Louisiana State University
LSU Digital Commons

LSU Doctoral Dissertations | Graduate School

2002

Racks, quandles and virtual knots

Victor Samuel Nelson
Louisiana State University and Agricultural and Mechanical College, nelson@math.lsu.edu

Follow this and additional works at: https://digitalcommons.lsu.edu/gradschool_dissertations

Part of the Applied Mathematics Commons

Recommended Citation
Nelson, Victor Samuel, "Racks, quandles and virtual knots" (2002). *LSU Doctoral Dissertations*. 4022.
https://digitalcommons.lsu.edu/gradschool_dissertations/4022

This Dissertation is brought to you for free and open access by the Graduate School at LSU Digital Commons. It has been accepted for inclusion in LSU Doctoral Dissertations by an authorized graduate school editor of LSU Digital Commons. For more information, please contactgradetd@lsu.edu.

RACKS, QUANDLES AND VIRTUAL KNOTS

A Dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in

The Department of Mathematics

by
V. Samuel Nelson
B.S. in Mathematics, University of Wyoming, 1996
M.S. in Mathematics, Louisiana State University, 1998
August 2002

Acknowledgments

This dissertation would not be possible without several contributions. It is a pleasure to thank Dr. L. Smolinsky, Dr. J. Scott Carter, Dr. S. Kamada, Dr. S. Satoh, Dr. L. Kauffman, and Dr. T. Kanenobu, each of whom played a role in guiding the development of this work.

This work was motivated in part by Polyak, Goussarov and Viro's work on Gauss diagrams and virtual knots, and partly by the work of J. Scott Carter and Seichi Kamada, my conversations with whom got me interested in racks and quandles.

It is a pleasure also to thank Louisiana State University for providing me with a pleasant working environment. A special thanks to Dr. R. A. Litherland for his wisdom and guidance as both advisor and coauthor.

This dissertation is dedicated to my wife, Shanda Nelson, for her tireless support and encouragement.

Table of Contents

Abstract

In this work we begin with a brief survey of the theory of virtual knots, which was announced in 1996 by L. Kauffman. This leads naturally to the subject of quandles and quandle homology, which we also briefly introduce.

Chapter 2 contains a proof in terms of Gauss diagrams that the forbidden moves of [8] unknot virtual knots. This chapter includes material which appeared in the Journal of Knot Theory and its Ramifications and is reprinted here by permission of World Scientific Publishing.

In chapter 3 (cowritten with my advisor R. A. Litherland) we confirm a conjecture of J. S. Carter et. al. that the long exact sequence in rack homology is split. We go on to show that for racks with homogeneous orbits, the lower bounds for the Betti numbers given in [2] are exact. We end chapter three with some explicit isomorphisms between Alexander quandles of certain forms and we describe some calculations of the second and third homology groups for a selection of quandles.

Chapter 4 contains a classification result for the category of finite Alexander quandles. This result give us easy conditions for comparing finite Alexander quandles as well as a general procedure for listing all Alexander quandles with a given number of elements. As an application we list the number of distinct Alexander quandles (and how many of these are connected) with up to 15 elements.

Chapter 1
Introduction

1.1 Virtual Knots

A *knot* is an embedding $k : S^1 \to S^3$ of the circle into the 3-sphere. A *link* is a disjoint collection of knots. To deal with knots and links combinatorially, we draw *knot diagrams*, four-valent graphs with each vertex representing a "crossing"; the undercrossing strand is indicated in the diagram by drawing the strand broken.

Two embeddings $k : S^1 \to S^3$ and $k' : S^1 \to S^3$ are *ambient isotopic* if there is an isotopy $S^3 \to S^3$ carrying $k(S^1)$ to $k'(S^1)$. Equivalently (for knots with a finite number of crossings, called *tame knots*) two diagrams are *isotopic* if one diagram can be transformed into the other via a finite sequence of planar isotopies and *Reidemeister moves*.

In [12], L. Kauffman introduced the notion of *virtual knots*, a generalization of knot theory which includes classical knot theory as a special case. Virtual knot theory generalizes classical knot theory in a way similar to how complex arithmetic generalizes real arithmetic.

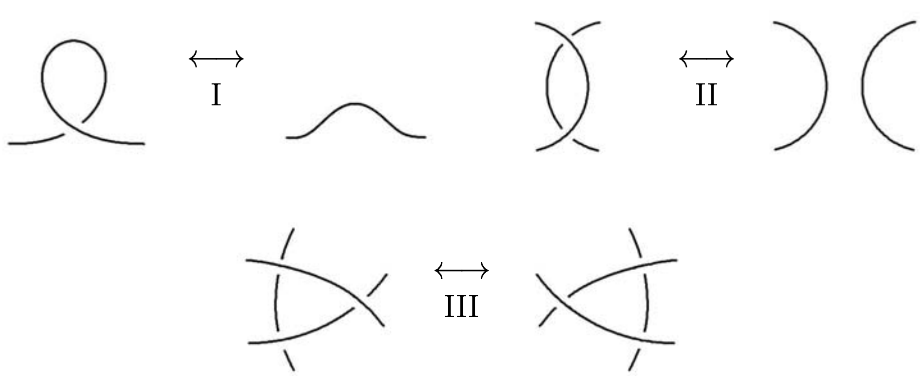


FIGURE 1.1. Reidemeister moves

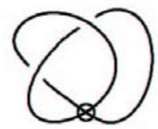


FIGURE 1.2. A virtual knot diagram

Every classical knot diagram is a planar 4-valent graph with vertices enhanced with crossing information; it is planar since it is the image of a projection onto a plane. In virtual knot theory, we consider equivalence classes under the usual Reidemeister moves of arbitrary 4-valent graphs with finitely many vertices, planar or not, with crossing information given at each vertex.

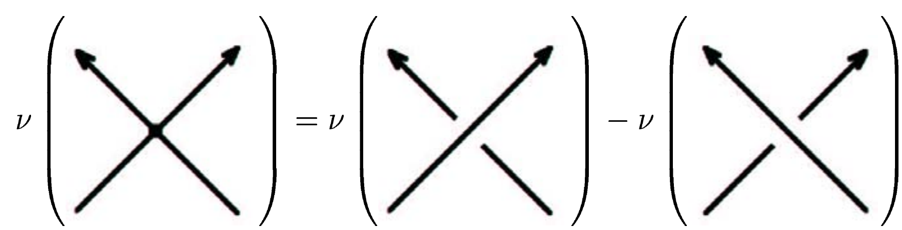
In order to draw nonplanar graphs in the plane, one normally introduces crossings; however, since the vertices are already interpreted as crossings, we distinguish these *virtual* crossings (which are merely artifacts of drawing a nonplanar graph in the plane) from the classical crossings by drawing them as circled intersections; neither strand crosses over or under the other in a virtual crossing (since the "crossing" isn't really there).

Since we now have a new type of crossing, we must specify how these crossings are allowed to interact with classical crossings by listing virtual Reidemeister moves. Since the virtual crossings are "not really there", we may move a strand with only virtual crossings anywhere we like. This "detour move" implies three all-virtual versions of ordinary Reidemeister moves, as well as a variant of the Reidemeister type III move with two virtual crossings and one classical crossing. See Chapter 1 figure 2.3 for details.

In [8], M. Polyak, M. Goussarov and O. Viro use the theory of virtual knots as an approach to calculating Vassiliev (or *finite-type*) invariants of classical knots. Finite type invariants are actually invariants of *singular knots*, that is, circles immersed (rather than embedded) in $\mathbb{R}^3$. Since every embedding is also an immersion, invariants of singular knots restrict to invariants of normal (non-singular) knots.

Singular knots may be viewed as equivalence classes of knotted 4-valent graphs under Reidemeister moves, planar isotopies which fix a neighborhood of each singular crossing, and a Reidemeister type III move variant where a strand may pass over or under a singular crossing.

Then a Vassiliev invariant is a function ν from the set of singular knot diagrams to an Abelian group A such that (1) the value of ν stays fixed under Reidemeister moves (this makes ν a knot invariant) and (2) ν satisfies



meaning that ν evaluates on a diagram with a singular crossing to ν on the same diagram with the singular crossing replaced by a positive crossing minus ν on the same diagram with the singular crossing replaced by a negative crossing.

Polyak, Goussarov and Viro noted that one can calculate finite type invariants from a *Gauss diagram* of a knot, which is a circle with points representing preimages of crossing points in usual planar knot diagram connected by chords. These chords are oriented "in the direction of gravity", i.e. with the undercrossing point receiving the arrowhead and the overcrossing point the tail. Each chord is then decorated with a plus or minus sign according to the sign (local writhe number) of the crossing.

Once can view a Gauss diagram as the preimage of a knot diagram with arrows connecting preimages of crossing points decorated with signs.

In representing knots with Gauss diagrams, we run into a potential problem: while every classical knot diagram has a corresponding Gauss diagram, the converse is not true. There are Gauss diagrams which do not correspond to classical knots. The insight of L. Kauffman, rediscovered by PGV, was to not worry about whether or not a given Gauss diagram corresponds to a classical knot and just consider equivalence classes of Gauss diagrams under the Gauss diagram versions of the classical Reidemeister moves; that is, to consider Gauss diagrams as defining "virtual" knots.

in [8], the authors revisit the topic of Reidemeister moves for virtual knots and discover that there are two Reidemeister-type moves which are not allowed; they dubbed these the "forbidden moves" since allowing them renders virtual knot theory trivial. They prove this fact in their paper via n-variations, and the proof is fairly abstract.

While doing some sample computations with virtual knots, I noticed that the forbidden moves work by sliding an arrowhead past an adjacent arrowhead or tail past an adjacent tail. I then used these two moves to construct two other move-sequences which allow us to move an arrowhead past an adjacent tail, thus showing that the forbidden moves unknot without the use of n-variations. My brief paper recording this fact appeared in the Journal of Knot Theory and its Ramifications in July 2001, and here makes up the bulk of chapter 1.

We thus have a generalization of classical knot theory, since every classical knot is also a virtual knot, and since the equivalence relations of classical knots form a subset of the equivalence relations of virtual knots, two equivalent classical knots are likewise equivalent classical knots.

Indeed, more is true; PGV point out that since the virtual moves don't change the fundamental quandle, virtually equivalent classical knots are classically equivalent.

1.2 Rack and Quandle Homology

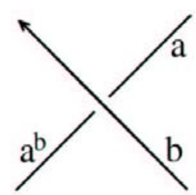
In [9], D. Joyce solved the (classical) knot classification problem by introducing the *fundamental quandle*, a complete invariant of nonsplit links in homology 3-spheres. A *quandle* is an algebraic object subject to axioms which are essentially the three Reidemeister moves translated into an algebraic form. Quandles and groups are closely related, and indeed the fundamental group of a knot is recoverable from the fundamental quandle via the associated group functor described by Fenn and Rourke in [5].

Two classical knots are ambient isotopic if and only if their fundamental quandles are isomorphic. Unfortunately, as with groups, it can be as difficult to tell whether two quandles are isomorphic as it is to tell whether two knots are ambient isotopic. We may then use the same strategy for distinguishing racks and quandles that we use with knots, namely, find invariants.

Thus quandles afford us a new way of thinking of the knot classification problem – we can find new knot invariants by finding invariants of quandles, which in turn are automatically invariants of knots.

In [6], R. Fenn, C. Rourke and B. Sanderson define a chain complex associated to any rack (quandles form a subcategory of the category of racks). The resulting homology and cohomology groups are thus examples of invariants of quandles which can be applied to define invariants of knots.

In [1], quandle cohomology is used by J. S. Carter, D. Jelsovsky, S. Kamada, L. Langford, and M. Saito to define a new family of knot invariants, the CJKLS state-sum invariants. Calculation of these invariants involves choosing an element ϕ of the second cohomology $H^2_Q(X)$ of a quandle X and a coloring of each arc in the knot diagram with elements of the quandle so that the following condition is satisfied at each crossing (note that the orientation of the undercrossing strand does not matter):



We then take the product over all crossings of $\phi(a, b)$ for positive crossings and $\phi(a, b)^{-1}$ for negative crossings, and finally we take the sum over all colorings of the arcs in the knot diagram to obtain the CJKLS invariant $\Phi_\phi(K)$ of the knot diagram K. One can check easily that the value of $\Phi_\phi(K)$ is unchanged by Reidemeister moves, so indeed it is an invariant of knots.

Further, cohomologous cocyles define the same invariant, so we have one CJKLS invariant for each element of the second cohomology of each quandle. Clearly, calculating the homology and cohomology groups of quandles is the necessary first step in calculating these new invariants.

In chapter 2 (co-authored with my advisor, R. A. Litherland), we show that the lower bounds for Betti numbers (the rank of each homology group) given in [2] are in fact equalities for a class of racks that includes dihedral and Alexander racks. We confirm a conjecture from the same paper by defining a splitting for the short exact sequence of quandle chain complexes. We define explicit isomorphisms between Alexander racks of certain forms, and we also calculate the second and third homology groups of some dihedral and Alexander quandles.

1.3 Finite Alexander Quandles

The category of Alexander quandles is a subcategory of the category of quandles. Any module over the ring $\Lambda = \mathbb{Z}[t^{\pm 1}]$ of Laurent polynomials in in one variable is also a Alexander quandle. Alexander quandles are particularly nice to work with since their quandle structure is determined by their module structure (though the converse is not true; there are nonisomorphic Λ-modules which are isomorphic as Alexander quandles). In particular, finite Alexander quandles are good candidates to use as coloring quandles in invariants such as CJKLS, since colorings of knot diagrams with quandle elements are homomorphisms from the knot quandle to the coloring quandle, and thus if the target is finite, we have a finite sum.

The final chapter of this dissertation contains my classification result for the category of finite Alexander quandles: two Alexander quandles are isomorphic if and only if their submodules $\text{Im}(1-t)$ are isomorphic as Λ-modules. This result thus reduces the problem of comparing Alexander quandles to comparing their $\text{Im}(1-t)$ submodules as Λ-modules.

This enables us to answer two of the previously open questions in [14], namely, when are two Alexander quandles of the form $\mathbb{Z}_n[t^{\pm 1}]/(t-a)$ where $\gcd(n,a) = 1$ (which we call *linear* quandles) isomorphic, and when are two linear quandles dual. We apply the classification result to obtain simple numeric conditions on a and b which are necessary and sufficient for $\Lambda_n/(t-a)$ and $\Lambda_n/(t-b)$ to be isomorphic and to be dual.

We also give an easy condition for an Alexander quandle to be *connected*, that is, for the set $X^a = X$ for all $a \in X$. In particular, we show that connected finite Alexander quandles are isomorphic if and only if they are isomorphic as Λ-modules. Connected quandles are of special interest since every knot quandle is connected, and therefore only connected quandles can act as coloring quandles for knots in invariants such as CJKLS (since a coloring quandle is the homomorphic image of the fundamental quandle, it must also be connected).

We then apply this classifying result to give a general procedure for classifying Alexander quandles of any finite order n. Any $\mathbb{Z}$-automorphism of an Abelian group defines an Alexander module structure on that group, so for a given n we consider each Abelian group of order n and find its $\mathbb{Z}$-automorphism group, then compare the submodules $\mathrm{Im}(1-t)$ for each element of the automorpishm group.

We show that every Alexander quandle of prime order is linear. In [7], Graña classifies indecomposable racks of order p^2 for p prime, and in the case that a rack X is an Alexander quandle, "indecomposable" means "connected." We show that Graña's result as it applies to Alexander quandles agrees with our classification theorem.

We show that for $n = p_1 p_2 \dots p_m$ a product of distinct primes, an Alexander quandle of order n is a direct sum of Alexander quandles of orders $p_1, p_2, \dots, p_m$.

This covers the cases $n = 2, 3, 5, 6, 7, 10, 11, 12, 13, 14$ and 15. For the cases $n =$ 4 and 9 we apply the classification of modules over PIDs to explicitly list all Alexander quandles of order 4 and 9. Only for the case $n = 8$ do we need to apply the general procedure of calculating $\mathrm{Aut}_{\mathbb{Z}}(\mathbb{Z}_2 \oplus \mathbb{Z}_4)$ to complete the calculation.

As a final application, we summarize our results in a table by listing the numbers of distinct Alexander quandles with up to fifteen elements and how many of each order are connected.

Chapter 2

Unknotting Virtual Knots via Gauss Diagram Forbidden Moves[1]

In 1996 Kauffman [12] introduced the theory of virtual knots, extending the topological concept of "knots" to include general Gauss codes. In 1999 Goussarov, Polyak and Viro [8] described virtual knots in terms of Gauss diagrams, which provide a visual way to represent Gauss codes.

Consider a classical knot diagram $K \subset \mathbb{R}^2$ as an immersion $K : S^1 \to \mathbb{R}^2$ of the circle in the plane with crossing information specified at each double point. A *Gauss diagram* for a classical knot diagram is an oriented circle considered as the preimage of the immersed circle with chords connecting the preimages of each double point. We specify crossing information on each chord by directing the chord toward the undercrossing point and decorating each with with signs specifying the local writhe number.

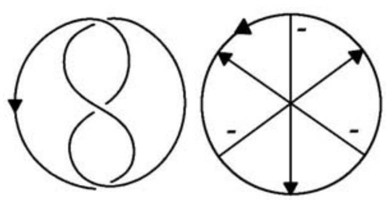


FIGURE 2.1. A simple knot and its Gauss Diagram

A *virtual knot* is an equivalence class of Gauss diagrams under the relations in Figure 2, which are the classical Reidemeister moves written in terms of Gauss diagrams. Note that there are several variations of move III depending on the orientations of the strands; we only depict two.

[1]This chapter incorporates material reprinted with the permisssion of the *Journal of Knot Theory and its Ramifcations,* Copyright ©2001 World Scientific Publishing.

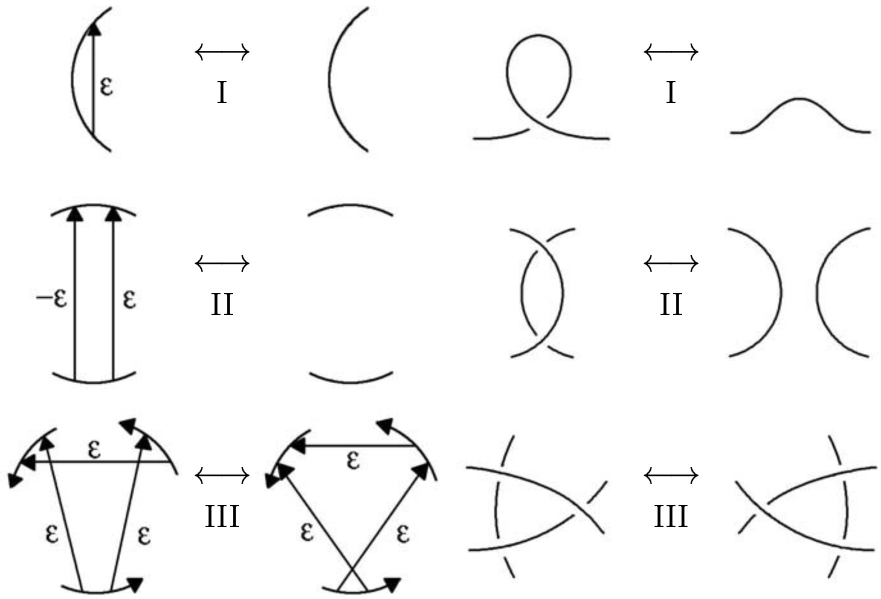


FIGURE 2.2. Moves I, II and III.

Not every Gauss diagram corresponds to a classical knot. Indeed, a Gauss diagram determines a 4-valent graph with crossing information specified at the vertices; such a graph represents a classical knot or link diagram if it is planar, but, of course, not every 4-valent graph is planar. To draw non-planar graphs in the plane, we usually introduce crossings, but these new crossings must be kept distinct from the vertices, which represent classical crossings specified by the Gauss diagram. To draw these non-planar graphs as *virtual knot diagrams*, we introduce *virtual crossings* to distinguish crossings arising from non-planarity of the graph from real crossings represented by vertices. Virtual crossings are drawn as an intersection surrounded by a circle. A virtual crossing has no over- or under-sense and no sign, and virtual crossings do not appear on Gauss diagrams – they are artifacts of our representing a non-planar graph in the plane.

A Gauss diagram determines a neighborhood of each real crossing and the order in which the edges entering and leaving such a neighborhood are connected. Outside these neighborhoods, we are free to draw the arcs connecting the neighborhoods

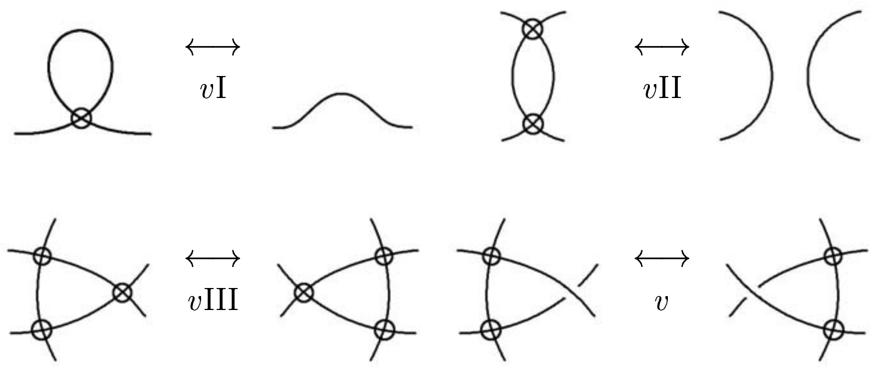


FIGURE 2.3. Virtual Moves

however we want, introducing virtual crossings as necessary. The *virtual moves* in figure 3 allow us to change any virtual knot diagram representing a particular Gauss diagram into any other virtual knot diagram representing the same Gauss diagram by allowing the interior of an arc containing only virtual crossings to be moved arbitrarily around the diagram.

Goussarov, Polyak and Viro [2] observe that there are two potential moves on virtual knot diagrams which resemble Reidemeister moves that are not allowed – these "forbidden moves" depicted in figure 4 alter the Gauss diagram, unlike the other virtual moves. Worse yet, if these two moves are allowed, together they allow us to unknot any knot, rendering the theory trivial. For this reason, these moves are called "forbidden". On Gauss diagrams, the forbidden move F_t moves an arrowtail of either sign past an adjacent arrowtail with either sign without conditions on the relative positions of the heads of these arrows, and the other forbidden move F_h moves an arrowhead past an arrowhead similarly.

The fact that allowing the forbidden moves would render virtual (and hence classical) knot theory trivial by making every knot unknotted is proven in [8] in terms of n-variations. In this paper we present a short combinatorial proof in terms

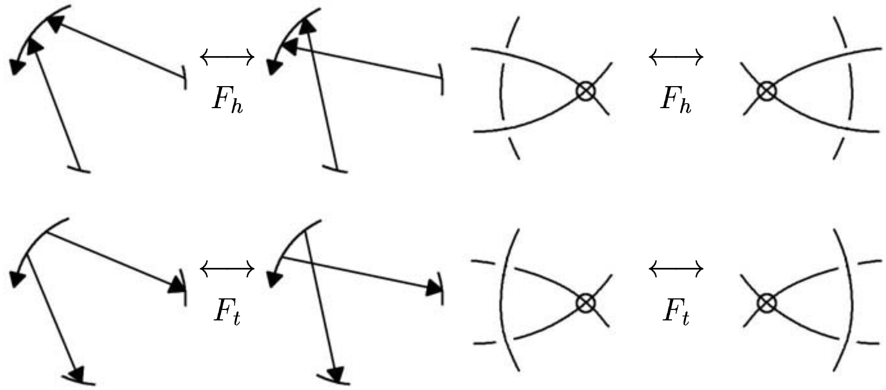


FIGURE 2.4. The Forbidden moves F_h and F_t.

of Gauss diagrams. The author has subsequently learned that Taizo Kanenobu [11] has a different combinatorial proof of this result using virtual braid moves.

Theorem 2.1. *Any Gauss diagram can be changed into any other Gauss diagram by a sequence of moves of types I, II, III, F_h and F_t.*

Proof. The forbidden move F_h allows us to move an arrowhead with either sign past an adjacent arrowhead with either sign without conditions on the tails of these respective arrows, and the move F_t lets us do the same with arrowtails. If we could move an arrowhead of either sign past an arrowtail of either sign in the same manner, we could simply rearrange the arrows in a given diagram at will.

The sequences of moves in figures 5 and 6 show how to move an arrowhead past an arrowtail of the same sign (move F_s; see Figure 4) or past an arrowtail of the opposite sign (move F_o; see Figure 5) using ordinary Reidemeister moves and both forbidden moves.

Now, to change one Gauss diagram into another with the same numbers of arrows of each sign, we simply use the forbidden moves and moves sequences F_o and F_s to rearrange the arrows. If we need more arrows of either sign, we can introduce them using type I moves and then move them into position with moves the F moves and sequences; if we have extra arrows, we can use the F moves and sequences to move

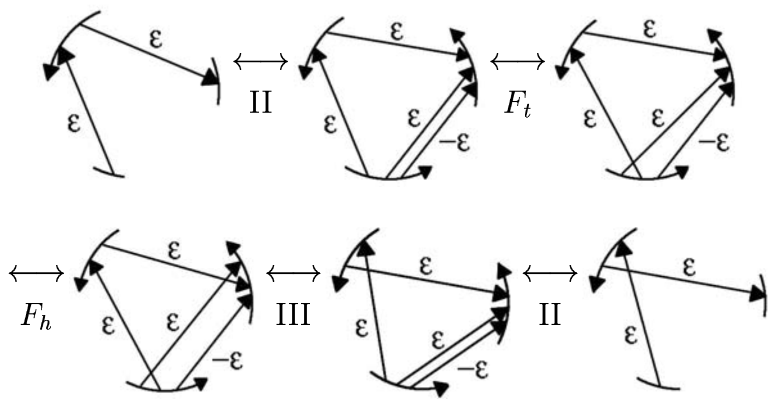


FIGURE 2.5. Move sequence F_s.

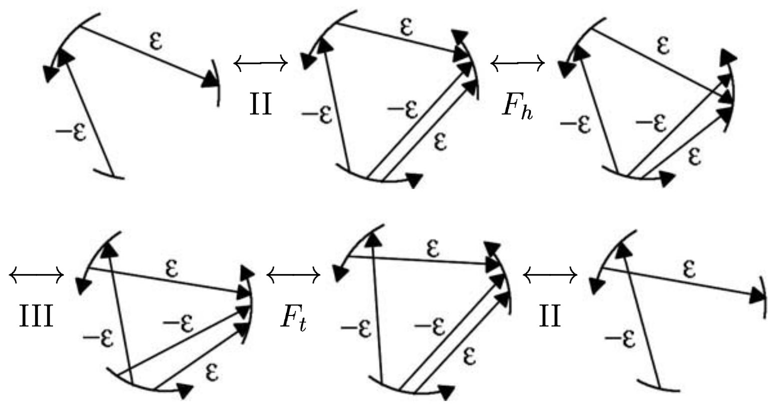


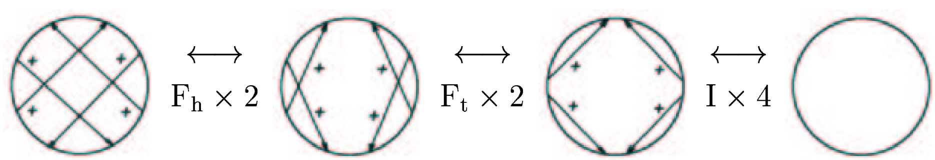
FIGURE 2.6. Move sequence F_o.

unwanted arrows into position to be removed by type I moves. In particular, any virtual knot can be unknotted by this technique. □

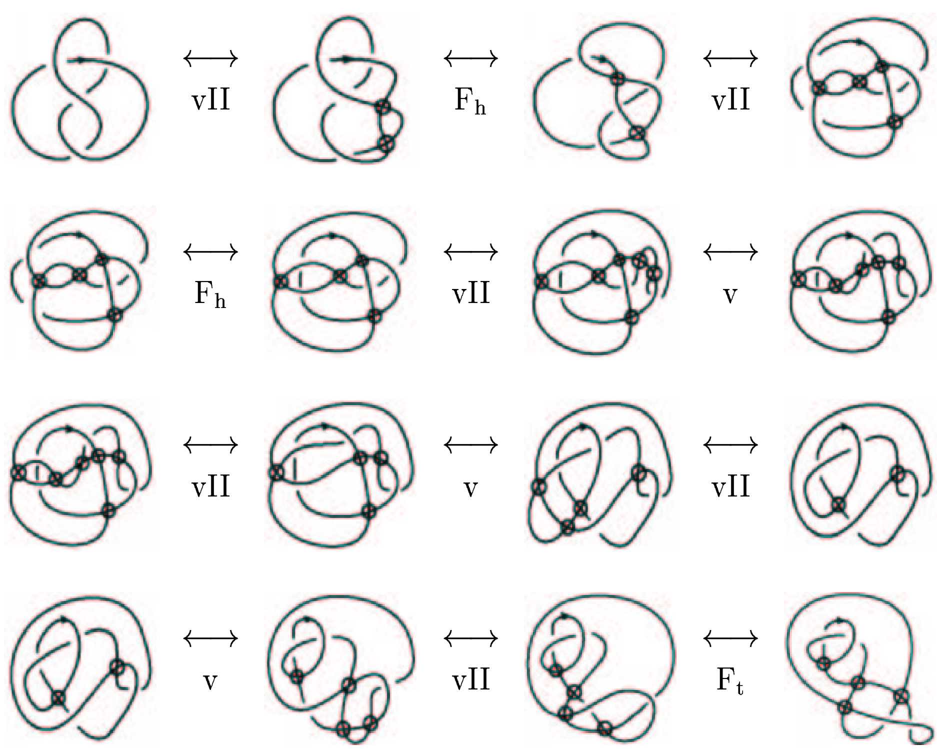
Note that the move sequences F_s and F_o each use both of the forbidden moves. If we define a new equivalence relation on Gauss diagrams by allowing the usual Reidemeister moves and one forbidden move but not the other, we arrive at the *welded knots* of S. Kamada [10] or the *weakly virtual knots* of S. Satoh [15]. Neither of the move sequences F_s or F_o can be constructed for welded knots since each move sequence requires the use of both forbidden moves.

As an application, we now demonstrate how the moves F_h and and F_t may be used to unknot any virtual knot by explicitly unknotting the trefoil using these moves.[2]

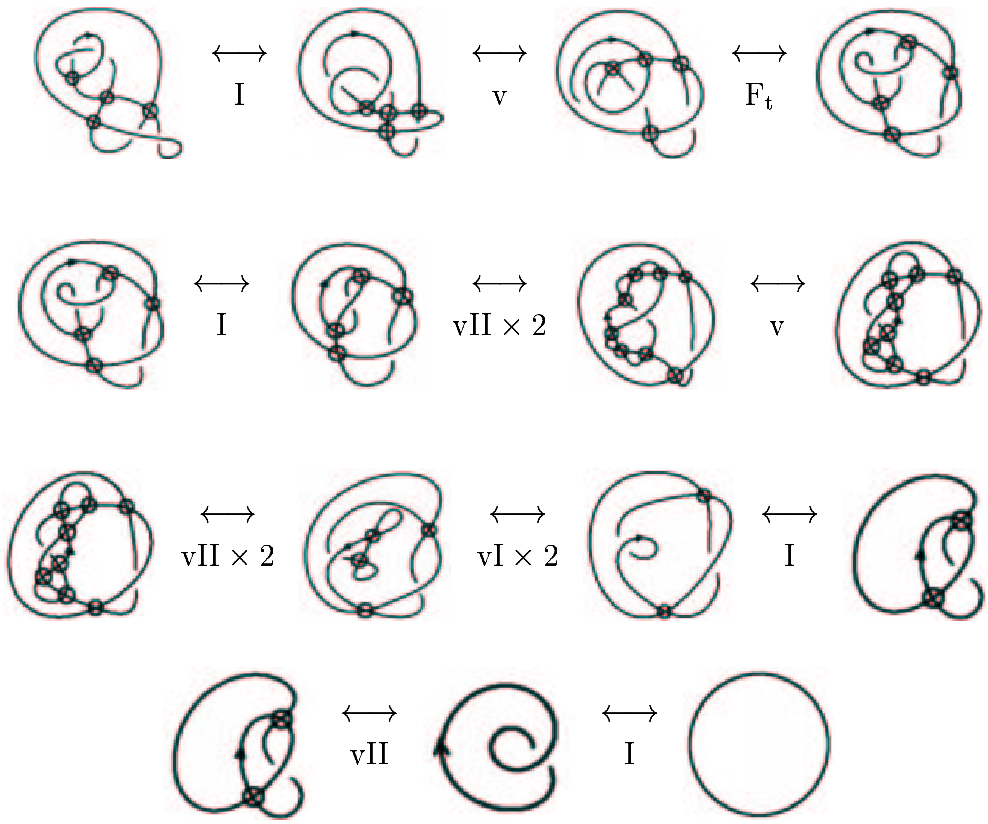
We begin with a Gauss diagram of the trefoil. Applying the forbidden move F_h twice lets us uncross the two pairs of arrowheads, and applying the forbidden move F_t twice lets us uncross the tails. Four Reidemeister type I moves later, we have a unknotted Gauss diagram.



Since virtual crossings and hence moves do not appear in Gauss diagrams, the virtual isotopy sequence is much longer than the Gauss diagram sequence.



[2]This demonstration originally appeared on the author's mathematics website hosted by the LSU Department of Mathematics.


I
v
F_t
I
vII × 2
v
vII × 2
vI × 2
I
vII
I

Chapter 3

The Betti Numbers of Some Finite Racks[1]

3.1 Introduction

We start by recalling some basic definitions. Let X be a non-empty set with a binary operation, which, following Fenn and Rourke [5], we write as exponentiation: $(a, b) \mapsto a^b$. This allows us to dispense with brackets by using the standard conventions that a^{b^c} means $a^{(b^c)}$ and a^{bc} means $(a^b)^c$. Then X is a *rack* if it satisfies the following two axioms.

(i) For all $a, b \in X$, there is a unique element c of X such that $c^a = b$.

(ii) (The rack identity) For all $a, b, c \in X$, $a^{bc} = a^{cb^c}$.

A *quandle* is a rack satisfying one further axiom.

(iii) (The quandle condition) For all $a \in X$, $a^a = a$.

A rack is *trivial* if $a^b = a$ for all a and b.

By axiom (i), the function $f_a\colon X \to X$ defined by $f_a(b) = b^a$ is a bijection. For $a, b \in X$, we set $a^{\bar{b}} = f_b^{-1}(a)$. Here $\bar{b}$ does not denote an element of X, but we may identify $\bar{b}$ with the inverse of b in the free group $F(X)$ on X. This allows us to define a (right) action of $F(X)$ on X, and by an *orbit* of X we mean an orbit under this action. The set of orbits of X will be denoted by $\mathcal{O}_X$, and the projection from X to $\mathcal{O}_X$ by π. We regard $\mathcal{O}_X$ as a trivial rack, and then π is a rack homomorphism.

We now define the class of racks that we shall study in §3 of this paper. Let X be a finite rack, and $a, b \in X$. Let $N(a, b)$ be the number of elements c of X such

[1] Coauthored with R. A. Litherland; to appear in the *Journal of Pure and Applied Algebra*

that $a^c = b$. Of course, $N(a, b) = 0$ if a and b are in different orbits. We say that X *has homogeneous orbits* if, for each orbit ω and each pair of elements a and b of ω, $N(a, b)$ depends only on ω. If this is so, then $|\omega|$ divides $|X|$ for each $\omega \in \mathcal{O}_X$, since the total number of actions $|X| = \sum_{b \in \omega} N(a, b)$, and we have $N(a, b) = |X|/|\omega|$ for all $a, b \in \omega$; we set $N_\omega = |X|/|\omega|$.

Let us consider some of the standard examples of racks in the light of this definition. Clearly (if uninterestingly), any trivial finite rack has homogeneous orbits. So does any finite conjugation rack $\mathrm{conj}(G)$. (Here G is a group, and $\mathrm{conj}(G)$ denotes G with the rack operation $g^h = h^{-1}gh$.) Fenn and Rourke use the term *conjugation rack* in a broader sense, to refer to any union of conjugacy classes in a group. In general, these do not have homogeneous orbits (consider $G - \{1\}$); however, any dihedral rack R_n does. (R_n is the set of reflections in the dihedral group of order $2n$.) This is easy to verify directly, and also follows from Proposition 1 below. Any cyclic rack (except the trivial rack of order 1) does not have homogeneous orbits. (The cyclic rack C_n of order n is the set $\{\,0, 1, \ldots, n-1\,\}$ with the operation $a^b = a + 1 \bmod n$. Here there is only one orbit, but $N(a, b) = n$ if $b = a + 1 \bmod n$, and is 0 otherwise.)

As an example of a non-quandle that does have homogeneous orbits, consider a four-element set $X = \{\,a, b, c, d\,\}$. We define the operation by specifying the permutations f_x of X: $f_a = f_b$ is the transposition exchanging a and b, and $f_c = f_d$ is the identity. One may check that the rack identity holds, most easily by using the third form of the identity given in [5]; the quandle condition clearly does not. The only non-trivial orbit is $\{\,a, b\,\}$, and $N(a, a) = N(a, b) = N(b, a) = N(b, b) = 2$.

Next we consider the finite Alexander racks. Let M be any module over the ring $\Lambda = \mathbb{Z}[t, t^{-1}]$ of one-variable Laurent polynomials. Then M may be made into a rack by the operation $a^b = ta + (1 - t)b$, and a rack obtained this way is called an

Alexander rack. For $M = \mathbb{Z}_n[t, t^{-1}]/(t+1)$, the Alexander rack is isomorphic to R_n.

Proposition 3.1. *Let M be a finite Λ-module, and let $\bar{M}$ be the quotient of M by the submodule $(1-t)M$. When M is considered as an Alexander rack:*

(a) *M has homogeneous orbits; and*

(b) *$\mathcal{O}_M$ may be identified with $\bar{M}$.*

Proof. Let $p\colon M \to \bar{M}$ be the natural map. We have $a^x = a^y$ iff $(1-t)(x-y) = 0$, so for any $a, b \in M$, $N(a,b)$ is either 0 or the order of $\mathrm{Ker}(1-t\colon M \to M)$. The result will follow once we show that, for $a, b \in M$, the following statements are equivalent:

(1) a and b are in the same orbit;

(2) $p(a) = p(b)$;

(3) $N(a,b) \neq 0$.

Now $a - a^b = (1-t)(a-b)$, so $p(a) = p(a^b)$, from which it follows that (1) implies (2). If $p(a) = p(b)$, then $b = a + (1-t)c$ for some $c \in M$, which gives $b = a^{a+c}$. Thus (2) implies (3), and trivially (3) implies (1). □

In [6], Fenn, Rourke and Sanderson associate to each rack X a $\square$−set (a cubical set without degeneracies) as follows. The set of n-cubes is X^n, and the face maps $\partial_i^\epsilon\colon X^n \to X^{n-1}$ ($1 \leq i \leq n$, $\epsilon = 0$ or 1) are defined by

$$\partial_i^0(x_1, \ldots, x_n) = (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n);$$

$$\partial_i^1(x_1, \ldots, x_n) = (x_1^{x_i}, \ldots, x_{i-1}^{x_i}, x_{i+1}, \ldots, x_n).$$

We follow Carter, Jelsovsky, Kamada and Saito [2] in denoting the associated chain complex by $C^R_*(X)$, and calling its homology $H^R_*(X)$ the *rack homology* of X. Thus $C^R_n(X)$ is the free abelian group on X^n, and the boundary map $\partial\colon C^R_n(X) \to C^R_{n-1}(X)$ is defined by $\partial = \sum_{i=1}^n (-1)^i(\partial_i^0 - \partial_i^1)$. Now suppose that X is a quandle, and define $C^D_n(X)$ to be the subgroup of $C^R_n(X)$ generated by n-tuples $(x_1, \ldots, x_n)$ with $x_i = x_{i+1}$ for some i, $1 \leq i < n$. It follows from the quandle condition that $C^D_*(X)$ is a subcomplex of $C^R_*(X)$. The quotient complex is denoted by $C^Q_*(X)$, and its homology $H^Q_*(X)$ is called the *quandle homology* of X. The homology $H^D_*(X)$ of $C^D_*(X)$ is the *degeneration homology* of X. We shall use the convention that in an expression such as $C^W_n(X)$, W may be any one of R, Q or D if X is a quandle, but is always R if not. There are Betti numbers $\beta^W_n(X) = \text{rank} H^W_n(X)$. There are also homology and cohomology groups with coefficients in any abelian group G, denoted by $H^W_n(X; G)$ and $H^n_W(X; G)$. For the applications to knot theory, the groups of interest are the cohomology groups with coefficients in $\mathbb{Z}_p$ (the integers modulo a prime p), but since these are determined by the integral homology groups we shall concentrate on the latter. The homology groups in dimensions 0 and 1 are easily computed; see Proposition 3.8 of [2]. When the set of orbits of X is regarded as a trivial rack, the chain complex $C^W_*(\mathcal{O}_X)$ has all its boundary maps zero, so $H^W_n(\mathcal{O}_X) = C^W_n(X)$. Thus when X is a finite rack with m orbits, $H^W_n(\mathcal{O}_X)$ $(n \geq 1)$ is a free abelian group of rank m^n, $m(m-1)^{n-1}$ or $m^n - m(m-1)^{n-1}$ for $W = R$, Q or D, respectively. In [2], it is shown that in this case $\beta^W_n(X) \geq \beta^W_n(\mathcal{O}_X)$. (It is not explicitly stated in [2] that the case $W = R$ holds when X is not a quandle, but this is so by essentially the same proof.) We now state our main result, which shows that these bounds are exact in many cases.

Theorem 3.2. *Let X be a finite rack with homogeneous orbits. Then $\beta_n^W(X) = \beta_n^W(\mathcal{O}_X)$, and the torsion subgroup of $H_n^W(X)$ is annihilated by $|X|^n$.*

Remark 3.3. *While this paper was in preparation, we learned that Mochizuki has proved an almost identical theorem by a different method ([13], Theorem 1.1). The main difference in the results is that Mochizuki's theorem applies only to finite Alexander racks.*

The case $W = R$ of Theorem 1.1 is proved directly. For the other cases, we need to prove conjecture 3.11 of [2]; this is done in §3.2. Theorem 3.2 is proved in §3.3, and in §3.4 we report on some machine calculations of homology groups.

3.2 Splitting the Difference Between Quandle and Rack Homology

In this section, X will always denote a quandle. Also, we redefine $C_0^R(X)$ and $C_0^Q(X)$ to be 0. ($C_0^D(X)$ is already 0.) This loses no information, and allows us to avoid treating dimension 0 as a special case at various points. Strictly speaking, we shall be working with the reduced complexes $\tilde{C}_*^R(X)$ and $\tilde{C}_*^Q(X)$, but we abuse notation by leaving off the tildes. From the short exact sequence

$$0 \to C_*^D(X) \to C_*^R(X) \to C_*^Q(X) \to 0 \tag{3.1}$$

of chain complexes, we have a long exact sequence

$$\cdots \to H_n^D(X) \to H_n^R(X) \to H_n^Q(X) \to H_{n-1}^D(X) \to \dots$$

of homology groups. In [2] it is proved (in Proposition 3.9) that the connecting homomorphism $H_n^Q(X) \to H_{n-1}^D(X)$ is the zero map when $n = 3$, and conjectured that this is so for all n; in [4] (Theorem 8.2) the case $n = 4$ is proved. We show that the conjecture is indeed true; in fact we prove more.

Theorem 3.4. *For any quandle X, the short exact sequence* (1) *is split.*

Remark 3.5. *It is easy to see that, for each n, the sequence*

$$0 \to C_n^D(X) \to C_n^R(X) \to C_n^Q(X) \to 0$$

of abelian groups is split, but the obvious splittings are not compatible with the boundary maps.

If $\mathbf{x} = (x_1, \ldots, x_n) \in X^n$ and $y \in X$, we set $\mathbf{x} * y = (x_1, \ldots, x_n, y) \in X^{n+1}$ and $\mathbf{x}^y = (x_1^y, \ldots, x_n^y) \in X^n$. Then, for $c \in C_n^R(X)$ we define $c * y \in C_{n+1}^R(X)$ and $c^y \in C_n^R(X)$ by linearity in c. Note that $\partial(c * y) = \partial(c) * y + (-1)^{n+1}(c - c^y)$. Next we define homomorphisms $\alpha_n \colon C_n^R(X) \to C_n^R(X)$ by induction on n. We take α_1 to be the identity map, and for $n \geq 1$, $\mathbf{x} \in X^n$ and $y \in X$ we set

$$\alpha_{n+1}(\mathbf{x} * y) = \alpha_n(\mathbf{x}) * y - \alpha_n(\mathbf{x}) * x_n.$$

We also define homomorphisms $\beta_n \colon C_n^R(X) \to C_{n+1}^R(X)$ by $\beta_n(\mathbf{x}) = \alpha_n(\mathbf{x}) * x_n$. Then, for any $c \in C_n^R(X)$ and $y \in X$ we have

$$\alpha_{n+1}(c * y) = \alpha_n(c) * y - \beta_n(c).$$

Lemma 3.6. *The homomorphisms $\alpha_n \colon C_n^R(X) \to C_n^R(X)$ form a chain map $\alpha \colon C_*^R(X) \to C_*^R(X)$.*

Proof. Note first that for $\mathbf{x} \in X^n$ and $y \in X$ we have $\alpha_n(\mathbf{x}^y) = \alpha_n(\mathbf{x})^y$. We prove that $\partial \alpha_n = \alpha_{n-1}\partial$ by induction on $n \geq 2$. For $n = 2$ we have $\alpha_2(x, y) = (x, y) - (x, x)$, so since (x, x) is a cycle, $\partial \alpha_2(x, y) = \partial(x, y) = \alpha_1 \partial(x, y)$. Suppose then that the result is true for some $n \geq 2$, and let $\mathbf{x} \in X^n$ and $y \in X$. We compute

$$\begin{aligned}
\partial\alpha_{n+1}(\mathbf{x} * y) &= \partial\big(\alpha_n(\mathbf{x}) * y\big) - \partial\big(\alpha_n(\mathbf{x}) * x_n\big) \\
&= \partial\alpha_n(\mathbf{x}) * y + (-1)^{n+1}\big(\alpha_n(\mathbf{x}) - \alpha_n(\mathbf{x})^y\big) \\
&\qquad - \partial\alpha_n(\mathbf{x}) * x_n - (-1)^{n+1}\big(\alpha_n(\mathbf{x}) - \alpha_n(\mathbf{x})^{x_n}\big) \\
&= \alpha_{n-1}\partial(\mathbf{x}) * y - \alpha_{n-1}\partial(\mathbf{x}) * x_n + (-1)^n\alpha_n(\mathbf{x}^y) - (-1)^n\alpha_n(\mathbf{x}^{x_n})
\end{aligned}$$

and

$$\begin{aligned}
\alpha_n\partial(\mathbf{x} * y) &= \alpha_n\big(\partial(\mathbf{x}) * y + (-1)^{n+1}(\mathbf{x} - \mathbf{x}^y)\big) \\
&= \alpha_{n-1}\partial(\mathbf{x}) * y - \beta_{n-1}\partial(\mathbf{x}) - (-1)^n\alpha_n(\mathbf{x}) + (-1)^n\alpha_n(\mathbf{x}^y).
\end{aligned}$$

Hence $\partial\alpha_{n+1}(\mathbf{x} * y) = \alpha_n\partial(\mathbf{x} * y)$ iff

$$\alpha_{n-1}\partial(\mathbf{x}) * x_n + (-1)^n\alpha_n(\mathbf{x}^{x_n}) = \beta_{n-1}\partial(\mathbf{x}) + (-1)^n\alpha_n(\mathbf{x}). \tag{2}$$

Now, for $1 \leq i < n$ and $\epsilon = 0$ or 1, $\partial_i^\epsilon(\mathbf{x})$ is an element of X^{n-1} with last entry x_n, so $\alpha_{n-1}\partial_i^\epsilon(\mathbf{x}) * x_n = \beta_{n-1}\partial_i^\epsilon(\mathbf{x})$. Further,

$$\begin{aligned}
&\alpha_{n-1}\partial_n^0(\mathbf{x}) * x_n - \beta_{n-1}\partial_n^0(\mathbf{x}) = \alpha_n\big(\partial_n^0(\mathbf{x}) * x_n\big) = \alpha_n(\mathbf{x}) \\
\text{and} \qquad &\alpha_{n-1}\partial_n^1(\mathbf{x}) * x_n - \beta_{n-1}\partial_n^1(\mathbf{x}) = \alpha_n\big(\partial_n^1(\mathbf{x}) * x_n\big) = \alpha_n(\mathbf{x}^{x_n}).
\end{aligned}$$

(The last step here uses the quandle condition.) It follows that

$$\alpha_{n-1}\partial(\mathbf{x}) * x_n - \beta_{n-1}\partial(\mathbf{x}) = (-1)^n\big(\alpha_n(\mathbf{x}) - \alpha_n(\mathbf{x}^{x_n})\big),$$

proving equation (2), and with it the lemma. □

Proof of Theorem 3.4. We show that the chain map $C_*^R(X) \to C_*^R(X)$ sending c to $c - \alpha(c)$ is a projection onto the subcomplex $C_*^D(X)$. We must prove the following two statements.

(a) If $c \in C_n^D(X)$ then $\alpha_n(c) = 0$.

(b) If $c \in C_n^R(X)$ then $c - \alpha_n(c) \in C_n^D(X)$.

For $n = 1$, $C_n^D(X) = 0$, so (a) is true in this case. Let $\mathbf{x} \in X^n$ ($n \geq 1$) and $y \in X$, and suppose that $\mathbf{x} * y \in C_{n+1}^D(X)$. Then either $\mathbf{x} \in C_n^D(X)$ or $x_n = y$, and it follows that $\alpha_{n+1}(\mathbf{x} * y) = 0$ (using induction in the first case). Thus (a) is proved. As for (b), this is clear for $n = 1$, so suppose that it holds for some $n \geq 1$ and take $\mathbf{x} \in X^n$ and $y \in X$. Then

$$\begin{aligned} \mathbf{x} * y - \alpha_{n+1}(\mathbf{x} * y) - \mathbf{x} * x_n &= \big(\mathbf{x} - \alpha_n(\mathbf{x})\big) * y - \big(\mathbf{x} - \alpha_n(\mathbf{x})\big) * x_n \\ &\in C_{n+1}^D(X). \end{aligned}$$

Since $\mathbf{x} * x_n$ is in $C_{n+1}^D(X)$ by the inductive hypothesis, so is $\mathbf{x} * y - \alpha_{n+1}(\mathbf{x} * y)$, and (b) follows. □

We shall denote the free abelian group on a set A by $\mathbb{Z}[A]$. (This is consistent with the usage $\mathbb{Z}[G]$ for a group ring.) It is shown in Proposition 3.9 of [2] that $H_2^D(X) \cong \mathbb{Z}[\mathcal{O}_X]$. Combining this with Theorem 3.4 gives the first assertion of the next theorem; for the second we need some lemmas.

Theorem 3.7. *For any quandle X, we have*

$$\begin{aligned} & H_2^R(X) \cong H_2^Q(X) \oplus \mathbb{Z}[\mathcal{O}_X] \\ \textit{and} \quad & H_3^R(X) \cong H_3^Q(X) \oplus H_2^Q(X) \oplus \mathbb{Z}[\mathcal{O}_X^2]. \end{aligned}$$

Let $C_n^L(X)$ be the subgroup of $C_n^D(X)$ generated by n-tuples $(x_1, \ldots, x_n)$ with $x_i = x_{i+1}$ for some i, $2 \leq i < n$. (We use the letter L because the degeneracy occurs late in these n-tuples.) Note that $C_n^L(X) = 0$ for $n < 3$.

Lemma 3.8. *The subgroups $C_n^L(X)$ form a subcomplex of $C_*^D(X)$.*

Proof. Let $\mathbf{x} = (x_1, \ldots, x_n)$ have $x_i = x_{i+1}$ for some i with $2 \leq i < n$. Since $\partial_i^\epsilon(\mathbf{x}) = \partial_{i+1}^\epsilon(\mathbf{x})$ for $\epsilon = 0$ or 1 (and, as for any $\mathbf{x} \in X^n$, $\partial_1^0(\mathbf{x}) = \partial_1^1(\mathbf{x})$), we have

$$\partial(\mathbf{x}) = \sum_{j=2}^{i-1}(-1)^j\big(\partial_j^0(\mathbf{x}) - \partial_j^1(\mathbf{x})\big) + \sum_{j=i+2}^{n}(-1)^j\big(\partial_j^0(\mathbf{x}) - \partial_j^1(\mathbf{x})\big). \tag{3}$$

Fix j and ϵ, and set $\mathbf{y} = (y_1, \ldots, y_{n-1}) = \partial_j^\epsilon(\mathbf{x})$. If $i = 2$, the first sum in (3) is empty. If $i > 2$ and $2 \leq j \leq i-1$, $y_{i-1} = y_i$, so $\mathbf{y} \in C_{n-1}^L(X)$. For $i+2 \leq j \leq n$, $y_i = y_{i+1}$, so again $\mathbf{y} \in C_{n-1}^L(X)$, and it follows that $\partial(\mathbf{x}) \in C_{n-1}^L(X)$. □

Lemma 3.9. *There is an isomorphism of chain complexes $C_*^D(X) \cong C_{*-1}^Q(X) \oplus C_*^L(X)$.*

Proof. We let $i\colon C_*^D(X) \to C_*^R(X)$ and $j\colon C_*^L(X) \to C_*^D(X)$ be the inclusions. Define $r\colon C_{*-1}^R(X) \to C_*^D(X)$ by

$$r_n(x_1, x_2, \ldots, x_{n-1}) = (x_1, x_1, x_2, \ldots, x_{n-1})$$

for $n \geq 2$. (For $n \leq 1$ the groups involved are 0.) A straightforward computation shows that r is a chain map. Since $r(C_{*-1}^D(X)) \leq C_*^L(X)$, r induces $s\colon C_{*-1}^D(X) \to C_*^L(X)$.

Now r is injective, $C_*^D(X)$ is generated by $\mathrm{Im}(r)$ and $C_*^L(X)$, and $\mathrm{Im}(r) \cap C_*^L(X) = \mathrm{Im}(r \circ i) = \mathrm{Im}(j \circ s)$. Hence there is a short exact sequence

$$0 \to C_{*-1}^D(X) \xrightarrow{\phi} C_{*-1}^R(X) \oplus C_*^L(X) \xrightarrow{\psi} C_*^D(X) \to 0,$$

where $\phi(c) = (i(c), -s(c))$ and $\psi(d, e) = r(d) + j(e)$. By Theorem 1, there is an isomorphism of chain complexes $\chi\colon C_{*-1}^R(X) \to C_{*-1}^Q(X) \oplus C_{*-1}^D(X)$ such that, for $c \in C_{*-1}^D(X)$, $\chi i(c) = (0, c)$. Then $C_*^D(X)$ is isomorphic to the cokernel of

$$(\chi \oplus \mathrm{id}) \circ \phi\colon C_{*-1}^D(X) \to C_{*-1}^Q(X) \oplus C_{*-1}^D(X) \oplus C_*^L(X).$$

But, for $c \in C^D_{*-1}(X)$, $(\chi \oplus \mathrm{id})(\phi(c)) = (0, c, -s(c))$, so this cokernel is isomorphic as a chain complex to $C^Q_{*-1}(X) \oplus C^L_*(X)$, and we are done. □

We denote the homology of $C^L_*(X)$ by $H^L_*(X)$.

Lemma 3.10. *For any quandle X, $H^L_3(X) \cong \mathbb{Z}[\mathcal{O}^2_X]$.*

Proof. A basis for $C^L_3(X)$ consists of all elements of X^3 of the form (x, y, y), and these are all cycles. The group $C^L_4(X)$ is generated by all elements of X^4 of one of the forms (x, y, y, z) and (x, z, y, y), and we have

$$\partial(x, y, y, z) = (x, y, y) - (x^z, y^z, y^z)$$

$$\text{and} \qquad \partial(x, z, y, y) = (x, y, y) - (x^z, y, y).$$

It follows that $H^L_3(X)$ is free abelian, with a basis consisting of the equivalence classes of triples (x, y, y) under the equivalence relation $\sim$ generated by

$$(x, y, y) \sim (x^z, y, y) \sim (x^z, y^z, y^z) \qquad \text{for all } x, y, z \in X.$$

Given $x, y, z \in X$, let w be the element of X such that $w^z = x$. Then $(w, y, y) \sim (w^z, y, y) = (x, y, y)$ and $(w, y, y) \sim (w^z, y^z, y^z) = (x, y^z, y^z)$, so $(x, y, y) \sim (x, y^z, y^z)$. It follows that $(x, y, y) \sim (x', y', y')$ iff $\pi(x) = \pi(x')$ and $\pi(y) = \pi(y')$, so the set of equivalence classes of $\sim$ may be identified with $\mathcal{O}^2_X$. □

The second assertion of Theorem 3.7 follows immediately from Theorem 3.4 and Lemmas 3.9 and 3.10.

3.3 Proof of Theorem 3.2

In this section, X is a rack with homogeneous orbits, and $\mathbf{x} = (x_1, \ldots, x_n)$ is an element of X^n ($n >= 0$). Define $\phi_n^j : C_n^R(X) \to C_n^R(X)$ by

$$\phi_n^j(\mathbf{x}) = \begin{cases} \mathbf{x} & \text{for } j = 0 \\ \sum_{\mathbf{y} \in X^j} (x_1^{y_1}, \ldots, x_j^{y_j}, x_{j+1}, \ldots, x_n) & \text{for } 1 \le j \le n \\ |X|^{j-n} \phi_n^n(\mathbf{x}) & \text{for } j > n \end{cases}$$

and $D_n^j : C_n^R(X) \to C_{n+1}^R(X)$ by

$$D_n^j(\mathbf{x}) = \begin{cases} \sum_{\mathbf{y} \in X^j} (x_1^{y_1}, \ldots, x_{j-1}^{y_{j-1}}, x_j, y_j, x_{j+1}, \ldots, x_n) & \text{for } 1 \le j \le n \\ 0 & \text{for } j > n. \end{cases}$$

Note that $D_n^1 = \sum_{y \in X} (x_1, y, x_2, \ldots, x_n)$.

We have homomorphisms of graded groups $\phi^j = (\phi_n^j)_{n=0}^{\infty} \colon C_*^R(X) \to C_*^R(X)$ for $j \ge 0$ and $D^j = (D_n^j)_{n=0}^{\infty} \colon C_*^R(X) \to C_{*+1}^R(X)$ for $j \ge 1$. We will show through a series of lemmas that D^j is a chain homotopy carrying ϕ^j to $|X|\phi^{j-1}$, and hence each ϕ^j is chain homotopic to $|X|^j$ times the identity. Note that this also implies ϕ^j is a chain map.

Lemma 3.11. *Let G be an abelian group. Then if $g \colon X \to G$ is a function we have*

$$\sum_{y \in X} g(x^y) = \sum_{y \in X} g(x^{yw})$$

for any word $w \in F(X)$ in the free group on X.

Proof. As y runs over X, x^y runs over $\pi(x)$, taking on each value $N_{\pi(x)}$ times. Thus

$$\sum_{y \in X} g(x^y) = N_{\pi(x)} \sum_{z \in \pi(x)} g(z).$$

The automorphism $f_w : X \to X$ given by $f_w(x) = x^w$ is in particular a bijection and carries $\pi(x)$ to itself, so the restriction $f \mid_{\pi(x)}$ is also a bijection. Hence the sum

$$\sum_{y\in X} g(x^{yw}) = \sum_{y\in X} g(f_w(x^y)) = N_{\pi(x)} \sum_{z\in\pi(x)} g(z) = \sum_{y\in X} g(x^y).$$

□

Lemma 3.12. *Let G be an abelian group. Then if $g\colon X \to G$ is a function we have*

$$\sum_{y\in X} g(x^y) = \sum_{y\in X} g(x^{wy})$$

for any word $w \in F(X)$ in the free group on X.

Proof. Since $\pi(x^w) = \pi(x)$, we have

$$\sum_{y\in X} g(x^y) = N_{\pi(x)} \left(\sum_{z\in\pi(x)} g(z) \right) = N_{\pi(x^w)} \left(\sum_{z\in\pi(x^w)} g(z) \right) = \sum_{y\in X} g(x^{wy}).$$

□

Lemma 3.13. *For $1 \le i \le j \le n$, $\partial_i^0 D_n^j(\mathbf{x}) = \partial_i^1 D_n^j(\mathbf{x})$.*

Proof. For $i < j$, we have

$$\begin{aligned}\partial_i^0 D_n^j(\mathbf{x}) &= \partial_i^0 \left(\sum_{\mathbf{y}\in X^j} (x_1^{y_1}, \dots, x_{j-1}^{y_{j-1}}, x_j, y_j, x_{j+1}, \dots, x_n) \right) \\ &= \sum_{\mathbf{y}\in X^j} (x_1^{y_1}, \dots, x_{i-1}^{y_{i-1}}, x_{i+1}^{y_{i+1}}, \dots, x_{j-1}^{y_{j-1}}, x_j, y_j, \dots, x_n)\end{aligned}$$

and

$$\begin{aligned}\partial_i^1 D_n^j(\mathbf{x}) &= \partial_i^1 \left(\sum_{\mathbf{y}\in X^j} (x_1^{y_1}, \dots, x_{j-1}^{y_{j-1}}, x_j, y_j, x_{j+1}, \dots, x_n) \right) \\ &= \sum_{\mathbf{y}\in X^j} (x_1^{y_1 x_i^{y_i}}, \dots, x_{i-1}^{y_{i-1} x_i^{y_i}}, x_{i+1}^{y_{i+1}}, \dots, x_{j-1}^{y_{j-1}}, x_j, y_j, \dots, x_n).\end{aligned}$$

For $i = j$ we have

$$\partial_j^0 D_n^j(\mathbf{x}) = \sum_{\mathbf{y}\in X^j} (x_1^{y_1}, \dots, x_{j-1}^{y_{j-1}}, y_j, \dots, x_n)$$

and

$$\partial_j^1 D_n^j(\mathbf{x}) = \sum_{\mathbf{y}\in X^j} (x_1^{y_1 x_j}, \ldots, x_{j-1}^{y_{j-1} x_j}, y_j, \ldots, x_n).$$

Applying Lemma 3.11 $i-1$ times, the sums agree as required. □

Lemma 3.14. *For* $1 \le i \le j < n$, $D_{n-1}^j \partial_i^0(\mathbf{x}) = D_{n-1}^j \partial_i^1(\mathbf{x})$.

Proof. For $1 \le i \le j$,

$$\begin{aligned} D_{n-1}^j \partial_i^0(\mathbf{x}) &= D_{n-1}^j (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \\ &= \sum_{\mathbf{y}\in X^j} (x_1^{y_1}, \ldots, x_{i-1}^{y_{i-1}}, x_{i+1}^{y_i}, \ldots, x_j^{y_{j-1}}, x_{j+1}, y_j, x_{j+2}, \ldots, x_n) \end{aligned}$$

and

$$\begin{aligned} D_{n-1}^j \partial_i^1(\mathbf{x}) &= D_{n-1}^j (x_1^{y_1}, \ldots, x_{i-1}^{y_{i-1}}, x_{i+1}, \ldots, x_n) \\ &= \sum_{\mathbf{y}\in X^j} (x_1^{x_i y_1}, \ldots, x_{i-1}^{x_i y_{i-1}}, x_{i+1}^{y_i}, \ldots, x_j^{y_{j-1}}, x_{j+1}, y_j, x_{j+2}, \ldots, x_n). \end{aligned}$$

Applying Lemma 3.12 $i-1$ times, the sums agree as required. □

Lemma 3.15. *For* $1 \le j \le n$, $\partial_{j+1}^0 D_n^j(\mathbf{x}) = |X| \phi_n^{j-1}(\mathbf{x})$.

Proof.

$$\begin{aligned} \partial_{j+1}^0 D_n^j(\mathbf{x}) &= \partial_{j+1}^0 \left(\sum_{\mathbf{y}\in X^j} (x_1^{y_1}, \ldots, x_{j-1}^{y_{j-1}}, x_j, y_j, x_{j+1}, \ldots, x_n) \right) \\ &= \sum_{\mathbf{y}\in X^j} (x_1^{y_1}, \ldots, x_{j-1}^{y_{j-1}}, x_j, x_{j+1}, \ldots, x_n) \\ &= \sum_{y_j \in X} \phi_n^{j-1}(\mathbf{x}) \\ &= |X| \phi_n^{j-1}(\mathbf{x}). \end{aligned}$$

□

Lemma 3.16. *For* $1 \le j \le n$, $\partial_{j+1}^1 D_n^j(\mathbf{x}) = \phi_n^j(\mathbf{x})$.

Proof.

$$\begin{aligned}
\partial_{j+1}^1 D_n^j(\mathbf{x}) &= \partial_{j+1}^1 \left(\sum_{\mathbf{y}\in X^j} (x_1^{y_1}, \ldots, x_{j-1}^{y_{j-1}}, x_j, y_j, x_{j+1}, \ldots, x_n) \right) \\
&= \sum_{\mathbf{y}\in X^j} (x_1^{y_1 y_j}, \ldots, x_{j-1}^{y_{j-1} y_j}, x_j^{y_j}, x_{j+1}, \ldots, x_n) \\
&= \sum_{\mathbf{y}\in X^j} (x_1^{y_1}, \ldots, x_{j-1}^{y_{j-1}}, x_j^{y_j}, x_{j+1}, \ldots, x_n) \\
&= \phi_n^j(\mathbf{x})
\end{aligned}$$

by $j-1$ applications of Lemma 3.11. □

Lemma 3.17. *For* $1 \leq j < i \leq n$, $D_{n-1}^j \partial_i^0(\mathbf{x}) = \partial_{i+1}^0 D_n^j(\mathbf{x})$.

Proof.

$$\begin{aligned}
D_{n-1}^j \partial_i^0(\mathbf{x}) &= D_{n-1}^j(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \\
&= \sum_{\mathbf{y}\in X^j} (x_1^{y_1}, \ldots, x_{j-1}^{y_{j-1}}, x_j, y_j, x_{j+1}, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)
\end{aligned}$$

and

$$\begin{aligned}
\partial_{i+1}^0 D_n^j(\mathbf{x}) &= \partial_{i+1}^0 \left(\sum_{\mathbf{y}\in X^j} (x_1^{y_1}, \ldots, x_{j-1}^{y_{j-1}}, x_j, y_j, x_{j+1}, \ldots, x_n) \right) \\
&= \sum_{\mathbf{y}\in X^j} (x_1^{y_1}, \ldots, x_{j-1}^{y_{j-1}}, x_j, y_j, x_{j+1}, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n).
\end{aligned}$$

□

Lemma 3.18. *For* $1 \leq j < i \leq n$, $D_{n-1}^j \partial_i^1(\mathbf{x}) = \partial_{i+1}^1 D_n^j(\mathbf{x})$.

Proof.

$$\begin{aligned}
D_{n-1}^j \partial_i^1(\mathbf{x}) &= D_{n-1}^j(x_1^{x_i}, \ldots, x_{i-1}^{x_i}, x_{i+1}, \ldots, x_n) \\
&= \sum_{\mathbf{y}\in X^j} (x_1^{x_i y_1}, \ldots, x_{j-1}^{x_i y_{j-1}}, x_j^{x_i}, y_j, x_{j+1}^{x_i}, \ldots, x_{i-1}^{x_i}, x_{i+1}, \ldots, x_n) \\
&= \sum_{\mathbf{y}\in X^j} (x_1^{y_1}, \ldots, x_{j-1}^{y_{j-1}}, x_j^{x_i}, y_j, x_{j+1}^{x_i}, \ldots, x_{i-1}^{x_i}, x_{i+1}, \ldots, x_n)
\end{aligned}$$

and

$$\begin{aligned}\partial^1_{i+1} D^j_n(\mathbf{x}) &= \partial^1_{i+1}\left(\sum_{\mathbf{y}\in X^j}(x_1^{y_1},\ldots,x_{j-1}^{y_{j-1}},x_j,y_j,x_{j+1},\ldots,x_n)\right)\\ &= \sum_{\mathbf{y}\in X^j}(x_1^{y_1x_i},\ldots,x_{j-1}^{y_{j-1}x_i},x_j^{x_i},y_j^{x_i},x_{j+1}^{x_i},\ldots,x_{i-1}^{x_i},x_{i+1},\ldots,x_n),\\ &= \sum_{\mathbf{y}\in X^j}(x_1^{y_1},\ldots,x_{j-1}^{y_{j-1}},x_j^{x_i},y_j^{x_i},x_{j+1}^{x_i},\ldots,x_{i-1}^{x_i},x_{i+1},\ldots,x_n)\end{aligned}$$

by $j-1$ applications of Lemmas 3.11 and 3.12. But these sums agree as the set $\{\, y_j^{x_i} \mid y_j \in X \,\}$ is the image of $\{\, y_j \mid y_j \in X \,\}$ under the bijection f_{x_i}. □

Putting all this together, we have

Proposition 3.19. *For $j \geq 1$, $D^j : C^R_*(X) \to C^R_{*+1}(X)$ is a chain homotopy from ϕ^j to $|X|\phi^{j-1}$.*

Proof. We need to show that

$$\partial_{n+1} D^j_n(\mathbf{x}) + D^j_{n-1}\partial_n(\mathbf{x}) = \pm(\phi^j_n(\mathbf{x}) - |X|\phi^{j-1}_n(\mathbf{x})).$$

For $j > n$, we have $D^j_n = D^j_{n+1} = 0$, while

$$\phi^j_n(\mathbf{x}) = |X|^{j-n}\phi^n_n(\mathbf{x}) = |X|(|X|^{(j-1)-n}\phi^n_n(\mathbf{x})) = |X|\phi^{j-1}_n(\mathbf{x})$$

as required.

For $j = n$, we have $D^j_{n-1} = 0$ and

$$\begin{aligned}\partial_{n+1} D^j_n(\mathbf{x}) &= \sum_{i=1}^{n+1}(-1)^i(\partial^0_i D^n_n(\mathbf{x}) - \partial^1_i D^n_n(\mathbf{x}))\\ &= \sum_{i\leq n}(-1)^i(\partial^0_i D^n_n(\mathbf{x}) - \partial^1_i D^n_n(\mathbf{x}))\\ &\quad +(-1)^{n+1}(\partial^0_{n+1} D^n_n(\mathbf{x}) - \partial^1_{n+1} D^n_n(\mathbf{x})).\end{aligned}$$

By Lemma 3.13, the first sum adds to zero, and by Lemmas 3.15 and 3.16 we have

$$\partial_{n+1} D^j_n(\mathbf{x}) = (-1)^{n+1}(|X|\phi^{n-1}_n(\mathbf{x}) - \phi^n_n(\mathbf{x})),$$

as required.

For $j < n$,

$$\begin{aligned}
\partial_{n+1} D_n^j(\mathbf{x}) &= \sum_{i=1}^{n+1} (-1)^i (\partial_i^0 D_n^j(\mathbf{x}) - \partial_i^1 D_n^j(\mathbf{x})) \\
&= \sum_{i \leq n} (-1)^i (\partial_i^0 D_n^j(\mathbf{x}) - \partial_i^1 D_n^j(\mathbf{x})) \\
&\quad + (-1)^{j+1} (\partial_{n+1}^0 D_n^j(\mathbf{x}) - \partial_{n+1}^1 D_n^j(\mathbf{x})) \\
&\quad + \sum_{i=j+2}^{n+1} (-i)^i (\partial_i^0 D_n^j(\mathbf{x}) + \partial_i^1 D_n^j(\mathbf{x}))
\end{aligned}$$

which, by Lemmas 3.13, 3.15 and 3.16 as above yields

$$\partial_{n+1} D_n^j(\mathbf{x}) = (-1)^{j+1} (|X| \phi_n^{j-1}(\mathbf{x}) - \phi_n^j(\mathbf{x})) + \sum_{i=j+2}^{n+1} (-i)^i (\partial_i^0 D_n^j(\mathbf{x}) + \partial_i^1 D_n^j(\mathbf{x}))$$

Now,

$$\begin{aligned}
D_{n-1}^j \partial_n(\mathbf{x}) &= \sum_{i=1}^{n} (-1)^i (D_{n-1}^j \partial_i^0(\mathbf{x}) - D_{n-1}^j \partial_i^1(\mathbf{x})) \\
&= \sum_{i=1}^{j} (-1)^i (D_{n-1}^j \partial_i^0(\mathbf{x}) - D_{n-1}^j \partial_i^1(\mathbf{x})) \\
&\quad + \sum_{i=j+1}^{n} (-1)^i (D_{n-1}^j \partial_i^0(\mathbf{x}) - D_{n-1}^j \partial_i^1(\mathbf{x})).
\end{aligned}$$

The first sum is zero by Lemma 3.14, and applying Lemmas 3.17 and 3.18 we get

$$D_{n-1}^j \partial_n(\mathbf{x}) = \sum_{i=j+1}^{n} (-1)^i (\partial_{i+1}^0 D_n^j(\mathbf{x}) - \partial_{i+1}^1 D_n^j(\mathbf{x})).$$

Reindexing this sum by replacing $i+1$ with i', we have

$$D_{n-1}^j \partial_n(\mathbf{x}) = \sum_{i'=j+2}^{n+1} (-1)^{i'+1} (\partial_{i'}^0 D_n^j(\mathbf{x}) - \partial_{i'}^1 D_n^j(\mathbf{x})),$$

so that

$$\partial_{n+1} D_n^j(\mathbf{x}) + D_{n-1}^j \partial_n(\mathbf{x}) = (-1)^{j+1} (|X| \phi_n^{j-1}(\mathbf{x}) - \phi_n^j(\mathbf{x}))$$

as required. $\square$

Proof of Theorem 3.2. We deal first with the case $W = R$. There is a chain map $\pi^R\colon C_*(X) \to C_*(\mathcal{O}_X)$ induced by the projection of X onto its orbit rack. In Lemma 4.2 of [2], it is proved that for $\boldsymbol{\omega} = (\omega_1, \ldots, \omega_n) \in \mathcal{O}_X^n$, the element $\sum_{z_j \in \omega_j, j=1,\ldots,n} (z_1, \ldots, z_n)$ of $C_n^R(X)$ is a cycle. Since the boundary maps in $C_*(\mathcal{O}_X)$ are all zero, this means that we can define a chain map $\psi\colon C_*^R(\mathcal{O}_X) \to C_*^R(X)$ by setting

$$\psi_n(\boldsymbol{\omega}) = \left(\prod_{i=1}^{n} N_{\omega_i}\right) \sum_{z_j \in \omega_j, j=1,\ldots,n} (z_1, \ldots, z_n).$$

This is almost the same as the chain map used in the proof of Theorem 4.1 of [2].) Then, for $\mathbf{x} \in X^n$,

$$\begin{aligned}\psi_n \pi_n^R(\mathbf{x}) &= \left(\prod_{i=1}^{n} N_{\pi(x_i)}\right) \sum_{z_j \in \pi(x_j), j=1,\ldots,n} (z_1, \ldots, z_n) \\ &= \sum_{\mathbf{y} \in X^n} (x_1^{y_1}, \ldots, x_n^{y_n}) \\ &= \phi_n^n(\mathbf{x}).\end{aligned}$$

Hence, by Proposition 3.19, the induced map $\psi_* \pi_*^R\colon H_n^R(X) \to H_n^R(X)$ is multiplication by $|X|^n$. It follows, since $H_n^R(\mathcal{O}_X)$ is free abelian, that the torsion subgroup of $H_n^R(X)$ is equal to $\operatorname{Ker} \pi_*^R$ and is annihilated by $|X|^n$, and that $\beta_n^R(X) \leq \beta_n^R(\mathcal{O}_X)$. Since the reverse inequality was proved in [2], the proof in the case of rack homology is complete.

When X is a quandle, the other two cases follow from the case just proved, Theorem 3.4, and Theorem 4.1 of [2]. □

3.4 Computations

In [3] (Table 1), the cohomology groups $H_Q^n(X; \mathbb{Z}_p)$ of some Alexander racks are given for $n = 2$ or 3 and the first few primes p. These racks are of the form $\Lambda_n/(h)$, and the number m of orbits is easily computed from Proposition 3.1(b).

For $X = \Lambda_3/(t^2+t+1)$, $m = 3$, so according to Theorem 3.2, the dimension of $H^2_Q(X;\mathbb{Z}_p)$ should be 6 for $p \neq 3$, while the value in [3] is 3 in these cases. This led Dr. Litherland to write a C program to check the computations. Apart from $\Lambda_3/(t^2+t+1)$, where the recomputation gave the same values as for $\Lambda_9/(t-4)$, the results agreed with one exception, for $X = \Lambda_3/(t^2-t+1)$. Here [3] has $\dim H^2_Q(X;\mathbb{Z}_3) = 0$, while the recomputation yields $\dim H^2_Q(X;\mathbb{Z}_3) = 1$. The value 1 is in agreement with Corollary 2.4 of [13]. It turns out that the disagreement is due to typographical errors in [3], and the values just given are the ones computed by Carter et al.

A variant of this program computes the integral homology of racks; we present in Table 1 the results of some calculations. In view of Theorem 3.7, we give only the quandle homology, though the program has been run to compute rack homology with the results expected from Theorem 3.7. As in [3], the racks considered are non-trivial, of order at most 9, and of the form $\Lambda_n/(h)$ where h is a monic polynomial whose constant term is a unit in $\mathbb{Z}_n$. The list of racks is different from that in [3] in two ways. First, we have included $\Lambda_3/(t^2-t-1)$ and $\Lambda_2/(t^3+t^2+t+1)$. Second, it turns out that $R_4 \simeq \Lambda_2/(t^2+1)$, $\Lambda_9/(t-4) \simeq \Lambda_9/(t-7) \simeq \Lambda_3/(t^2+t+1)$, and $R_8 \simeq \Lambda_8/(t-3)$ (where $\simeq$ denotes rack-isomorphism), and we have omitted all but the first of each isomorphism class. That $R_4 \simeq \Lambda_2/(t^2+1)$ and $\Lambda_9/(t-4) \simeq \Lambda_9/(t-7)$ was noted in [3]. The other isomorphisms were discovered by a brute-force computation. The existence of all these isomorphisms follows from the next two propositions.

Proposition 3.20. *If k is coprime to n then $\Lambda_{n^2}/(t-(kn+1)) \simeq \Lambda_n/((t-1)^2)$.*

TABLE 3.1. Some quandle homology groups.

X	$H_2^Q(X)$	$H_3^Q(X)$
R_3	0	$\mathbb{Z}_3$
R_4	$\mathbb{Z}^2 \oplus \mathbb{Z}_2^2$	$\mathbb{Z}^2 \oplus \mathbb{Z}_2^4$
R_5	0	$\mathbb{Z}_5$
R_6	$\mathbb{Z}^2$	$\mathbb{Z}^2 \oplus \mathbb{Z}_3^2$
R_7	0	$\mathbb{Z}_7$
R_8	$\mathbb{Z}^2 \oplus \mathbb{Z}_2^2$	$\mathbb{Z}^2 \oplus \mathbb{Z}_2^2 \oplus \mathbb{Z}_8^2$
R_9	0	$\mathbb{Z}_9$
$\Lambda_5/(t-2)$	0	0
$\Lambda_5/(t-3)$	0	0
$\Lambda_7/(t-2)$	0	0
$\Lambda_7/(t-3)$	0	0
$\Lambda_7/(t-4)$	0	0
$\Lambda_7/(t-5)$	0	0
$\Lambda_8/(t-5)$	$\mathbb{Z}^{12} \oplus \mathbb{Z}_2^4$	$\mathbb{Z}^{36} \oplus \mathbb{Z}_2^{24}$
$\Lambda_9/(t-2)$	0	$\mathbb{Z}_3$
$\Lambda_9/(t-4)$	$\mathbb{Z}^6 \oplus \mathbb{Z}_3^3$	$\mathbb{Z}^{12} \oplus \mathbb{Z}_3^{12}$
$\Lambda_9/(t-5)$	0	$\mathbb{Z}_3$
$\Lambda_2/(t^2+t+1)$	$\mathbb{Z}_2$	$\mathbb{Z}_2 \oplus \mathbb{Z}_4$
$\Lambda_3/(t^2+1)$	$\mathbb{Z}_3$	$\mathbb{Z}_3^3$
$\Lambda_3/(t^2-1)$	$\mathbb{Z}^6$	$\mathbb{Z}^{12} \oplus \mathbb{Z}_3^3$
$\Lambda_3/(t^2-t+1)$	$\mathbb{Z}_3$	$\mathbb{Z}_3 \oplus \mathbb{Z}_9$
$\Lambda_3/(t^2+t-1)$	0	0
$\Lambda_3/(t^2-t-1)$	0	0
$\Lambda_2/(t^3+1)$	$\mathbb{Z}^2 \oplus \mathbb{Z}_2^2$	$\mathbb{Z}^2 \oplus \mathbb{Z}_2^6 \oplus \mathbb{Z}_4^2$
$\Lambda_2/(t^3+t^2+1)$	0	$\mathbb{Z}_2$
$\Lambda_2/(t^3+t+1)$	0	$\mathbb{Z}_2$
$\Lambda_2/(t^3+t^2+t+1)$	$\mathbb{Z}^2 \oplus \mathbb{Z}_2^4$	$\mathbb{Z}^2 \oplus \mathbb{Z}_2^8 \oplus \mathbb{Z}_8^2$

Proof. We identify $\Lambda_{n^2}/(t-(kn+1))$ with $\mathbb{Z}_{n^2}$ under the operation $a^b = (kn+1)a - knb$. There is a short exact sequence of abelian groups

$$0 \to \mathbb{Z}_n \xrightarrow{\alpha} \mathbb{Z}_{n^2} \xrightarrow{\beta} \mathbb{Z}_n \to 0,$$

where $\alpha(1) = n$ and $\beta(1) = 1$. Note that for $a \in \mathbb{Z}_{n^2}$, $\alpha^{-1}(na) = \beta(a)$. Let $\gamma\colon \mathbb{Z}_n \to \mathbb{Z}_{n^2}$ be a function such that $\beta\gamma = \mathrm{id}$, and define $\delta\colon \mathbb{Z}_{n^2} \to \mathbb{Z}_n$ by $\delta(a) = \alpha^{-1}(a - \gamma\beta(a))$. The function $\mathbb{Z}_{n^2} \to \mathbb{Z}_n^2$ sending a to $(\beta(a), \delta(a))$ is a bijection. Now define $f\colon \mathbb{Z}_{n^2} \to \Lambda_n/((t-1)^2)$ by $f(a) = k\beta(a) + (t-1)\delta(a)$; because k is coprime to n, f is also a bijection. We have, for $a, b \in \mathbb{Z}_{n^2}$, $\beta(a^b) = \beta(a)$ and

$$\begin{aligned} \delta(a^b) &= \alpha^{-1}((kn+1)a - knb - \gamma\beta(a)) \\ &= \alpha^{-1}(kna) - \alpha^{-1}(knb) + \alpha^{-1}(a - \gamma\beta(a)) \\ &= k\beta(a) - k\beta(b) + \delta(a). \end{aligned}$$

Hence

$$\begin{aligned} f(a^b) &= k\beta(a) + (t-1)(k\beta(a) - k\beta(b) + \delta(a)) \\ &= kt\beta(a) + (t-1)\delta(a) + k(1-t)\beta(b) \end{aligned}$$

On the other hand,

$$\begin{aligned} f(a)^{f(b)} &= t(k\beta(a) + (t-1)\delta(a)) + (1-t)(k\beta(b) + (t-1)\delta(b)) \\ &= kt\beta(a) + (t-1)\delta(a) + k(1-t)\beta(b), \end{aligned}$$

so f is the desired isomorphism. □

Proposition 3.21. *If n is divisible by 4 then $R_{2n} \simeq \Lambda_{2n}/(t-(n-1))$.*

Proof. Here the underlying sets of both racks are naturally identified with $\mathbb{Z}_{2n}$. We use a^b for the rack operation in R_{2n}, and $a^{[b]}$ for that in $\Lambda_{2n}/(t-(n-1))$. Thus, for $a, b \in \mathbb{Z}_{2n}$,

$$\begin{aligned} a^b &= 2b - a \\ \text{and} \qquad a^{[b]} &= (n-1)a + (2-n)b. \end{aligned}$$

Define functions ϵ and f from $\mathbb{Z}_{2n}$ to itself by

$$\epsilon(a) = \begin{cases} 0, & \text{if } a \equiv 0 \text{ or } 1 \pmod 4; \\ n, & \text{if } a \equiv 2 \text{ or } 3 \pmod 4; \end{cases}$$

and $f(a) = a + \epsilon(a)$. Since $f(a) \equiv a \pmod 4$, f is an involution. Since $a^b \equiv a \pmod 2$, we have that $\epsilon(a^b) = \epsilon(a)$ iff $a^b \equiv a \pmod 4$, which in turn is equivalent to $a \equiv b \pmod 2$. Since ϵ only takes on the values 0 and n, this implies that $\epsilon(a^b) = \epsilon(a) + n(a-b)$. Hence

$$\begin{aligned} f(a^b) &= 2b - a + \epsilon(a) + n(a-b) \\ &= (n-1)a + \epsilon(a) + (2-n)b. \end{aligned}$$

On the other hand,

$$\begin{aligned} f(a)^{[f(b)]} &= (n-1)(a + \epsilon(a)) + (2-n)(b + \epsilon(b)) \\ &= (n-1)a + \epsilon(a) + (2-n)b, \end{aligned}$$

so f is the desired isomorphism. □

Chapter 4

Classification of Finite Alexander Quandles

4.1 Introduction

Recall that a *quandle* is a set X with a binary operation written as exponentiation satisfying

(i) For every $a, b \in X$ there exists a unique $c \in X$ such that $a = c^b$,

(ii) For every $a, b, c \in X$ we have $a^{bc} = a^{cb^c}$, and

(iii) For every $a \in X$ we have $a^a = a$.

Any module over $\Lambda = \mathbb{Z}[t^{\pm 1}]$ is a quandle under the operation $a^b = ta + (1-t)b$. Quandles of this form are called *Alexander quandles.* To obtain finite Alexander quandles, we typically consider $\Lambda_n/(h)$ where $\Lambda_n = \mathbb{Z}_n[t^{\pm 1}]$ and h is a monic polynomial in t. In an earlier version of [14], the open questions list included when two Alexander quandles of the form $\Lambda_n/(t-a)$ with $\gcd(n, a) = 1$ (we call Alexander quandles of this form *linear*) are isomorphic and when two linear quandles are dual.

To answer these questions, we first consider the general case of when two arbitrary Alexander quandles of finite cardinality are isomorphic. We obtain a result which reduces the problem of comparing Alexander quandles to comparing certain Λ-submodules. We then apply this result to obtain a pair of simple conditions on a and b which are necessary and sufficient for two linear Alexander quandles $\Lambda_n/(t-a)$ and $\Lambda_n/(t-b)$ to be isomorphic.

In the course of answering the question of classifying linear quandles, we also answer the question of when linear quandles are dual and we obtain results on when Alexander quandles are connected.

4.2 Alexander Quandles and Λ-Modules

Since the quandle structure of an Alexander quandle is determined by its Λ-module structure, any isomorphism of Λ-modules is also an isomorphism of Alexander quandles. The converse is not true, however: $\Lambda_9/(t-4)$ is isomorphic to $\Lambda_9/(t-7)$ as an Alexander quandle but not as a Λ-module.

Nonetheless, an isomorphism of Alexander quandles is in a sense almost an isomorphism of Λ-modules; in fact, (after applying a shift if necessary) its restriction to the submodule $(1-t)M$ is a Λ-module isomorphism onto its image. Theorem 4.1 says that we can determine whether two Alexander quandles of the same finite cardinality are isomorphic simply by comparing these Λ-submodules. This reduces the problem of classifying finite Alexander quandles to classifying Λ-modules of the form $(1-t)M$.

Theorem 4.1. *Two finite Alexander quandles M and N of the same cardinality are isomorphic iff there is an isomorphism $h : (1-t)M \to (1-t)N$ of Λ-modules.*

Proof. Let $f : M \to N$ be an isomorphism of Alexander quandles. We may assume without loss of generality that $f(0) = 0$ since $f' : M \to N$ defined by $f'(x) = f(x) + c$ is also an isomorphism of Alexander quandles for any $c \in N$. Then $f(tx + (1-t)y) = tf(x) + (1-t)f(y)$ implies

$$f(tx) = f(tx + (1-t)0) = tf(x) + (1-t)f(0) = tf(x)$$

and

$$f((1-t)y) = f(t0 + (1-t)y) = tf(0) + (1-t)f(y) = (1-t)f(y)$$

so that

$$f(tx + (1-t)y) = f(tx) + f((1-t)y) \tag{4.1}$$

Denote $M' = (1-t)M$ and $N' = (1-t)N$. Since $t^{-1} \in \Lambda$, every element of M is tx for some $x \in M$, and since $f(0) = 0$, f takes the coset $0 + M'$ of M' in $\bar{M} = M/M'$ to the coset $0 + N'$ of N' in $\bar{N} = N/N'$, so we have that $h = f|_{M'} : M' \to N'$ is a homomorphism of Λ-modules. Since f is injective, its restriction h is a bijection onto its image $0 + N' = N'$, and hence h is an isomorphism of Λ-modules.

Conversely, suppose $h : M' \to N'$ is an isomorphism of finite Λ-modules with $|M| = |N|$. Let $A \subset M$ be a set of representatives of cosets of M' in $\bar{M}$. Then every $m \in M$ has the form $m = \alpha + \omega$ for a unique $\alpha \in A$ and $\omega \in M'$. We will show that there exists a bijection $k : A \to B$ onto a set B of representatives of cosets of N' in $\bar{N}$ such that the map $f : M \to N$ defined by

$$f(\alpha + \omega) = k(\alpha) + h(\omega)$$

is an isomorphism of Alexander quandles (though typically not of Λ-modules).

Note that for any $\alpha_1 \in M$ we have $t\alpha_1 = \alpha_1 - (1-t)\alpha_1$, so that

$$\begin{aligned}
&f(t(\alpha_1 + \omega_1) + (1-t)(\alpha_2 + \omega_2)) \\
&\quad = f(\alpha_1 + t\omega_1 + (1-t)(\alpha_2 - \alpha_1 + \omega_2)) \\
&\quad = k(\alpha_1) + h(t\omega_1 + (1-t)(\alpha_2 - \alpha_1 + \omega_2)) \\
&\quad = k(\alpha_1) + th(\omega_1) + h((1-t)\alpha_2) \\
&\qquad\quad - h((1-t)\alpha_1) + (1-t)h(\omega_2).
\end{aligned}$$

On the other hand,

$$\begin{aligned} tf(\alpha_1 + \omega_1) + (1-t)f(\alpha_2 + \omega_2) \\ &= t(k(\alpha_1) + h(t(\omega_1))) + (1-t)(k(\alpha_2) + h(\omega_2)) \\ &= tk(\alpha_1) + th(\omega_1) + (1-t)k(\alpha_2) + (1-t)h(\omega_2) \end{aligned}$$

so for f to be a homomorphism of quandles we must have that

$$(1-t)k(\alpha_1) - h((1-t)\alpha_1) = (1-t)k(\alpha_2) - h((1-t)\alpha_2) \qquad (4.2)$$

for all $\alpha_1, \alpha_2 \in A$. We will show that given a set of coset representatives $A \subset M$ we can choose a set $B \subset N$ of coset representatives and a bijection $k : A \to B$ so that $(1-t)k(\alpha) = h((1-t)\alpha)$ for all $\alpha \in A$, which satisfies (4.2) and thus yields a homomorphism $f : M \to N$ of Alexander quandles. Since this f is setwise the Cartesian product $k \times h$ of the bijections $k : A \to B$ and $h : M' \to N'$, f is bijective and hence an isomorphism of quandles.

Denote $M'' = (1-t)^2 M$, $\bar{\bar{M}} = M'/M''$ and similarly for N. The isomorphism $h : M' \to N'$ induces an isomorphism $\bar{h} : \bar{\bar{M}} \to \bar{\bar{N}}$. There are surjective maps $\psi : \bar{M} \to \bar{\bar{M}}$ and $\phi : \bar{N} \to \bar{\bar{N}}$ induced by multiplication by $(1-t)$. Then $|M'| = |N'|$ and $|M| = |N|$ imply that $|\bar{M}| = |\bar{N}|$, and in turn $|\bar{\bar{M}}| = |\bar{\bar{N}}|$. Hence $|\psi^{-1}(y)| = [\bar{M} : \bar{\bar{M}}] = [\bar{N} : \bar{\bar{N}}] = |\phi^{-1}(\bar{h}(y))|$ for all $y \in \bar{\bar{M}}$ since $\psi^{-1}(y)$ and $\phi^{-1}(h(y))$ are cosets of isomorphic submodules in $\bar{M}$ and $\bar{N}$. Thus there is a bijection of sets $g : \bar{M} \to \bar{N}$ such that the diagram

$$\begin{array}{ccccc} & \bar{M} & \xrightarrow{g} & \bar{N} & \\ \psi & \downarrow & & \downarrow & \phi \\ & \bar{\bar{M}} & \xrightarrow{\bar{h}} & \bar{\bar{N}} & \end{array}$$

commutes.

Let B be a set of coset representatives for $\bar{N}$. Then there is a unique bijection $k : A \to B$ such that

$$\begin{array}{ccccc} & A & \xrightarrow{k} & B & \\ & \downarrow & & \downarrow & \\ & \bar{M} & \xrightarrow{g} & \bar{N} & \\ \psi & \downarrow & & \downarrow & \phi \\ & \bar{\bar{M}} & \xrightarrow{\bar{h}} & \bar{\bar{N}} & \end{array}$$

commutes. In particular, we have

$$\bar{h}((1-t)\alpha + (1-t)^2 M) = \bar{h}\psi(\alpha) = \phi k(\alpha) = (1-t)k(\alpha) + (1-t)^2 N. \qquad (4.3)$$

Define $\gamma : M' \to \bar{M}$ and $\epsilon : N' \to \bar{N}$ by $\gamma((1-t)m) = (1-t)m + (1-t)^2 M \in \bar{M}$ and $\epsilon((1-t)n) = (1-t)n + (1-t)^2 N \in \bar{N}$, the classes of $(1-t)m$ and $(1-t)n$ in $\bar{\bar{M}}$ and $\bar{\bar{N}}$ respectively. We then have commutative diagrams

$$\begin{array}{cccc} A & \xrightarrow{(1-t)} & M' & \\ \downarrow & & \downarrow & \gamma \\ \bar{M} & \xrightarrow{\psi} & \bar{\bar{M}} & \end{array} \quad \text{and} \quad \begin{array}{cccc} B & \xrightarrow{(1-t)} & N' & \\ \downarrow & & \downarrow & \epsilon \\ \bar{N} & \xrightarrow{\phi} & \bar{\bar{N}}. & \end{array}$$

Equation (4.3) then says that outside rectangle of the diagram

$$\begin{array}{ccccc} & A & \xrightarrow{k} & B & \\ (1-t) & \downarrow & & \downarrow & (1-t) \\ & M' & \xrightarrow{h} & N' & \\ \gamma & \downarrow & & \downarrow & \epsilon \\ & \bar{\bar{M}} & \xrightarrow{\bar{h}} & \bar{\bar{N}} & \end{array}$$

commutes. The bottom square commutes by definition of $\bar{h}$, and thus we have $\epsilon(h((1-t)\alpha)) = \epsilon((1-t)k(\alpha))$, that is,

$$h((1-t)\alpha) + (1-t)^2 N = (1-t)k(\alpha) + (1-t)^2 N.$$

In particular, there is a $\xi \in N$ so that

$$h((1-t)\alpha) = (1-t)k(\alpha) + (1-t)^2\xi = (1-t)(k(\alpha) + (1-t)\xi).$$

Then for each $\alpha \in A$ with $\xi \neq 0$ we may replace $k(\alpha)$ with the coset representative $k'(\alpha) = k(\alpha) + (1-t)\xi$ to obtain a new set B' of coset representatives for $\bar{N}$ and a bijection $k' : A \to B'$ with $(1-t)k'(\alpha) = h((1-t)\alpha)$ so that (4.2) is satisfied. Then $f : M \to N$ by $f(\alpha + \omega) = k'(\alpha) + h(\omega)$ for all $\alpha \in A$ is an isomorphism of Alexander quandles, as required. □

As a consequence, we obtain corollary 4.2, which gives specific conditions on a and b for $\Lambda_n/(t-a) \cong \Lambda_n/(t-b)$ when a and b are coprime to n. Note that the case where a and b are not coprime to n reduces to this case.

Denote $n_a = \frac{n}{\gcd(n, 1-a)}$ for any $a \in \mathbb{Z}_n$.

Corollary 4.2. *Let a and b be coprime to n. Then the Alexander quandles $\Lambda_n/(t-a)$ and $\Lambda_n/(t-b)$ are isomorphic iff $n_a = n_b$ and $a \equiv b (\text{mod } n_a)$.*

Proof. By theorem 4.1,

$$\Lambda_n/(t-a) \cong \Lambda_n/(t-b) \iff (1-t)[\Lambda_n/(t-a)] \cong (1-t)[\Lambda_n/(t-b)]$$

where the isomorphism on the left is an isomorphism of Alexander quandles and the one on the right is of Λ-modules. As a $\mathbb{Z}$-module, $(1-t)[\Lambda_n/(t-a)]$ is $(1-a)\mathbb{Z}_n$ and $(1-t)[\Lambda_n/(t-b)]$ is $(1-b)\mathbb{Z}_n$ with the action of t given by multiplication by a in $(1-a)\mathbb{Z}_n$ and by b in $(1-b)\mathbb{Z}_n$.

The $\mathbb{Z}$-module $(1-a)\mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_n/\mathrm{Ann}(1-a)$, so as $\mathbb{Z}$-modules

$$\begin{aligned}\Lambda_n/(t-a) \cong \Lambda_n/(t-b) &\iff \mathbb{Z}_n/\mathrm{Ann}(1-a) \cong \mathbb{Z}_n/\mathrm{Ann}(1-b)\\ &\iff \mathrm{Ann}(1-a) = \mathrm{Ann}(1-b)\\ &\iff \mathrm{Ord}_{\mathbb{Z}_n}(1-a) = \mathrm{Ord}_{\mathbb{Z}_n}(1-b)\\ &\iff \frac{n}{gcd(n,1-a)} = \frac{n}{gcd(n,1-b)}\\ &\iff n_a = n_b.\end{aligned}$$

Denote $n' = n_a = n_b$. Then $(1-t)[\Lambda_n/(t-a)]$ is $\mathbb{Z}_{n'}$ with t acting by multiplication by a, and if $n_a = n_b = n'$ then $(1-t)[\Lambda_n/(t-b)]$ is $\mathbb{Z}_{n'}$ with t acting by multiplication by b.

Multiplication by a agrees with multiplication by b on $\mathbb{Z}_{n'}$ iff $a \equiv b(\mathrm{mod}\ n')$, so the Λ-module structures on $\mathbb{Z}_{n'}$ determined by a and b agree iff $a \equiv b(\mathrm{mod}\ n')$. $\square$

An Alexander quandle is said to be *connected* if it has only one orbit, that is, if $M' = M$.

Corollary 4.3. *Two finite connected Alexander modules are isomorphic iff they are isomorphic as* Λ*-modules.*

Proof. This follows from the proof of theorem 4.1. Specifically, if M and N are connected and $f : M \to N$ is an isomorphism of quandles with $f(0) = 0$, then f is an isomorphism of Λ-modules. $\square$

Corollary 4.4. *A linear Alexander quandle* $\Lambda_n/(t-a)$ *is connected iff* $\gcd(n, 1-a) = 1$.

Proof. An Alexander quandle is connected iff $M = (1-t)M$. Since $(1-t)[\Lambda_n/(t-a)]$ is $\mathbb{Z}_{n_a}$ with t acting by multiplication by a, we have $\Lambda_n/(t-a)$ is connected iff $n_a = n$, that is, iff $\gcd(n, 1-a) = 1$. $\square$

Corollary 4.5. *No linear Alexander quandle $\Lambda_n/(t-a)$ with n even is connected.*

Proof. For $\Lambda_n/(t-a)$ to be a linear quandle with n elements, we must have $\gcd(n,a) = 1$, so if n is even, a must be odd. But then $1-a$ is even and $\gcd(n, 1-a) \neq 1$, and $\Lambda_n/(t-a)$ is not connected. □

For each $y \in X$ we can define a map of sets $f_y : X \to X$ by $f_y(x) = x^y$. Quandle axiom (i) then says that f_y is a bijection for each $y \in X$. We may then define a new quandle structure on X by $x^{\bar{y}} = f_y^{-1}(x)$; this is the *dual* quandle of X.

Lemma 4.6. *The dual of an Alexander quandle X is the set X with quandle operation given by $x^{\bar{y}} = t^{-1}x + (1-t^{-1})y$.*

Proof. If $f_y(x) = c = tx+(1-t)y$ then $t^{-1}c = x+(t^{-1}-1)y \Rightarrow x = t^{-1}c+(1-t^{-1})y$; thus $f_y^{-1}(x) = t^{-1}x + (1-t^{-1})y$. □

Corollary 4.7. *Let a, b be coprime to n. Then $\Lambda_n/(t-a)$ is dual to $\Lambda_n/(t-b)$ iff $n_a = n_b$ and $ab \equiv 1 (\mathrm{mod}\ n_a)$. In particular, a linear Alexander quandle $\Lambda_n/(t-a)$ is self-dual iff a is a square mod n_a.*

Proof. If n and a are coprime, then a is invertible in $\mathbb{Z}_n$ and the dual of $\Lambda_n/(t-a)$ is given by $\Lambda_n/(t-a^{-1})$ by lemma 4.6. Then corollary 4.2 says that $\Lambda_n/(t-b)$ is isomorphic to $\Lambda_n/(t-a^{-1})$ iff $n_b = n_{a^{-1}}$ and $b \equiv a^{-1} (\mathrm{mod}\ n_b)$.

Since $\gcd(n,a) = 1$ we have $\gcd(n, 1-a) = \gcd(n, -a(1-a^{-1})) = \gcd(n, 1-a^{-1})$ so that $n_a = n_{a^{-1}}$ as required. □

4.3 $\mathbb{Z}$-Automorphisms and Computations

Let X be a finite Alexander quandle and let X_A denote X regarded as an Abelian group. The map $\phi : X_A \to X_A$ defined by $\phi(x) = tx$ is a homomorphism of $\mathbb{Z}$-modules. Since $t^{-1} \in \Lambda$, the map $\psi : X_A \to X_A$ by $\psi(x) = t^{-1}x$ is a two-sided inverse for ϕ as $\psi(\phi(x)) = t^{-1}tx = x$ and $\phi(\psi(x)) = tt^{-1}x = x$, and ϕ is in fact a $\mathbb{Z}$-automorphism.

Conversely, if A is a finite Abelian group and $\phi : A \to A$ is a $\mathbb{Z}$-module automorphism, we can give A the structure of an Alexander quandle by defining $tx = \phi(x)$. This yields a general strategy for listing all finite Alexander quandles of a given size n: first, list all Abelian groups A of order n; then, for each element of $\mathrm{Aut}_{\mathbb{Z}}(A)$ find $(1-t)A = \mathrm{Im}(1-\phi)$ and compare these as Λ-modules. In practice, for low order (i.e., $|A| \leq 15$) Alexander quandles this procedure in its full generality is necessary only for one case, namely Alexander quandles with underlying Abelian group isomorphic to $\mathbb{Z}_4 \oplus \mathbb{Z}_2$. We shall see that Alexander quandles with $X_A \cong \mathbb{Z}_4 \oplus \mathbb{Z}_2$ are isomorphic to linear Alexander quandles (in six cases) or to Alexander quandles with underlying group $(\mathbb{Z}_2)^3$ (in two cases).

We first obtain a few simplifying results:

Lemma 4.8. *If the underlying Abelian group X_A of X is cyclic, then X is linear.*

Proof. Suppose $X_A = \mathbb{Z}_n$. Then for any $x \in \mathbb{Z}_n$ and any $\phi \in \mathrm{Aut}_{\mathbb{Z}}(\mathbb{Z}_n)$, we must have $\phi(x) = \phi(x \cdot 1) = x\phi(1)$, so the action of t agrees with multiplication by $a = \phi(1)$ on $\mathbb{Z}_n$. Further, we must have $\gcd(n, a) = 1$ since ϕ is surjective. Hence X is $\mathbb{Z}_n$ with t acting by multiplication by a, that is, $X \cong \Lambda_n/(t-a)$. □

Remark 4.9. *Lemma 4.8 was also noted in [14].*

Corollary 4.10. *For any prime p, there are exactly $p-1$ distinct Alexander quandles with p elements, namely $\Lambda_p/(t-a)$ for $a = 1, \ldots, p-1$. Further, every Alexander quandle of prime order is either trivial ($\Lambda_p/(t-1) \cong T_p$, the trivial quandle of p elements) or connected.*

Proof. If p is prime, $n_a = \frac{n}{\gcd(p,1-a)} = 1$ for each $a \in 1, \ldots, p-1$. Then by corollary 4.2, these are all distinct. By lemma 4.8, every quandle of order p is linear, so these are all of the Alexander quandles of order p.

Since $\gcd(p, 1-a) = 1$ for $a = 2, \ldots, p-1$, corollary 4.4 gives us that $\Lambda_p/(t-a)$ is connected. □

Corollary 4.11. *Let $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$ be a product of powers of distinct primes. Then there are exactly $N_{p_1} N_{p_2} \ldots N_{p_k}$ distinct Alexander quandles of order n, where N_{p_i} is the number of distinct Alexander quandles of order ${p_i}^{e_i}$.*

Proof. Since any $\mathbb{Z}$-automorphism must respect order, every Alexander quandle structure on a direct sum of Abelian groups $A_{p_1^{e_1}} \oplus \cdots \oplus A_{p_k^{e_k}}$ with order $p_1^{e_1}, \ldots, p_k^{e_k}$ must respect this direct sum structure. Hence we may obtain a complete list of Alexander quandles of order n by listing all direct sums of Alexander quandles of orders $p_1^{e_1}, \ldots, p_k^{e_k}$. □

Corollary 4.12. *If the order of an Alexander quandle $n \equiv 2 (\mathrm{mod}\ 4)$, the quandle is not connected.*

Proof. If $n \equiv 2 (\mathrm{mod}\ 4)$, then the underlying Abelian group of the quandle has a summand of $\mathbb{Z}_2$. Hence the quandle has a summand isomorphic to $\Lambda_2/(t+1) \cong T_2$, and therefore is not connected. □

In light of corollary 4.11, to classify finite Alexander quandles it is sufficient to consider Alexander quandles of prime power order. Alexander quandles with prime order are cyclic as Abelian groups and hence are linear quandles, and so are classified by corollary 4.10. Alexander quandles with order a product of distinct primes are classified by corollary 4.11.

If the underlying Abelian group of X is $(\mathbb{Z}_p)^n$, then X is not only a Λ-module but also a Λ_p-module, so we may use the classification theorem for finitely generated modules over a PID. Thus any Alexander quandle X with $X_A = (\mathbb{Z}_p)^n$ must be of the form $\Lambda_p/(h_1) \oplus \cdots \oplus \Lambda_p/(h_k)$ with $h_1|h_2|\ldots|h_k$, $h_i \in \Lambda_p$ and $\sum \deg(h_i) = n$. We may further assume without loss of generality that each $h_i \in \mathbb{Z}_p[t]$, is monic, and has nonzero constant term.

Proposition 4.13. *$M = \Lambda/(h)$ is connected iff $(1-t) \nmid h$.*

Proof. Since M is finite, $(1-t)M = M$ iff $(1-t) : M \to M$ is bijective. If $(1-t)|h$ then $h = (1-t)g$ for some nonzero $g \in M$, and hence $\ker(1-t) \neq \{0\}$, so $(1-t)$ fails to be injective.

Conversely, $(1-t)$ is prime in Λ, so $(1-t)$ coprime to h implies that every $l \in \Lambda$ is $a(1-t) + bh$ for some $a, b \in \Lambda$. Hence every $m \in M$ is $a(1-t)$ for some $a \in M$. $\square$

Proposition 4.14. *$\Lambda_{p^n}/\left(t^n + \sum_{i=0}^{n-1} a_i t^i\right)$ is connected iff $\sum_{i=0}^{n-1} a_i = -1$.*

Proof. By 4.13, $\Lambda_{p^n}/(t^n + \sum_{i=0}^{n-1} a_i t^i)$ is connected iff $t-1|t^n + \sum_{i=0}^{n-1} a_i t^i$. That is, $\Lambda_{p^n}/(t^n + \sum_{i=0}^{n-1} a_i t^i)$ is connected iff there are $b_i \in \Lambda_p$, $0 \leq i \leq n-2$ such that

$$(t-1)\left(t^{n-1} + \sum_{i=0}^{n-2} b_i t^i\right) = t^n + \sum_{i=0}^{n-1} a_i t^i.$$

Comparing coefficients, we must have that $a_{n-1} + b_{n-2} = -1$, $b_i = a_i + b_{i-1}$ for all $1 \leq i \leq n-2$, and $b_0 = a_0$. Then $\sum_{i=0}^{n-1} a_i = -1$. $\square$

Proposition 4.15. *There are $2p^2 - 3p - 1$ connected Alexander quandles of order p^2 where p is prime.*[1]

[1] This agrees with the result of Graña in [7].

Proof. Every Alexander quandle of order p^2 has Abelian group $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \oplus \mathbb{Z}_p$. A linear quandle $\Lambda_{p^2}/(t-a)$ of order p^2 is connected iff $\gcd(1-a,p)=1$, and there are $p(p-2)$ such quandles.

An Alexander quandle M with underlying Abelian group $\mathbb{Z}_p \oplus \mathbb{Z}_p$ is a module over the PID Λ_p, so we have either $M \equiv \Lambda_p/(t-a) \oplus \Lambda_p/(t-a)$ or $M \equiv \Lambda_p/(t^2+at+b)$ where $b \neq 0$. There are $p-2$ connected quandles of the first type and $(p-1)^2$ of the second type, so in total there are $2p^2-3p-1$ connected Alexander quandles of order p^2. $\square$

For arbitrary values of n and p we may classify Alexander quandles with underlying abelian group $(\mathbb{Z}_p)^n$ by listing all possible Λ-modules with underlying group $(\mathbb{Z}_p)^n$ and comparing the submodules $\mathrm{Im}(1-t)$.

The results of applying this procedure to Alexander quandles with underlying Abelian group $(\mathbb{Z}_2)^2$, $(\mathbb{Z}_2)^3$ and $(\mathbb{Z}_2)^2$ are collected in table 1. As we expect, these results agree with proposition 4.15.

Note that by theorem 4.1 and corollary 4.2, the results in table 1 show that $\Lambda_2/(t^2+1) \cong \Lambda_4/(t-3)$ and $(\Lambda_2/(t+1))^2 \cong \Lambda_4/(t-1) \cong T_4$, the trivial quandle of order 4, while $\Lambda_2/(t^2+t+1)$ is the only connected Alexander quandle of order 4.

Alexander quandles with underlying Abelian group $(\mathbb{Z}_2)^3$ include $\Lambda_2/(t+1) \oplus \Lambda_2/(t^2+1) \cong \Lambda_8/(t-5)$ and $(\Lambda_2/(t+1))^3 \cong T_8$. Also, theorem 4.1 yields an isomorphism $\Lambda_8/(t-3) \cong \Lambda_8/(t-7)$; otherwise, the order eight quandles listed are all distinct. Of these, only $\Lambda_2/(t^3+t^2+1)$ and $\Lambda_2/(t^3+t+1)$ are connected. Note that none of the linear Alexander quandles of order eight are connected.

For Alexander quandles with Abelian group $(\mathbb{Z}_3)^2$, we have $\Lambda_9/(t-4) \cong \Lambda_9/(t-7) \cong \Lambda_9/(t^2+t+1)$ (the first isomorphism was noted by J.S. Carter et. al. in [3]

TABLE 4.1. Computations of $\mathrm{Im}(1-t)$ for $(\mathbb{Z}_2)^2$, $(\mathbb{Z}_2)^3$ and $(\mathbb{Z}_3)^2$.

X_A	Module	$\mathrm{Im}(1-t)$
$(\mathbb{Z}_2)^2$	$(\Lambda_2/(t+1))^2$	0
	$\Lambda_2/(t^2+1)$	$\Lambda_2/(t+1)$
	$\Lambda_2/(t^2+t+1)$	$\Lambda_2/(t^2+t+1)$
$(\mathbb{Z}_2)^3$	$(\Lambda_2/(t+1))^3$	0
	$\Lambda_2/(t+1)\oplus\Lambda_2/(t^2+1)$	$\Lambda_2/(t+1)$
	$\Lambda_2/(t^3+1)$	$\Lambda_2/(t^2+t+1)$
	$\Lambda_2/(t^3+t+1)$	$\Lambda_2/(t^3+t+1)$
	$\Lambda_2/(t^3+t^2+1)$	$\Lambda_2/(t^3+t^2+1)$
	$\Lambda_2/(t^3+t^2+t+1)$	$\Lambda_2/(t^2+1)$
$(\mathbb{Z}_3)^2$	$(\Lambda_3/(t+2))^2$	0
	$(\Lambda_3/(t+1))^2$	$(\Lambda_3/(t+1))^2$
	$\Lambda_3/(t^2+2)$	$\Lambda_3/(t+1)$
	$\Lambda_3/(t^2+1)$	$\Lambda_3/(t^2+1)$
	$\Lambda_3/(t^2+2t+2)$	$\Lambda_3/(t^2+2t+2)$
	$\Lambda_3/(t^2+2t+1)$	$\Lambda_3/(t^2+2t+1)$
	$\Lambda_3/(t^2+t+2)$	$\Lambda_3/(t^2+t+2)$
	$\Lambda_3/(t^2+t+1)$	$\Lambda_3/(t+2)$

and the second follows from proposition 4.1 of chapter 2, and otherwise the linear quandles of order nine and the quandles listed in table 1 are all distinct. Note that five of the eight listed quandles of order nine are connected; of the linear quandles of order nine, $\Lambda_9/(t-2)$, $\Lambda_9/(t-5)$ and $\Lambda_9/(t-8)$ are connected.

To count distinct Alexander quandles whose underlying Abelian group is neither cyclic nor a direct sum of n copies of $\mathbb{Z}_p$, the following observation is useful.

Lemma 4.16. *The number of conjugacy classes in* $\mathrm{Aut}_{\mathbb{Z}}(X_A)$ *is an upper bound on the number of distinct Alexander quandles* X *with underlying Abelian group* X_A.

Proof. Let $\phi_1, \phi_2 \in \mathrm{Aut}_{\mathbb{Z}}X_A$. Then if $t_1 = \phi_1(1)$ and $t_2 = \phi_2(1)$, we have $\phi_2^{-1}\phi_1\phi_2$ acting by multiplication by $t_2^{-1}t_1t_2 = t_1$ since multiplication in Λ is commutative. Thus any two conjugate automorphisms define the same Alexander quandle structure. □

To complete the classification of Alexander quandles with up to fifteen elements, we now only need to consider the case $X_A = \mathbb{Z}_4 \oplus \mathbb{Z}_2$.

Proposition 4.17. *There are three distinct Alexander quandles with underlying Abelian group* $\mathbb{Z}_4 \oplus \mathbb{Z}_2$*, defined by* $\mathbb{Z}$*-automorphisms* $\phi_1 = \mathrm{id}$*,* $\phi_2((1,0)) = (1,1)$*,* $\phi_2((0,1)) = (0,1)$*,* $\phi_3((1,0)) = (1,1)$ *and* $\phi_3((0,1)) = (2,1)$*. Further, these quandles are isomorphic to previously listed quandles, namely* $(\mathbb{Z}_4 \oplus \mathbb{Z}_2, \phi_1) \cong T_8$*,* $(\mathbb{Z}_4 \oplus \mathbb{Z}_2, \phi_2) \cong \Lambda_2/(t+1) \oplus \Lambda_2/(t^2+1)$*, and* $(\mathbb{Z}_4 \oplus \mathbb{Z}_2, \phi_3) \cong \Lambda_2/(t^3+t^2+t+1)$*.*

Proof. Direct calculation shows that $\mathrm{Aut}_{\mathbb{Z}}(\mathbb{Z}_4 \oplus \mathbb{Z}_2) \cong D_8$, the dihedral group of order eight, so by lemma 4.16 there are at most five Alexander quandle structures on $\mathbb{Z}_4 \oplus \mathbb{Z}_2$. Of the eight $\mathbb{Z}$-automorphisms of $\mathbb{Z}_4 \oplus \mathbb{Z}_2$, one is the identity, yielding the trivial quandle structure; five have $\mathrm{Im}(1-t) \cong \Lambda_2/(t+1)$ (including ϕ_2) and hence yield quandles isomorphic to $\Lambda_2/(t+1) \oplus \Lambda_2/(t^2+1)$, and two have $\mathrm{Im}(1-t) \cong \Lambda_2/(t^2+1)$ (including ϕ_3), yielding quandles isomorphic to $\Lambda_2/(t^3+t^2+t+1)$. □

We now have enough information to determine all Alexander quandles with up to fifteen elements. In light of corollaries 4.10 and 4.11, we list in table 2 only the numbers of distinct and connected Alexander quandles of each order.

TABLE 4.2. The number of Alexander quandles and connected Alexander quandles of size $n \leq 15$.

n	# of Alexander quandles	# connected
2	1	0
3	2	1
4	3	1
5	4	3
6	2	0
7	6	5
8	7	2
9	11	8
10	4	0
11	10	9
12	6	1
13	12	11
14	6	0
15	8	3

References

[1] J.S. Carter, D. Jelsovsky, L. Langford, S. Kamada, M. Saito, *Quandle cohomology and state-sum invariants of knotted curves and surfaces*, preprint, arXiv.org reference math.GT/9903135.

[2] J.S. Carter, D. Jelsovsky, S. Kamada, M. Saito, *Quandle homology groups, their Betti numbers, and virtual knots*, J. Pure Appl. Algebra, 157 (2001) 135-155.

[3] J.S. Carter, D. Jelsovsky, S. Kamada, M. Saito, *Computations of quandle cocycle invariants of knotted curves and surfaces*, Adv. Math. 157 (2001) 36-94.

[4] J.S. Carter, D. Jelsovsky, S. Kamada, M. Saito, *Geometric interpretations of quandle homology*, J. Knot Theory Ramifications, 10 (2001) 345-358.

[5] R. Fenn, C. Rourke, *Racks and links in codimension two*, J. Knot Theory Ramifications, 1 (1992) 343-406.

[6] R. Fenn, C. Rourke, B. Sanderson, *Trunks and classifying spaces*, Appl. Categor. Struct., 3 (1995) 321-356.

[7] M. Graña, *Indecomposable racks of order p^2*, preprint, arXiv.org reference math.QA/0203157.

[8] M. Goussarov, M. Polyak and O.Viro, *Finite type invariants of classical and virtual knots*, Topology 39 (2000) 1045-1068.

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

[10] S. Kamada, *Braid presentation of virtual knots and welded knots*, preprint.

[11] T. Kanenobu, *Forbidden moves unknot a virtual knot*, J. Knot Theory Ramifications 10 (2001) 89-96.

[12] L. H. Kauffman, *Virtual Knot Theory*, Europ. J. Combinatorics 20 (1999) 663-690.

[13] T. Mochizuki, *Some calculations of cohomology groups of finite Alexander quandles*, preprint.

[14] T. Ohtsuki, Ed. *Problems on Invariants of Knots and 3-Manifolds*, available at www.is.titech.ac.jp/~tomotada/proj01.

[15] S. Satoh, *Virtual knot presentation of ribbon torus-knots*, J. Knot Theory Ramifications, 9 (2000) 531-542.

Appendix: Letters of Permission

Date: Thu, 18 Apr 2002 12:02:35 +0800
From: Ye Qiang <qye@wspc.com.sg>
To: nelson@math.lsu.edu
Cc: jennifer@wspc.com, kauffman@uic.edu
Subject: Re: [Fwd: Article permission]

Dear Nelson,

World Scientific is pleased to grant the permission of your article in JKTR to you for including it in your thesis. Please include an acknowledgement that the paper is reprinted with the permission of Journal of Knot Theory and Its Ramifications. A copyright symbol shall also be included.

Please feel free to contact me if you need any further help.

Best regards,

Ye Qiang

> Subject: Re: Article permission
> Date: Tue, 16 Apr 2002 19:07:53 -0500 (CDT)
> From: Louis H Kauffman <kauffman@uic.edu>
> To: Eternal The Torment <nelson@math.lsu.edu>
> CC: Jennifer@wspc.com
>
> Dear Sam,
> You certainly have my permission as a Managing Editor of
> JKTR to include your JKTR paper in your thesis. Strictly
> speaking, I am not sure that I have this authority, so please
> write a note about this to
>
> Jennifer Cogollo, editorial assistant
> World Scientific Pub. Co.
> Suite 1B, 1060 Main Street
> River Edge, New Jersey 07661
> <Jennifer@wspc.com>
>
> I am forwarding this letter to Jennifer, and she will help you.
> Best,
> Lou Kauffman

Date: Fri, 31 May 2002 14:45:57 -0500 (CDT)
From: Judy Walker <jwalker@math.unl.edu>
To: Eternal The Torment <nelson@math.lsu.edu>
Subject: Re: JPAA submission

I checked with the editor-in-chief, who referred me to the webpage
http://authors.elsevier.com/JournalDetail.html?PubID=505614&dc=CI

The 8th bullet under "What rights do I retain as an author?" says:
"The right to include the article in a thesis or dissertation
provided that this is not to be published commercially."

****

Date: Thu, 20 Jun 2002 15:29:15 -0500 (CDT)
From: Richard A. Litherland <lither@math.lsu.edu>
To: Eternal The Torment <nelson@math.lsu.edu>
Subject: thesis

The contents of Chapter 3 of this thesis are substantially the same as a paper written jointly by Mr. Nelson and myself, and due to appear in the Journal of Pure and Applied Algebra. In common with almost all collaborative work in mathematics, the authors are listed alphabetically; there is no implication of seniority. Originally, I wrote sections 3.1, 3.2 and 3.4, and Sam wrote 3.3 (the proof of the main theorem). Subsequently, Sam rewrote parts of section 3.2 to incorporate a neater definition of the chain map alpha that he found.

Rick.
--
R. A. Litherland: <lither@math.lsu.edu>

Vita

Sam Nelson was born on December 17th, 1974, in Sidney, Nebraska. He finished his undergraduate studies at the University of Wyoming in May 1996. In August 1996 he came to Louisiana State University to pursue graduate studies in mathematics. He earned a master of science degree in mathematics from Louisiana State University in May 1998. He is currently a candidate for the degree of Doctor of Philosophy in mathematics, which will be awarded in August 2002.