i_3)} = \mu_{\mu_j(i_3)} = \mu_j \mu_{i_3} \mu_j^{-1}$$

i.e.,

$$(m_1 + m_2 + 1 \ \cdots \ m_1 + m_2 + m_3)\pi_{1,2} = \mu_j (m_1 + m_2 + 1 \ \cdots \ m_1 + m_2 + m_3)\pi_{1,2} \mu_j^{-1} \tag{1}$$

Assume now there is i_2 in M_2 such that $\pi_{2,3}(i_2)$ is in M_3. Then,

$$(m_1 + m_2 + 1 \ \cdots \ m_1 + m_2 + m_3)\pi_{1,2} = \mu_{\pi_{2,3}(i_2)} = \mu_{\mu_j(i_2)} = \mu_j \mu_{i_2} \mu_j^{-1}$$

i.e.,

$$(m_1 + m_2 + 1 \ \cdots \ m_1 + m_2 + m_3)\pi_{1,2} = \mu_j (m_1 + 1 \ \cdots \ m_1 + m_2)\pi_{1,3} \mu_j^{-1} \tag{2}$$

From (1) and (2) we have

$$(m_1 + m_2 + 1 \ \cdots \ m_1 + m_2 + m_3)\pi_{1,2} = \mu_{i_3} = \mu_{i_2} = (m_1 + 1 \ \cdots \ m_1 + m_2)\pi_{1,3}$$

so

$$\pi_{1,2} = \sigma(m_1 + 1 \ \cdots \ m_1 + m_2), \qquad \pi_{1,3} = \sigma(m_1 + m_2 + 1 \ \cdots \ m_1 + m_2 + m_3)$$

with σ an m_1-cycle in S_{M_1}.

From (1) we obtain

$$\begin{aligned}(m_1 + m_2 + 1 \ \cdots \ m_1 + m_2 + m_3) \cdot \sigma(m_1 + 1 \ \cdots m_1 + m_2) \cdot (1 \ \cdots \ m_1)\pi_{2,3} = \\ = (1 \ \cdots \ m_1)\pi_{2,3} \cdot (m_1 + m_2 + 1 \ \cdots \ m_1 + m_2 + m_3) \cdot \sigma(m_1 + 1 \ \cdots \ m_1 + m_2)\end{aligned}$$

so $\sigma(1 \ \cdots \ m_1) = (1 \ \cdots \ m_1)\sigma$ and

$$\begin{aligned}(m_1 + m_2 + 1 \ \cdots \ m_1 + m_2 + m_3)(m_1 + 1 \ \cdots \ m_1 + m_2)\pi_{2,3} = \\ = \pi_{2,3}(m_1 + m_2 + 1 \ \cdots \ m_1 + m_2 + m_3)(m_1 + 1 \ \cdots \ m_1 + m_2)\end{aligned} \tag{3}$$

We recall we are assuming there exists i_2 in M_2 such that $\pi_{2,3}(i_2)$ is in M_3. Then, using (3), we have mod m_3,

$$\begin{aligned}\pi_{2,3}(i_2 + 1) = \pi_{2,3}(m_1 + m_2 + 1 \ \cdots \ m_1 + m_2 + m_3)(m_1 + 1 \ \cdots \ m_1 + m_2)(i_2) = \\ = (m_1 + m_2 + 1 \ \cdots \ m_1 + m_2 + m_3)(m_1 + 1 \ \cdots \ m_1 + m_2)\pi_{2,3}(i_2) = \pi_{2,3}(i_2) + 1\end{aligned}$$

Now suppose there is s such that $\pi_{2,3}(i_2 + s) = \pi_{2,3}(i_2) + s$ in M_3. Then,

$$\begin{aligned}\pi_{2,3}(i_2 + s + 1) = \pi_{2,3}(m_1 + m_2 + 1 \ \cdots \ m_1 + m_2 + m_3)(m_1 + 1 \ \cdots \ m_1 + m_2)(i_2 + s) = \\ = (m_1 + m_2 + 1 \ \cdots \ m_1 + m_2 + m_3)(m_1 + 1 \ \cdots \ m_1 + m_2)\pi_{2,3}(i_2 + s) = \pi_{2,3}(i_2 + s) + 1 = \pi_{2,3}(i_2) + s + 1\end{aligned}$$

In particular,

$$\pi_{2,3}(i_2) = \pi_{2,3}(i_2 + m_2) = \pi_{2,3}(i_2) + m_2$$

so $m_2 = m_3$ mod m_3 but by hypothesis, $1 < m_2 < m_3$. Hence, there cannot be i_2 in M_2 such that $\pi_{2,3}(i_2)$ is in M_3. So

$$\pi_{2,3} = \gamma_2^1 \delta_3^1$$

where γ_2^1 is an m_2-cycle in S_{M_2}, and δ_3^1 is an m_3-cycle in S_{M_3}.

With similar arguments we obtain also that

$$\pi_{1,3} = \gamma_1^2 \delta_3^2$$

where γ_1^2 is an m_1-cycle in S_{M_1}, and δ_3^2 is an m_3-cycle in S_{M_3}, and

$$\pi_{1,2} = \gamma_1^3 \delta_2^3$$

where γ_1^3 is an m_1-cycle in S_{M_1}, and δ_2^3 is an m_2-cycle in S_{M_2}.

So, for any j_1 in M_1, j_2 in M_2 and j_3 in M_3, $\mu_{j_1}(j_2)$ is in M_2 and $\mu_{j_1}(j_3)$ is in M_3, so

$$\begin{aligned}(m_1+1\ \cdots\ m_1+m_2)\gamma_1^2\delta_3^2 &= \mu_{j_1}(j_2) = \mu_{j_1}\mu_{j_2}\mu_{j_1}^{-1}\\ &= (1\ \cdots\ m_1)\gamma_2^1\delta_3^1\cdot(m_1+1\ \cdots\ m_1+m_2)\gamma_1^2\delta_3^2\cdot(1\ \cdots\ m_1)^{-1}\gamma_2^1 sp{-}1{\delta_3^1}^{-1}\end{aligned}$$

i.e.,

$$(m_1+1\ \cdots\ m_1+m_2)\gamma_1^2\delta_3^2(1\ \cdots\ m_1)\gamma_2^1\delta_3^1 = (1\ \cdots\ m_1)\gamma_2^1\delta_3^1(m_1+1\ \cdots\ m_1+m_2)\gamma_1^2\delta_3^2$$

so

$$\gamma_1^2(1\ \cdots\ m_1) = (1\ \cdots\ m_1)\gamma_1^2, \qquad \gamma_2^1(m_1+1\ \cdots\ m_1+m_2) = (m_1+1\ \cdots\ m_1+m_2)\gamma_2^1, \qquad \delta_3^1\delta_3^2 = \delta_3^2\delta_3^1$$

So, in particular, γ_1^2 is an m_1-cycle in the centralizer of $(1\ \cdots\ m_1)$ in S_{M_1} i.e., $\gamma_1^2 = (1\ \cdots\ m_1)^{k_1^2}$, where k_1^2 is relatively prime to m_1. Also, γ_2^1 is an m_2-cycle in the centralizer of $(m_1+1\ \cdots\ m_1+m_2)$ in S_{M_2}, thus $\gamma_2^1 = (m_1+1\ \cdots\ m_1+m_2)^{k_2^1}$, with k_2^1 relatively prime to m_2. Repeating this argument with other pairs of indices we eventually obtain $\delta_3^1 = (m_1+m_2+1\ \cdots\ m_1+m_2+m_3)^{k_3^1}$, with k_3^1 relatively prime to m_3, $\delta_3^2 = (m_1+m_2+1\ \cdots\ m_1+m_2+m_3)^{k_3^2}$, with k_3^2 relatively prime to m_3, $\gamma_1^3 = (1\ \cdots\ m_1)^{k_1^3}$, with k_1^3 relatively prime to m_1, and $\delta_2^3 = (m_1+1\ \cdots\ m_1+m_2)^{k_2^3}$, with k_2^3 relatively prime to m_2 which gives the permutations in the statement. In particular, such a rack is decomposable since the elements which form the cycles the permutations are made of split into two disjoint subsets, see Proposition 7.1.

We remark that no two of these pracks are isomorphic, when the k_i^j's are picked less than the corresponding m_i's. The proof goes along the same lines as in the proofs to previous theorems. An isomorphism between two such pracks maps Δ-orbits into Δ-orbits, so it will be the product of three permutations each of which will map M_i into itself, for each i. Next each of these permutation has to be in a certain centralizer. Finally this will imply that the corresponding k_i^j exponents have to be equal which means the pracks are equal. It then follows that the number of distinct isomorphic classes is $\big(\varphi(m_1)\big)^2\cdot\big(\varphi(m_2)\big)^2\cdot\big(\varphi(m_3)\big)^2$, which concludes the proof. ∎

We turn now to quandles of specified profile. Clearly, there cannot be quandles of constant profile $(\{n\},\ldots,\{n\})$. What about quandles of constant profile $(\{1,n-1\},\ldots,\{1,n-1\})$?

Thm. 8.5 *Consider a finite quandle of order $n > 2$ with constant profile $(\{1,n-1\},\ldots,\{1,n-1\})$. Then, modulo isomorphism, its sequence of permutations is:*

1. $\mu_n = (1\ 2\ \cdots\ n-1)(n)$,
2. μ_{n-1} *is a solution to the system of equations:*
   - $\mu_{n-1}\mu_n\mu_{n-1}^{-1} = \mu_n^{\mu_{n-1}(n)}\mu_{n-1}\mu_n^{-\mu_{n-1}(n)}$
   - $\mu_{n-1}^{-1}\mu_n\mu_{n-1} = \mu_n^{\mu_{n-1}^{-1}(n)}\mu_{n-1}\mu_n^{-\mu_{n-1}^{-1}(n)}$
   - $\mu_n^{-\mu_{n-1}(l)}\mu_{n-1}\mu_n^l = \mu_{n-1}^{k_l}$, *for all* $l \in \{1,\ldots,n-2\}\setminus\{\mu_{n-1}^{-1}(n)\}$, *some* $k_l \in \{1,\ldots,n-2\}$.
3. $\mu_k = \mu_n^k\mu_{n-1}\mu_n^{-k}$, *for all* $1 \le k \le n-2$

Proof: Without loss of generality, assume $\mu_n = (1\ 2\ \cdots\ n-1)(n)$, whence 1. follows. Now, $\mu_{n-1} = (i_1\ i_2\ \cdots\ i_{n-1})(n-1)$, where $(i_1\ i_2\ \cdots\ i_{n-1})$ is a cycle of length $n-1$, permuting the elements of

$\{1,2,\ldots,n-2,n-1,n\}\setminus\{n-1\}$. Using (part of) the expressions corresponding to the self-distributivity axiom, we can define the remaining permutations. We have

$$\mu_1=\mu_{\mu_n(n-1)}=\mu_n\mu_{n-1}\mu_n^{-1}$$

If $\mu_k=\mu_n^k\mu_{n-1}\mu_n^{-k}$, then

$$\mu_{k+1}=\mu_{\mu_n(k)}=\mu_n\mu_k\mu_n^{-1}=\mu_n\mu_n^k\mu_{n-1}\mu_n^{-k}\mu_n^{-1}=\mu_n^{k+1}\mu_{n-1}\mu_n^{-(k+1)}$$

(where the free indices are to be read modulo $n-1$) whence 3. follows. Note that for $1\leq k\leq n-2$ we have

$$\begin{aligned}\mu_k(k)&=\mu_n^k\mu_{n-1}\mu_n^{-k}(k)=\mu_n^k\mu_{n-1}\mu_n^{-k+1}(k-1)=\cdots=\mu_n^k\mu_{n-1}\mu_n^{-1}(1)=\mu_n^k\mu_{n-1}(n-1)=\\&=\mu_n^k(n-1)=\mu_n^{k-1}(1)=\cdots=\mu_n(k-1)=k\end{aligned}$$

so these permutations comply with the quandle axiom. Now for the self-distributivity, $\mu_{\mu_i(j)}=\mu_i\mu_j\mu_i^{-1}$. Before, we used these expressions for $i=n$, and recursively $j=n-1,1,2,\ldots n-3$, for defining μ_k, $1\leq k\leq n-2$. For k and k' in $\{1,2,\ldots,n-1\}$ $(k\neq k')$ we must have

$$\mu_{\mu_k(k')}=\mu_k\mu_{k'}\mu_k^{-1}$$

Now,

$$\mu_{\mu_k(k')}=\mu_{\mu_n^k\mu_{n-1}\mu_n^{-k}(k')}=\mu_{\mu_n^k\mu_{n-1}(k'-k)}=\mu_{\mu_n^k(\mu_{n-1}(l))}=$$

$$=\begin{cases}\mu_n, & \text{if } \mu_{n-1}(l)=n\\ \mu_n^k\mu_{\mu_{n-1}(l)}\mu_n^{-k}, & \text{if } \mu_{n-1}(l)\in\{1,\ldots,n-2\}\end{cases}$$

with $l=k'-k$. On the other hand, again with $l=k'-k$,

$$\mu_k\mu_{k'}\mu_k^{-1}=\left(\mu_n^k\mu_{n-1}\mu_n^{-k}\right)\cdot\left(\mu_n^{k'}\mu_{n-1}\mu_n^{-k'}\right)\cdot\left(\mu_n^k\mu_{n-1}\mu_n^{-k}\right)^{-1}=\mu_n^k\mu_{n-1}\mu_n^l\mu_{n-1}\mu_n^{-l}\mu_{n-1}^{-1}\mu_n^{-k}$$

Suppose $\mu_{n-1}(l)=n$. Then, $\mu_n=\mu_{n-1}\mu_n^l\mu_{n-1}\mu_n^{-l}\mu_{n-1}^{-1}$, i.e.,

$$\mu_{n-1}^{-1}\mu_n\mu_{n-1}=\mu_n^l\mu_{n-1}\mu_n^{-l},\qquad \text{if } \mu_{n-1}(l)=n \tag{4}$$

Suppose $\mu_{n-1}(l)\in\{1,2,\ldots,n-2\}$. Then, $\mu_{\mu_{n-1}(l)}=\mu_{n-1}\mu_n^l\mu_{n-1}\mu_n^{-l}\mu_{n-1}^{-1}$. On the other hand, since $\mu_{n-1}(l)\in\{1,2,\ldots,n-2\}$, $\mu_{\mu_{n-1}(l)}=\mu_n^{\mu_{n-1}(l)}\mu_{n-1}\mu_n^{-\mu_{n-1}(l)}$ and so

$$\mu_n^{\mu_{n-1}(l)}\mu_{n-1}\mu_n^{-\mu_{n-1}(l)}=\mu_{n-1}\mu_n^l\mu_{n-1}\mu_n^{-l}\mu_{n-1}^{-1}$$

i.e.,

$$\mu_{n-1}\cdot\mu_n^{-\mu_{n-1}(l)}\mu_{n-1}\mu_n^l=\mu_n^{-\mu_{n-1}(l)}\mu_{n-1}\mu_n^l\cdot\mu_{n-1}$$

This means $\mu_n^{-\mu_{n-1}^l}\mu_{n-1}\mu_n^l$ is in the centralizer of μ_{n-1} in the symmetry group of $\{1,2,\ldots,n\}$ which is the cyclic subgroup generated by μ_{n-1}. Thus,

$$\mu_n^{-\mu_{n-1}(l)}\mu_{n-1}\mu_n^l=\mu_{n-1}^{k_l},\qquad \text{for all } l\in\{1,\ldots,n-2\}\setminus\{\mu_{n-1}^{-1}(n)\}, \text{ and some } k_l\in\{1,\ldots,n-2\} \tag{5}$$

We remark that $k_l=n-1$ leads to a contradiction.

There remains to ascertain the implications of $\mu_{\mu_k(n)}=\mu_k\mu_n\mu_k^{-1}$, for k in $\{1,\ldots,n-1\}$. With similar manipulations as above, noting that

$$\mu_k(n)=\mu_n^k\mu_{n-1}\mu_n^{-k}(n)=\mu_n^k\mu_{n-1}(n)=\mu_n^k\mu_n^{\mu_{n-1}(n)}(n-1)=\mu_n^{k+\mu_{n-1}(n)}(n-1)$$

we obtain,

$$\mu_{n-1}\mu_n\mu_{n-1}^{-1}=\mu_n^{\mu_{n-1}(n)}\mu_{n-1}\mu_n^{-\mu_{n-1}(n)} \tag{6}$$

(6), (4), and (5) now stand for statement 2.. This concludes the proof. ■

The following Corollaries depict restrictions the μ_{n-1} is subject to. In these Corollaries the context and notation are those of Theorem 8.5.

Cor. 8.4 *$\mu_{n-1}(i) \neq i+1$, for i in $\{1,2,\ldots,n-2\}$.*

Proof: Assume it is. Then $\mu_{i+1} = \mu_{\mu_{n-1}(i)} = \mu_{n-1}\mu_i\mu_{n-1}^{-1}$. Since $\mu_i = \mu_n^i\mu_{n-1}\mu_n^{-i}$ and analogously for μ_{i+1}, then $\mu_n^{i+1}\mu_{n-1}\mu_n^{-(i+1)} = \mu_{n-1}\mu_n^i\mu_{n-1}\mu_n^{-i}\mu_{n-1}^{-1}$ which can be rewritten as $\mu_{n-1}\mu_n^{-1}\cdot\mu_n^{-i}\mu_{n-1}\mu_n^i = \mu_n^{-1}\cdot\mu_n^{-i}\mu_{n-1}\mu_n^i\cdot\mu_{n-1}$, which means $\mu_{n-1}\mu_n^{-1}\mu_{-i} = \mu_n^{-1}\mu_{-i}\mu_{n-1}$, ($-i$ mod $n-1$) i.e., $\mu_n^{-1}\mu_{-i}$ is in the centralizer of μ_{n-1} in the symmetry group of $\{1,2,\ldots,n\}$. Hence, $\mu_n^{-1}\mu_{-i} = \mu_{n-1}^k$, for some k in $\{1,2,\ldots,n-1\}$. If $k = n-1$, then $\mu_{-i} = \mu_n$. Thus, modulo $n-1$, $-i = n$ which means that $i = n-2$. So $\mu_{n-1}(n-2) = n-1$ but by hypothesis, μ_{n-1} fixes $n-1$. This is impossible.

Assume now $k \neq n-1$. Then, since μ_{n-1}^k fixes $n-1$ and $\mu_n^{-1}\mu_{-i}$ fixes $\mu_{-i}^{-1}(n)$, hence $\mu_{-i}^{-1}(n) = n-1$, i.e., $n = \mu_{-i}(n-1) = \mu_n^{-i}\mu_{n-1}\mu_n^i(n-1) = \mu_n^{-i}\mu_{n-1}(i)$ from which follows that $n = \mu_{n-1}(i) = i+1$, by assumption, so $n-1 = i \in \{1,2,\ldots,n-2\}$. Again this is impossible.

■

We remark that $\mu_{n-1}(n-2) = n$ is possible: consider $\mathbb{Z}_5[T,T^{-1}]/(T-2)$; and that $\mu_{n-1}(n) = 1$ is also possible: $\mathbb{Z}_5[T,T^{-1}]/(T-3)$.

Cor. 8.5 *If, for $n > 3$,*

$$\mu_{n-1} = (n-2\ n\ k\ \cdots)(n-1)$$

then n is odd and $k = \frac{n-1}{2}$.

Proof: Suppose μ_{n-1} is as stated. Then,

$$\mu_{n-1}\mu_n\mu_{n-1}^{-1} = \big(\mu_{n-1}(1)\ \mu_{n-1}(2)\ \cdots\ \mu_{n-1}(n-2)\ \mu_{n-1}(n-1)\ \big)\big(\mu_{n-1}(n)\big) = \big(\cdots\ n\ n-1\ \big)\big(k\big)$$

On the other hand,

$$\mu_n^{\mu_{n-1}(n)}\mu_{n-1}\mu_n^{-\mu_{n-1}(n)} = \mu_n^k\mu_{n-1}\mu_n^{-k} = \big(\mu_n^k(n-2)\ \mu_n^k(n)\ \mu_n^k(k)\ \cdots\big)\big(\mu_n^k(n-1)\big) = \big(k-1\ n\ 2k\ \cdots\big)\big(k\big)$$

By (6) in the proof to the previous Theorem, these two expressions have to be equal. Then, we have $2k = n-1$ i.e., n is odd and $k = (n-1)/2$

■

Cor. 8.6 *If, for $n > 3$,*

$$\mu_{n-1} = (k\ n\ n-2\ \cdots)(n-1)$$

then $k = 1$.

Proof: Assume μ_{n-1} is as stated. Then

$$\mu_{n-1}^{-1}\mu_n\mu_{n-1} = \big(\mu_{n-1}^{-1}(1)\ \cdots\ \mu_{n-1}^{-1}(n-2)\ \cdots\ \mu_{n-1}^{-1}(n-1)\ \big)\big(\mu_{n-1}^{-1}(n)\big) = \big(\cdots\ n\ n-1\ \big)\big(k\big)$$

On the other hand,

$$\begin{aligned}\mu_n^{\mu_{n-1}^{-1}(n)}\mu_{n-1}\mu_n^{-\mu_{n-1}^{-1}(n)} &= \mu_n^k\mu_{n-1}\mu_n^{-k} = \big(\mu_n^k(k)\ \mu_n^k(n)\ \mu_n^k(n-2)\ \cdots\big)\big(\mu_n^k(n-1)\big) = \\ &= \big(2k\ n\ k-1\ \cdots\big)\big(k\big)\end{aligned}$$

and by comparison, $k = 1$. ■

The proofs of the following two Corollaries are similar to the ones in the preceding corollaries and so will be omitted.

Cor. 8.7 *If, for $n > 3$,*

$$\mu_{n-1} = (k\ n\ 1\ \cdots)(n-1)$$

then n is odd and $k = \frac{n-1}{2}$.

■

Order	μ_{n-1}	...isomorphic with...
3	(2)(1 3)	R_3
4	(3)(1 4 2)	$S_4 \cong \mathbb{Z}_2[T, T^{-1}]/(T^2 + T + 1)$
5	(4)(2 5 1 3)	$\mathbb{Z}_5[T, T^{-1}]/(T - 3)$
	(4)(3 5 2 1)	$\mathbb{Z}_5[T, T^{-1}]/(T - 2)$
6	no solutions	
7	(6)(1 7 5 2 4 3)	$\mathbb{Z}_7[T, T^{-1}]/(T - 5)$
	(6)(1 7 5 3 2 4)	$\mathbb{Z}_7[T, T^{-1}]/(T - 3)$
8	(7)(2 8 3 6 1 5 4)	$\mathbb{Z}_2[T, T^{-1}]/(T^3 + T + 1)$
	(7)(4 8 5 3 2 6 1)	$\mathbb{Z}_2[T, T^{-1}]/(T^3 + T^2 + 1)$

Table 8.1: Quandles of profile $(\{1, n-1\}, \ldots, \{1, n-1\})$ for each order $3 \leq n \leq 8$

Cor. 8.8 *If, for $n > 3$,*

$$\mu_{n-1} = (1 \; n \; k \; \cdots)(n-1)$$

then $k = n - 2$.

■

Using these results we tried to find μ_{n-1}'s which are solutions to the system of equations in 2. in the statement of Theorem 8.5. For each $n > 2$, each of these solutions together with $\mu_n = (1 \; 2 \ldots n-1)(n)$ and the μ_k's given by $\mu_k = \mu_n^k \mu_{n-1} \mu_n^{-k}$, for all $1 \leq k \leq n-2$, constitute the sequence of permutations of a finite quandle of order $n > 2$ with constant profile $(\{1, n-1\}, \ldots, \{1, n-1\})$. The general strategy was, for each order n, to set up a tentative μ_{n-1} by assigning the image and pre-image of n, taking into consideration the Corollaries above. Then, using the first two equations of the system of equations referred to above we tried either to show that such a μ_{n-1} would not be a solution to our problem or to complete μ_{n-1} and to verify that it satisfied the remaining equations.

For $n = 3$, the unique such μ_{n-1} is $\mu_2 = (1 \; 3)(2)$ which gives rise to the dihedral quandle of order 3, R_3. Applying Corollary 8.6, with $n = 4$, the unique such μ_{n-1} is $\mu_3 = (1 \; 4 \; 2 \;)(3)$ which gives rise to a quandle isomorphic to $S_4 \cong \mathbb{Z}_2[T, T^{-1}]/(T^2 + T + 1)$. And so on and so forth. We display our results in Table 8.1. The order is displayed in the first column. In the second column the μ_{n-1} is displayed since it identifies the quandle under study (see discussion above). In the third column, we give a more familiar quandle which is isomorphic with the quandle under study.

9 Final Remarks

In this work we developed a different approach to racks and quandles by regarding them as sequences of permutations. In the course of it, some issues concerning the structure of racks and quandles were found. In Proposition 5.4 it is proved that the opposite to an Alexander quandle also satisfies self-distributivity. We feel this is an indication to look for non-Alexander quandles. We have a first example in the octahedron quandle. This is an interesting quandle in that it is good at telling knots apart via counting colorings ([7]). This is also an indecomposable quandle. In this way, we would like to know if there is an infinite class of indecomposable non-Alexander quandles which are good at telling knots apart via counting colorings. Finally, we were able to identify all racks that have given profiles. In this connection we ask the following question. Are there indecomposable racks not isomorphic with cyclic racks?

9.1 Acknowledgements

The first author acknowledges support by *Programa Operacional "Ciência, Tecnologia, Inovação"* (POCTI) of the *Fundação para a Ciência e a Tecnologia* (FCT) cofinanced by the European Community fund

FEDER.

References

[1] N. Andruskiewitsch, M. Graña, *From racks to pointed Hopf algebras*, Adv. Math., **178** (2003), no. 2, 177-243

[2] J. Bojarczuk, P. Lopes, *Quandles at finite temperatures III*, J. Knot Theory Ramifications, to appear

[3] E. Brieskorn, *Automorphic sets and braids and singularities*, Contemp. Math., **78** (1988), 45-115

[4] J. S. Carter, M. Saito, *Knotted surfaces and their diagrams*, Mathematical Surveys and Monographs **55**, American Mathematical Society (1998)

[5] J. S. Carter, D. Jelsovsky, S. Kamada, L. Langford, M. Saito, *Quandle cohomology and state-sum invariants of knotted curves and surfaces*, Trans. Amer. Math. Soc., **355** (2003), no. 10, 3947- 3989

[6] P. Dehornoy, *Braids and self-distributivity*, Progress in Mathematics **192**, Birkhäuser (2000)

[7] F. M. Dionísio, Private communication

[8] F. M. Dionísio, P. Lopes, *Quandles at finite temperatures II*, J. Knot Theory Ramifications, **12** (2003), no. 8, 1049-1091

[9] R. Fenn, C. Rourke, *Racks and links in codimension two*, J. Knot Theory Ramifications, **1** (1992), no. 4, 343-406

[10] D. Joyce, *A classifying invariant of knots, the knot quandle*, J. Pure Appl. Alg., **23** (1982), 37-65

[11] D. Joyce, *Simple quandles*, J. Algebra, **79** (1982), no. 2, 307-318

[12] L. H. Kauffman, *Knots and physics*, 3rd edition, Series on Knots and Everything **1**, World Scientific Publishing Co., River Edge, NJ (2001)

[13] P. Lopes, *Quandles at finite temperatures I*, J. Knot Theory Ramifications, **12** (2003), no. 2, 159-186

[14] S. V. Matveev, *Distributive groupoids in knot theory*, Math. USSR Sbornik, **47** (1984), no. 1, 73-83

[15] S. Nelson, *Classification of finite Alexander quandles*, Proceedings of the Spring Topology and Dynamical Systems Conference, Topology Proc., **27** (2003), no. 1, 245-258

[16] J. Smith, A. Romanowska, *Post-modern algebra*, Series on Pure and Applied Mathematics, John Wiley and Sons. Inc., New York, NY (1999)

[17] D. Roseman, *Reidemeister-type moves for surfaces in four-dimensional space*, in “Knot Theory” (Warsaw, 1995), Banach Center Publ., 42, Polish Academy of Sciences, Warsaw (1998) 347-380

[18] D. Roseman, work in progress

[19] J. J. Rotman, *An introduction to the theory of groups*, Fourth Edition, Graduate Texts in Mathematics, Springer Verlag Inc., New York, NY (1995)

[20] H. Ryder, *The congruence structure of racks*, Comm. Algebra, **23** (1995), no. 13, 4971-4989