EQUIVALENCE CLASSES OF COLORINGS

JUN GE

School of Mathematical Sciences, Xiamen University
Xiamen, Fujian 361005, P. R. China
E-mail: mathsgejun@163.com

SLAVIK JABLAN

The Mathematical Institute
Knez Mihailova 36, P.O. Box 367, 11001, Belgrade, Serbia
E-mail: sjablan@gmail.com

LOUIS H. KAUFFMAN

Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago
851 S. Morgan St., Chicago IL 60607-7045, USA
E-mail: kauffman@uic.edu

PEDRO LOPES

Center for Mathematical Analysis, Geometry and Dynamical Systems
Department of Mathematics, Instituto Superior Técnico, Universidade de Lisboa
Av. Rovisco Pais, 1049-001 Lisbon, Portugal
E-mail: pelopes@math.ist.utl.pt

Abstract. For any link and for any modulus m we introduce an equivalence relation on the set of non-trivial m-colorings of the link (an m-coloring has values in $\mathbf{Z}/m\mathbf{Z}$). Given a diagram of the link, the equivalence class of a non-trivial m-coloring is formed by each assignment of colors to the arcs of the diagram that is obtained from the former coloring by a permutation of the colors in the arcs which preserves the coloring condition at each crossing. This requirement implies topological invariance of the equivalence classes. We show that for a prime modulus the number of equivalence classes depends on the modulus and on the rank of the coloring matrix (with respect to this modulus).

1. Introduction. Given a diagram D of a link and a modulus $m > 1$, a (Fox) coloring ([3, 9]) is an assignment of integers modulo m to the arcs of D such that at each crossing twice the color assigned to the over-arc equals the sum of the colors assigned to the under-arcs, modulo m (see Figure 1). For each diagram and for each modulus $m > 1$ there is

$$c_i + c_{i+1} - 2c_{j_i} = 0$$

Fig. 1. Arcs at a crossing and the equation read off it. The coloring system of equations is formed by each of these equations, one per crossing of the diagram under study.

always at least one solution to this problem namely by assigning the same color (i.e., integer modulo m) to each and every arc of the diagram; thus there are exactly m such solutions modulo m. These are the trivial solutions modulo m, i.e., the so-called trivial m-colorings of the diagram. The non-trivial m-colorings are the solutions, modulo m, which involve at least two distinct colors.

REMARK. We remark that it is well known that this system of equations is also a system of relations for the first homology group of the 2-fold branched covering along the link ([14], Theorem 3.3). In fact, the fundamental group of the 2-fold branched covering along a link is presented by labeling the arcs of the unoriented link diagram and having relations of the form $c = ba^{-1}b$ read off at each crossing when b is the label of the over-crossing line. It then follows that $H_1(M_2(L)) \oplus \mathbf{Z}$ (the first homology group of the 2-fold branched covering along the link L) has presentation with $C = B - A + B = 2B - A$, where A, B, C are the corresponding elements in the abelianization of the fundamental group ([14, 19, 20]). Should one set the color of one of the arcs equal to 0 then there would be a bijective correspondence between this set of colorings and $H_1(M_2(L))$. It is interesting to remark that the fundamental group of the 2-fold branched covering along the link is itself a non-abelian generalization of the Fox coloring. While we do not use this aspect of the topology here, we are aware of it and it may be of use in later work. For more background on this material see [5, 8, 15, 17].

If a diagram endowed with an m-coloring undergoes a Reidemeister move, there is a unique reassignment of colors to the arcs involved in the move such that the new assignment is an m-coloring of the resulting diagram. Since these reassignments are reversible there is a bijection between the m-colorings before and after the performance of a finite number of Reidemeister moves. Furthermore, these reassignments preserve trivial m-colorings and thus they preserve also non-trivial m-colorings.

Therefore the number of m-colorings is a link invariant; the fact that a diagram of a link admits or not non-trivial m-colorings is an invariant of that link. It is known that there are links which do not admit non-trivial colorings over a given modulus. For example, the trefoil only admits non-trivial colorings over moduli divisible by 3.

In the course of our work on colorings, we have observed that for some choices of a modulus $m > 1$ and a link admitting non-trivial m-colorings, the following occurs. There are distinct non-trivial m-colorings, $\mathcal{C}, \mathcal{C}'$ (realized on an otherwise arbitrary diagram D

of this link) and there is a permutation γ of the m colors such that, for each arc a of D, the colors assigned to a in the coloring $\mathcal{C}$, say $\mathcal{C}(a)$, and in the coloring $\mathcal{C}'$, say $\mathcal{C}'(a)$, satisfy:

$$\mathcal{C}'(a) = \gamma\big(\mathcal{C}(a)\big).$$

Two such colorings will be said "related". An instance where this occurs is depicted in Figure 2. On the other hand it is not true that any permutation transforms the colors of a coloring into the colors of another coloring (see Figure 3).
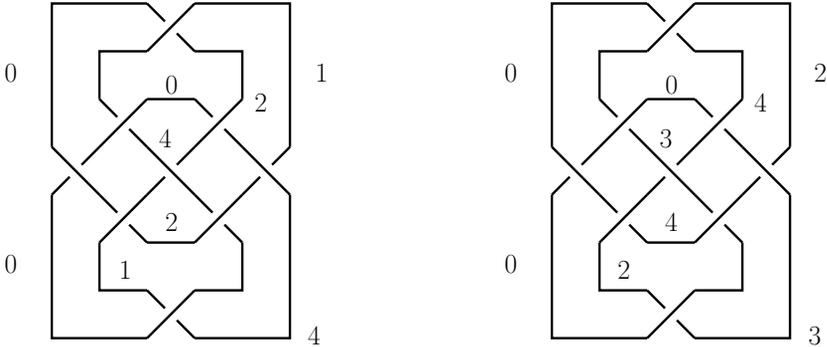
Fig. 2. Two identical diagrams of 9_{40} but endowed with distinct non-trivial 5-colorings. However, the colors of the one on the right are obtained from those of the one on the left by applying the permutation $(0)(1\,2\,4\,3)$. These two 5-colorings are related.
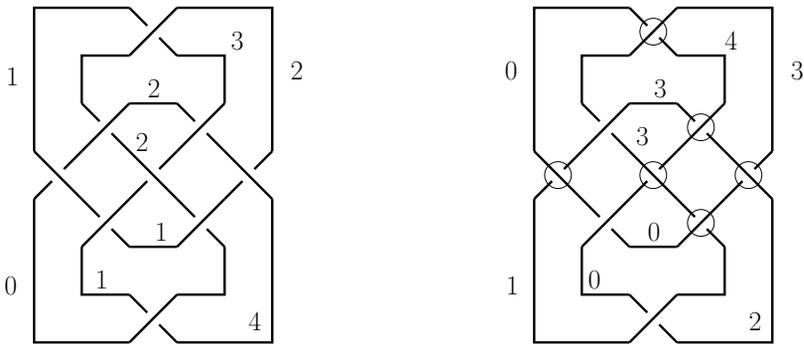
Fig. 3. On the left, knot 9_{40} endowed with the 5-coloring generated by the triplet $(0, 1, 2)$. On the right the action of permutation $(01)(234)$ on the colors of the coloring on the left: the result is not a 5-coloring (at the circled crossings the coloring condition is not satisfied).

Moreover, given non-trivial m-colorings $\mathcal{C}$ and $\mathcal{C}'$, realized on the same diagram, it may happen that there is no permutation γ of the m colors such that for each arc a of D

$$\mathcal{C}'(a) = \gamma\big(\mathcal{C}(a)\big).$$

We will then say "$\mathcal{C}'$ is essentially distinct from $\mathcal{C}$", in the given modulus, and the colorings split into equivalence classes (to be elaborated upon below). In Figure 4 we list representatives of the distinct equivalence classes of the non-trivial 5-colorings of 9_{40}.

c_1	c_2	c_3
0	0	1
0	1	0
0	1	1
0	1	2
0	1	3
0	1	4
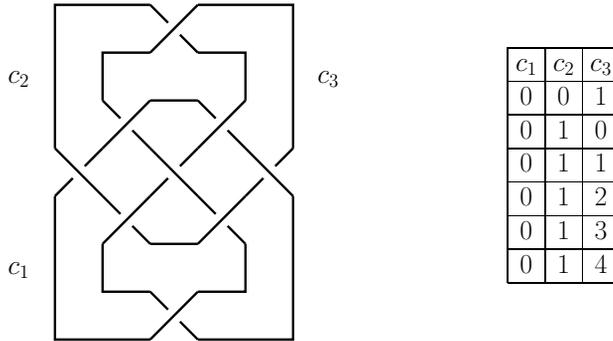
Fig. 4. On the left, knot 9_{40}. Assigning colors to the indicated c_i's will generate a coloring of the diagram (in the sense that the other colors of this coloring are uniquely determined by c_1, c_2, c_3—we elaborate on this issue below in the text). The table on the right displays six triplets (c_1, c_2, c_3) which generate essentially distinct 5-colorings on the diagram on the left.

We will be primarily concerned with permutations that preserve the coloring equation at each crossing for these are the ones that actually give us a corresponding coloring of the link and we will show that the relation sketched above among m-colorings of a diagram is an equivalence relation (see below).

We remark that the articles [2] and [1] address the same topic as the current article. Their definition of equivalent colorings assumes one has a list of all non-trivial m-colorings for a given diagram and states simply that any two of these colorings are equivalent provided there is a permutation of the m colors that, for each arc in the diagram, sends the color in this arc in the source coloring to the color in the same arc in the target coloring. This is equivalent to our definition. Unfortunately, for the purposes of counting equivalence classes of colorings in generic cases, the methodology in [2] and [1] seems to resort to generating classes of colorings by letting the symmetric group on the m colors act on a given m-coloring. As we see in Figure 3, there are assignments of colors to a diagram obtained in this way that do not constitute colorings. The formulas in the articles referred to above predict in general less equivalence classes than ours due to their over-counting of the elements on each orbit.

The equivalence classes of colorings constitute a topological invariant and in this article we provide combinatorial information about them. We hope this will prove to be useful for topological purposes.

In Section 2 we discuss preliminaries such as the nullity and the generating arcs of a coloring (Subsection 2.1), and the definition of the equivalence classes (Subsection 2.2). In Section 3 we calculate the number of equivalence classes in an infinite number of instances.

2. Preliminary material

2.1. Nullity and generating arcs of a coloring on a diagram.
Consider a link, L, along with a diagram D_L for that link. Regarding the arcs of this diagram as algebraic variables we write the homogeneous system of linear equations consisting of the equations

read off each crossing as illustrated in Figure 1. We call the matrix of the coefficients of this homogeneous system of linear equations *the coloring matrix of D_L*.

Any coloring matrix is made up of integers. Specifically, along each row one finds exactly two 1's and one -2, the rest being perhaps 0's. Thus, adding all the columns of a coloring matrix we obtain a column made up of 0's. It follows that the determinant of any coloring matrix is 0.

Upon performance of Reidemeister moves on a diagram, the changes on the original coloring matrix are realized by operations that constitute a subset of the following operations on integer matrices. These operations are generated by

1. multiplication of a row (column) by -1;
2. addition to one row (column) of integer linear combinations of other rows (columns);
3. insertion (deletion) of a row and column made up of 0's except for a 1 at the diagonal entry;
4. permutations of rows (columns).

These are the operations which relate equivalent matrices over the integers (see [11], p. 50). So the equivalence class of a coloring matrix is a topological invariant of the link under study. For each of these equivalence classes of matrices over the integers there is an outstanding representative which is called the Smith Normal Form (see [18]). Although the Smith Normal Form (SNF) is a familiar object we elaborate here slightly about it in order to bring out some connections with colorings of knots which we do not find in the literature.

An integer matrix in Smith Normal Form is a matrix such that its entries are all zero except perhaps along the diagonal. Along the diagonal the entries are non-negative (without loss of generality) and the i-th entry divides the $(i+1)$-th entry, up to a certain index l, and after that, the entries are all 0's:

$$d_1, d_2, \ldots, d_l, 0, 0, \ldots, 0 \qquad \text{with} \qquad d_i | d_{i+1} \quad 1 \leq i \leq l-1$$

The d_i's are called the *invariant factors* of the equivalence class; their name reflects the fact that the multi-set formed by them is an invariant of the equivalence class. This multi-set is then a topological invariant if it originates from a coloring matrix. Moreover, the Smith Normal Form of a coloring matrix is sure to have a 0 at the last entry of the diagonal since we proved above that the determinant of a coloring matrix is 0. The product of the remaining entries of the diagonal of the Smith Normal Form of a coloring matrix is *the determinant of the link* under study. This is also a topological invariant. (In passing, it is known that for knots, i.e., 1-component links, the determinant of the knot is an odd integer, see [16].)

We denote the Smith Normal Form of a matrix M by $S(M)$. Being an element of the equivalence class of M, $S(M)$ is obtained by a finite number of the operations listed above. We may then collect all the information concerning the row operations into an invertible matrix called R and likewise for the column operations into an invertible matrix called C to state ([18])

$$S(M) = RMC \tag{1}$$

with the juxtaposition of pairs of consecutive symbols on the right-hand side of the equation denoting matrix multiplication.

Let us now fix an otherwise arbitrary link along with one of its diagrams. Let us then relate the Smith Normal Form (and its invariant factors) of the coloring matrix of this diagram to the corresponding system of linear homogeneous equations and its solutions. There are always solutions of this system of equations namely by assigning the same integer to each arc. This corresponds to the fact that the determinant of the coloring matrix is 0. One of the algebraic variables may take on any value and if there is no other zero entry along the diagonal of the Smith Normal Form, then the remaining variables are uniquely determined once the former variable has been assigned a value. Going back to the original system of equations we obtain the so-called trivial solutions, i.e., those solutions that assign the same value to each and every arc of the diagram.

The invariant factors associated to our coloring matrix via its Smith Normal Form allow us to do something else. Suppose we choose a factor m of one of these invariant factors and decide to work over the integers modulo m. Then our Smith Normal Form in this new setting acquired at least one more 0 along the diagonal. Then, there is at least one more variable which can take on any value, modulo m. Going back to the original system of equations, there are at least two arcs which can take on any value modulo m. Hence, we now have polychromatic colorings, i.e., solutions where at least two distinct arcs take on two distinct colors that is, values modulo m. Had we chosen an m which does not possess common factors with the invariant factors, then modulo m there would have been only trivial colorings.

PROPOSITION 2.1. *Let p be an odd prime. Let D be a link diagram. The number of 0's (modulo p) along the diagonal of the Smith Normal Form of the coloring matrix, M, of D, equals the least number of arcs of D that can independently receive colors modulo p, and generate each p-coloring of D.*

Proof. If the Smith Normal Form exhibits n 0's modulo p, this means that the space of solutions has dimension n; working modulo a prime implies we are doing Linear Algebra over a field so it makes sense to talk about dimensions of spaces and bases. Then matrix C in (1) above operates a change of basis taking us back to algebraic variables equivalent to the arcs of the original diagram. Then n of these arcs have to generate all the colorings (i.e., all the solutions of the indicated system of equations modulo p) in terms of a basis of coloring vectors. ∎

DEFINITION 2.1. The number n in the proof of Proposition 2.1 is called the *p-nullity* (or the rank mod p) of the coloring matrix of D. Any set of n arcs that can independently receive colors modulo p and so generate each p-coloring of the diagram under study is said a *set of generating arcs* (of this diagram, with respect to this modulus).

COROLLARY 2.1. *We keep the notation of Proposition 2.1. If the p-nullity of a link is n then there are p^n p-colorings of the link, and $(p^n - p)$ non-trivial p-colorings of this link.*

Proof. There are p integers mod p so there are always p trivial p-colorings and p^n p-colorings. ∎

COROLLARY 2.2. *Let m be a composite positive integer. Let D be a link diagram. Each zero (modulo m) along the diagonal of the Smith Normal Form of the coloring matrix, M, of D contributes with a factor m for the number of solutions. Each zero divisor, z, of m along the diagonal contributes with a factor $\gcd(z, m)$ to the number of solutions. With n_Z for the number of 0's (modulo m) along the diagonal in $S(M)$, and $IZ(M)$ for the set the of invariant factors of M which are zero divisors of m, the formula for the number of m-colorings of D is*

$$m^{n_Z} \prod_{z \in IZ(M)} \gcd(z, m)$$

Proof. The contribution of the n_Z zero's (modulo m) along the diagonal of the Smith Normal Form to the number of solutions is clear. For the contribution of the zero divisors along the diagonal to the number of solutions see [10], page 40. This concludes the proof. ■

2.2. Equivalence classes of colorings. In this section we introduce equivalence classes of colorings as orbits of actions of certain groups of permutations on the set of colorings of a diagram. In order for this notion to be topological we require a special kind of permutation which we call a *coloring automorphism*. These are permutations which comply with the coloring operation,

$$a * b := 2b - a$$

in a pre-assigned modulus m. This operation generalizes to the quandle operation, generalizing also the notion of coloring ([7, 13]). In the particular instance $a * b = 2b - a$ we are dealing with the so-called dihedral quandles, one per integer modulus m.

DEFINITION 2.2 (coloring automorphism of $\mathbf{Z}_m$). Given an integer $m \geq 3$, we define a *coloring automorphism of $\mathbf{Z}_m$* to be a permutation, f, of $\mathbf{Z}_m$ such that

$$f(a * b) = f(a) * f(b)$$

for all $a, b \in \mathbf{Z}_m$, with $x * y = 2y - x \pmod{m}$, for every $x, y \in \mathbf{Z}_m$.

In [4] we find the following facts. For a given integer $m \geq 3$, each coloring automorphism of $\mathbf{Z}_m$ is given by

$$f_{\lambda, \mu}(x) = \lambda x + \mu$$

with $\mu \in \mathbf{Z}_m$ and $\lambda \in \mathbf{Z}_m^*$, the set of units of $\mathbf{Z}_m$. The set of all these coloring automorphisms of $\mathbf{Z}_m$ equipped with composition of functions, constitutes a group isomorphic to the affine group over $\mathbf{Z}_m$, i.e., isomorphic to the semi-direct product $\mathbf{Z}_m \rtimes \mathbf{Z}_m^*$. We denote it by $\mathbf{Aut}_m$.

For any integer $m \geq 3$ the inner coloring automorphism group of $\mathbf{Z}_m$ is generated by the automorphisms of the form $f_b(x) = x * b$. It is easy to see that this group consists of the elements of the form

$$f_{\pm, \mu}(x) = \pm x + \mu$$

If m is even this subgroup is isomorphic to the dihedral group of order m and μ can take on only "even" values from $\mathbf{Z}_m$. If m is odd, this subgroup is isomorphic to the dihedral group of order $2m$ and μ can take on any value from $\mathbf{Z}_m$. We denote it by $\mathbf{Inn}_m$. This information about coloring automorphisms of $\mathbf{Z}_m$ is contained in [4].

In the sequel, we will write "automorphism" (respectively, "inner automorphism") instead of the longer "coloring automorphism of $\mathbf{Z}_m$" (respectively, "inner coloring automorphism of $\mathbf{Z}_m$") since these are the only automorphisms of $\mathbf{Z}_m$ we consider in this article, i.e., the permutations of elements of $\mathbf{Z}_m$ that comply with the coloring operation.

Specifically, we will use the expression *automorphism* to designate a permutation of the form

$$f_{\lambda,\mu}(x) = \lambda x + \mu$$

with $\mu \in \mathbf{Z}_m$ and $\lambda \in \mathbf{Z}_m^*$, and *inner automorphism* to designate a permutation of the form

$$f_{\pm,\mu}(x) = \pm x + \mu$$

with μ taking on only "even" values from $\mathbf{Z}_m$ if m is even; with μ taking on any value from $\mathbf{Z}_m$ if m is odd.

We remark that it is well known that for a quandle $(Q, *)$ and a diagram D, the set of diagram colorings by elements of Q, $\mathrm{Col}_Q(D)$ is a Q-quandle set, where the action of Q on $\mathrm{Col}_Q(D)$ is given by $C * q$ for a coloring $C \in \mathrm{Col}_Q(D)$ and $q \in Q$ (Kamada was the first proponent of this language). Our considerations for dihedral quandles are related to this.

DEFINITION 2.3. Let $m > 1$ be an integer. Let L be a link admitting non-trivial m-colorings. Let D be a diagram of L. We let $m\mathcal{C}D$ stand for the set of *non-trivial m-colorings* of D.

PROPOSITION 2.2. *Let $m > 1$ be an integer. Let L be a link admitting non-trivial m-colorings and let D be a diagram of L. Let G be a subgroup of $\mathbf{Aut}_m$. Then G acts on $m\mathcal{C}D$ by permutations.*

Specifically, given $g \in G$ and $\mathcal{C}$, an m-coloring of D with colors c_i, then $g\mathcal{C}$ is the m-coloring of D obtained by replacing each color c_i by $g(c_i)$.

Moreover, this action is faithful and if m is prime this action is also free.

Proof. We keep the notation of the statement. We regard $\mathcal{C} \in m\mathcal{C}D$ as the map which assigns colors to the arcs of D in such a way that $\mathcal{C}(a_{i+1}) = 2\mathcal{C}(a_{j_i}) - \mathcal{C}(a_i)$, where j_i designates the index of the over-arc of the crossing where under-arcs with indices i and $i + 1$ meet, see Figure 1 (where now each c_k should be read $\mathcal{C}(a_k)$).

So, given $g \in G$ and $\mathcal{C} \in m\mathcal{C}D$, then $g\mathcal{C}$ is such that

$$g\big(\mathcal{C}(a_{i+1})\big) = g\big(2\mathcal{C}(a_{j_i}) - \mathcal{C}(a_i)\big) = 2g\big(\mathcal{C}(a_{j_i})\big) - g\big(\mathcal{C}(a_i)\big)$$

so $g\mathcal{C}$ is again an m-coloring of D.

Clearly, the identity element $1_G \in G$ is such that $1_G\mathcal{C} = \mathcal{C}$. Furthermore, for any two $g_1, g_2 \in G$, the composition of functions guarantees that $(g_1 g_2)\mathcal{C} = g_1\big(g_2\mathcal{C}\big)$.

We now prove that this action is faithful, i.e., we prove that given a non-identity $g \in G$ there exists a coloring $\mathcal{C} \in m\mathcal{C}D$ such that $g\mathcal{C} \in m\mathcal{C}D \neq \mathcal{C} \in m\mathcal{C}D$. We recall that the elements of G are, in particular, permutations of the elements of $\mathbf{Z}_m$. So given a non-identity element of G which moves $i \in \mathbf{Z}_m$, then the coloring obtained by assigning i to one of the generating arcs of the diagram is transformed via g into a coloring where now this generating arc is assigned $g(i) \neq i$.

We now prove that this action is free, i.e., that if given $g, h \in G$ there exists a coloring $\mathcal{C} \in m\mathcal{C}D$ such that $g(\mathcal{C}) = h(\mathcal{C})$ then $g = h$. We recall that, for some $\lambda, \lambda' \in \mathbf{Z}_m^*$ and $\mu, \mu' \in \mathbf{Z}_m$, $g(x) = \lambda x + \mu$, $h(x) = \lambda' x + \mu'$ for any $x \in \mathbf{Z}_m$. Since $g(\mathcal{C}) = h(\mathcal{C})$ then there exists two distinct colors in $\mathbf{Z}_m$, say $a \neq b$, such that $g(a) = h(a)$ and $g(b) = h(b)$. More precisely,

$$\begin{cases} 0 = (\lambda - \lambda')a + (\mu - \mu') \\ 0 = (\lambda - \lambda')b + (\mu - \mu') \end{cases} \qquad \Longleftrightarrow \qquad \begin{cases} \lambda = \lambda' \\ \mu = \mu' \end{cases}$$

since $a \neq b$ and m is prime. Thus $g = h$.

This concludes the proof. ■

DEFINITION 2.4 (*G-equivalence classes of m-colorings of D*). Let G be a subgroup of $\mathbf{Aut}_m$. The *G-equivalence classes* of *m*-Colorings of D are, by definition, the *G*-orbits over $m\mathcal{C}D$.

We will next prove that this notion provides topological invariants (in particular, the number of equivalence classes of *m*-colorings of a link).

It is well known that, given any two diagrams of the same link, there is a bijection between the two sets of *m*-colorings of these diagrams ([12], [14], Lemma 2.2). Moreover, this bijection takes trivial *m*-colorings to trivial *m*-colorings and non-trivial *m*-colorings to non-trivial *m*-colorings. This bijection is realized by the "Colored Reidemeister Moves". The Colored Reidemeister Moves apply to a diagram endowed with an *m*-coloring; a Reidemeister move is applied to the diagram and a local adjustment of the coloring is performed. These adjustements are unique and reversible thereby proving the bijection between the two sets of *m*-colorings of any two diagrams of the same link.

PROPOSITION 2.3. *Let m be an integer greater than 1. Let L be a link admitting non-trivial m-colorings and let D and D′ be two diagrams of L. Let G be a subgroup of $\mathbf{Aut}_m$.*

There is a bijection from $m\mathcal{C}D$ to $m\mathcal{C}D'$, which preserves the G-equivalence classes.

Proof. From [12] we know that the Colored Reidemeister Moves realize a bijection from the set of *m*-colorings of D to the set of *m* colorings of D', taking non-trivial colorings to non-trivial colorings. We now prove that the Colored Reidemeister Moves take distinct elements of $m\mathcal{C}D$ along a *G*-equivalence class, to distinct elements of $m\mathcal{C}D'$ along a *G*-equivalence class. Specifically, for $g \in G$ and $\mathcal{C} \in m\mathcal{C}D$, we prove that the "Colored Reidemeister moves" take $\mathcal{C} \in m\mathcal{C}D$ to $\mathcal{C}' \in m\mathcal{C}D'$ and $g\mathcal{C} \in m\mathcal{C}D$ to $g\mathcal{C}' \in m\mathcal{C}D'$. The proofs of these statements for the individual "Colored Reidemeister Moves" of type I, II, and III are displayed in Figures 5, 6, and 7. The $\sim$ associates horizontally colorings on distinct diagrams related by a Colored Reidemeister move. Vertically we display colorings $\mathcal{C}$ and $g\mathcal{C}$ ($\mathcal{C}'$ and $g\mathcal{C}'$, respect.) for diagram D (D', respect.).

In Figures 5 and 6 circles with dotted lines were drawn to bring out the local nature of the transformation. This was not done in Figure 7 in order not to overburden the figure. ■

REMARK. Proposition 2.3 can also be seen by regarding mod-m colorings as elements of $(H_1(M_L^{(2)}), Z/m) \cong Hom(H_1(M_L^{(2)}), Z/m)$.

$$\mathcal{C}(r) = x \qquad\qquad \sim \qquad\qquad \mathcal{C}'(r_1') = x = \mathcal{C}'(r_2')$$

D D'

$$g\big(\mathcal{C}(r)\big) = g(x) \qquad\qquad \sim \qquad\qquad g\big(\mathcal{C}'(r_1')\big) = g(x) = g\big(\mathcal{C}'(r_2')\big)$$
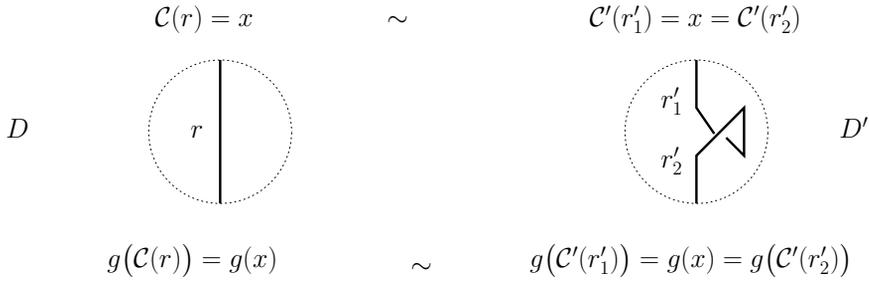
Fig. 5. Colored Reidemeister move of type I and G-equivalence relation of colorings
on the same diagram.

$$\mathcal{C}(r) = x \qquad\qquad \sim \qquad\qquad \mathcal{C}'(r_1') = x \qquad \mathcal{C}'(s') = y$$
$$\mathcal{C}(s) = y \qquad\qquad\qquad\qquad \mathcal{C}'(r_2') = 2\mathcal{C}'(s') - \mathcal{C}'(r_1') = 2y - x$$
$$\mathcal{C}'(r_3') = \ldots = 2y - (2y - x) = x$$

D D'

$$g\big(\mathcal{C}(r)\big) = g(x) \qquad\qquad \sim \qquad\qquad g\big(\mathcal{C}'(r_1')\big) = g(x) \qquad g\big(\mathcal{C}'(s')\big) = g(y)$$
$$g\big(\mathcal{C}(s)\big) = g(y) \qquad\qquad\qquad\qquad g\big(\mathcal{C}'(r_2')\big) = g(2\mathcal{C}'(s') - \mathcal{C}'(r_1')) = 2g(y) - g(x)$$
$$g\big(\mathcal{C}'(r_3')\big) = \ldots = g(2y - (2y - x)) = g(x)$$
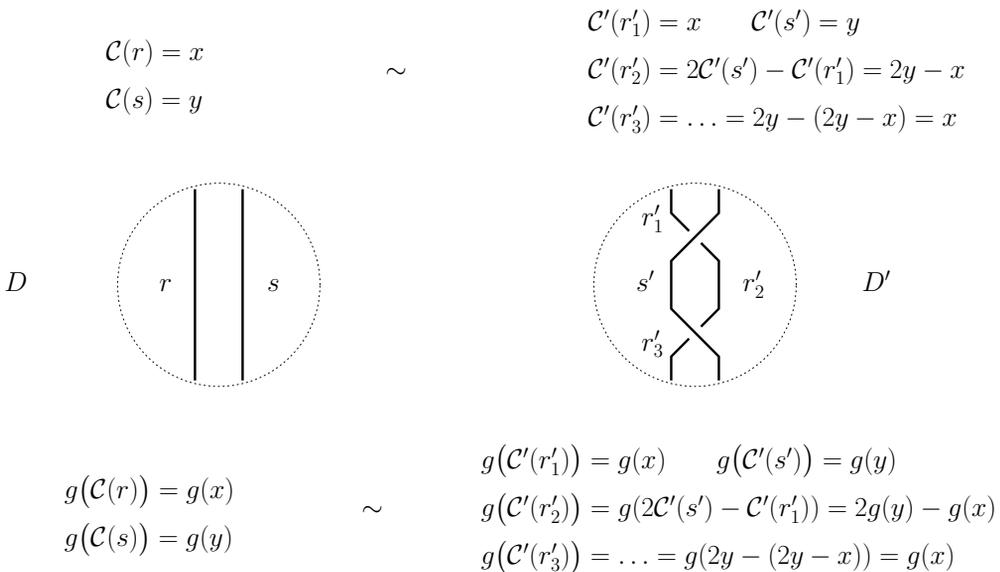
Fig. 6. Colored Reidemeister move of type II and G-equivalence relation of colorings
on the same diagram.

THEOREM 2.1. *Let L be a link and D one of its diagrams. Let $m > 1$ be an integer.*

The number of G-equivalence classes of m-colorings of D is a topological invariant. The multi-set whose elements are the number of m-colorings per G-equivalence class of m-colorings of D is a topological invariant.

Proof. This is a straight-forward consequence of Proposition 2.3. ∎

We remark that in the sequel G, the subgroup of $\mathbf{Aut}_m$, will be either $\mathbf{Aut}_m$ itself or $\mathbf{Inn}_m$. Figure 8 illustrates the fact that in general there are more inner equivalence classes than equivalence classes (for the same link and for the same modulus).

$\mathcal{C}(r_1) = x \qquad \mathcal{C}(s_1) = y \qquad \mathcal{C}(t) = z$

$\mathcal{C}(r_2) = \ldots = 2y - x$

$\mathcal{C}(s_2) = \ldots = 2z - y$

$\mathcal{C}(r_3) = \ldots = 2z - (2y - x) = 2z - 2y + x$

$\sim$

$\mathcal{C}'(r_1') = x \qquad \mathcal{C}'(s_1') = y \qquad \mathcal{C}'(t') = z$

$\mathcal{C}'(r_2') = \ldots = 2z - x$

$\mathcal{C}'(s_2') = \ldots = 2z - y$

$\mathcal{C}'(r_3') = \ldots = 2z - 2y + x$

$g\big(\mathcal{C}(r_1)\big) = g(x) \qquad g\big(\mathcal{C}(s_1)\big) = g(y)$

$\qquad g\big(\mathcal{C}(t)\big) = g(z)$

$g\big(\mathcal{C}(r_2)\big) = \ldots = 2g(y) - g(x)$

$g\big(\mathcal{C}(s_2)\big) = \ldots = 2g(z) - g(y)$

$g\big(\mathcal{C}(r_3)\big) = \ldots = 2g(z) - 2g(y) + g(x)$

$\sim$

$g\big(\mathcal{C}'(r_1')\big) = g(x) \quad g\big(\mathcal{C}'(s_1')\big) = g(y)$

$\qquad g\big(\mathcal{C}'(t)\big) = g(z)$

$g\big(\mathcal{C}'(r_2')\big) = \ldots = 2g(y) - g(x)$

$g\big(\mathcal{C}'(s_2')\big) = \ldots = 2g(z) - g(y)$

$g\big(\mathcal{C}'(r_3')\big) = \ldots = 2g(z) - 2g(y) + g(x)$
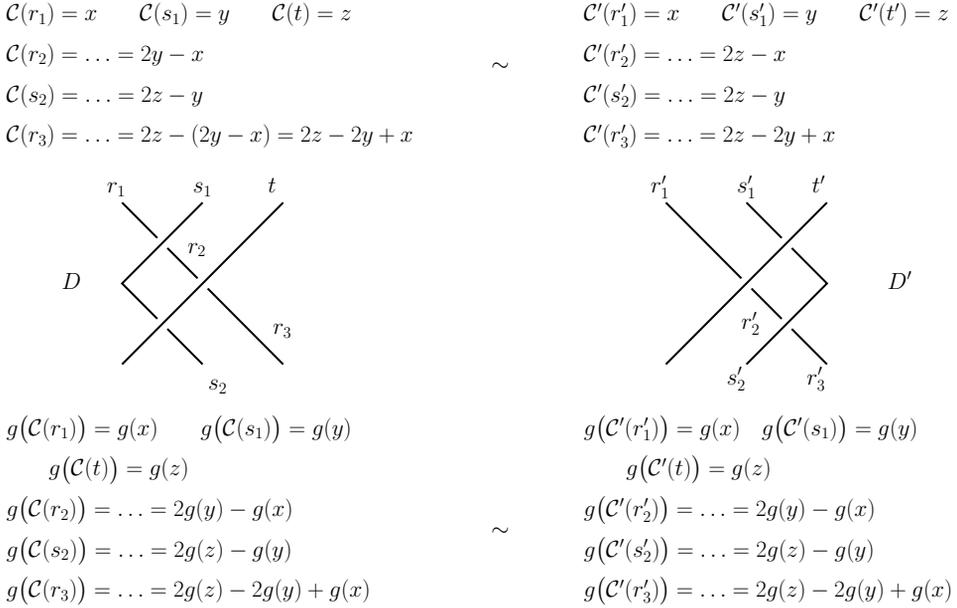
Fig. 7. Colored Reidemeister move of type III and G-equivalence relation of colorings on the same diagram.
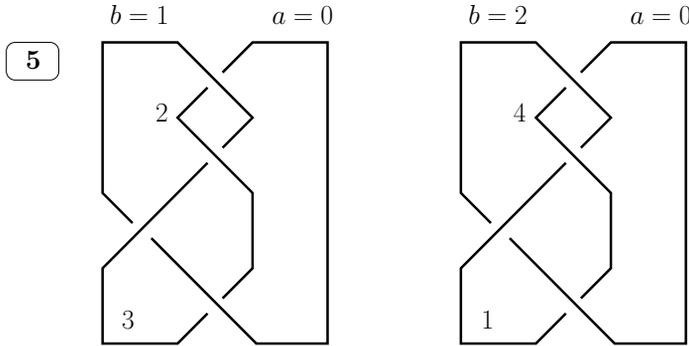
Fig. 8. Two 5-colorings of the Figure-8 knot (which has determinant 5). These colorings are representatives of the two distinct 5-coloring inner equivalence classes. On the other hand there is only one 5-coloring equivalence class. These facts will be clear from the results in Section 3.

3. Formulas for numbers of equivalence classes.

In this section we apply the theory developed above to specific situations. *We use p-nullity as in Definition* 2.1.

3.1. Equivalence classes

PROPOSITION 3.1. *Let p be an odd prime and n an integer greater than* 1. *A link L with p-nullity n has*

$$\frac{p^{n-1} - 1}{p - 1}$$

equivalence classes of p-colorings.

Proof. As discussed right after Definition 2.2, an automorphism of $\mathbf{Z}_p$

$$f_{\lambda,\mu}(x) = \lambda x + \mu$$

depends on two parameters $\lambda \in \mathbf{Z}_p^*$ and $\mu \in \mathbf{Z}_p$. Since $|\mathbf{Z}_p| = p$ and $|\mathbf{Z}_p^*| = p - 1$, there are then exactly $p(p - 1)$ automorphisms for $\mathbf{Z}_p$.

Now suppose $\mathcal{C}$ is in $p\mathcal{C}D$, where D is a diagram of L. Since the action of $\mathbf{Aut}_p$ is free (2.2) each orbit of the action has exactly $p(p - 1)$ elements. Since there are $p^n - p$ elements in $p\mathcal{C}D$, there are then

$$\frac{p^n - p}{p(p - 1)} = \frac{p^{n-1} - 1}{p - 1}$$

orbits of this action which is the number of equivalence classes of p-colorings for link L. ∎

COROLLARY 3.1. *We keep the notation of Proposition* 3.1.

1. *If a diagram D of link L admits a non-trivial p-coloring with the least number of colors (over all diagrams, over all non-trivial p-colorings), then there are at least $p(p - 1)$ such p-colorings of D.*
2. *If the nullity of $L \bmod p$ is 2 and a diagram D of L admits a non-trivial p-coloring with k colors, then any other non-trivial p-coloring of D uses k colors. In particular, if D is a diagram of L where a non-trivial p-coloring is realized with the least number of colors, then any other non-trivial p-coloring of this diagram uses also the least number of colors.*

Proof. 1. Since the automorphisms are permutations of the p colors they preserve the number of distinct colors. So if a non-trivial p-coloring of a diagram uses k colors, then along its equivalence class the non-trivial p-colorings use k colors each and there are $p(p - 1)$ non-trivial p-colorings per equivalence class. If a diagram D of link L admits a non-trivial p-coloring with the least number of colors then along its equivalence class the non-trivial p-colorings use the same number of colors each.

2. If the nullity of $L \bmod p$ is 2 then there is only one equivalence class (mod p). Then the arguing of 1. is valid for the $p(p - 1)$ non-trivial p-colorings in this orbit. ∎

COROLLARY 3.2. *Let L be a link with the following property.*

The Smith Normal Form of a(ny) coloring matrix of L has only one 0 and only one $0 \neq d \neq 1$ along the diagonal.

Then for any prime p such that $p \mid d$, there is only one equivalence class of p-colorings. In particular, rational links satisfy this property.

Proof. Working mod p the Smith Normal Form of the coloring matrix will exhibit exactly two zeros. Hence the p-nullity is 2 and the result follows from Proposition 3.1. ∎

COROLLARY 3.3. *The following links have only one class of p-colorings for each prime p for which they admit non-trivial p-colorings.*

1. *Links whose determinant is prime.*
2. *Links of non-zero determinant whose SNF of the coloring matrix displays different primes on different diagonal entries (besides the 0 entry and possible 1's).*
3. *Knots whose knot group can be presented using one relator (in particular, torus knots).*

Proof. 1. and 2. are particular cases of Corollary 3.2. As for 3., since the deficiency of knot groups is one then knot groups which can be presented with one relator only need two generators. Then the Smith Normal Form of the coloring matrix is diag $(d, 0)$ where d is the determinant of the knot. ∎

3.2. Inner-equivalence classes

PROPOSITION 3.2. *Let p be an odd prime and n an integer greater than* 1. *A link L with p-nullity n has*

$$\frac{p^{n-1} - 1}{2}$$

inner-equivalence classes of p-colorings.

Proof. As discussed right after Definition 2.2, an inner-automorphism of $\mathbf{Z}_p$ is of the form

$$f_{\pm,\mu}(x) = \pm x + \mu$$

with $\mu \in \mathbf{Z}_p$. There are then exactly $2p$ inner-automorphisms for $\mathbf{Z}_p$.

The rest of the proof goes through as in the proof of Proposition 3.1 leading to the following number of inner-orbits

$$\frac{p^n - p}{2p} = \frac{p^{n-1} - 1}{2}. \quad ∎$$

COROLLARY 3.4. *Let L be a link with the following property.*

The Smith Normal Form of a(ny) coloring matrix of L has only one 0 and only one $0 \neq d \neq 1$ along the diagonal.

Then for any prime p such that $p \,|\, d$, there are $\frac{p-1}{2}$ inner-equivalence classes of p-colorings. In particular, rational links satisfy this property.

Proof. Adapt the proof for Corollary 3.2. ∎

COROLLARY 3.5. *The following links have $\frac{p-1}{2}$ classes of p-colorings for each prime p for which they admit non-trivial p-colorings.*

1. *Links whose determinant is prime.*
2. *Links of non-zero determinant whose Smith Normal Form of the coloring matrix displays different primes on different diagonal entries (besides the 0 entry and possible 1's).*
3. *Knots whose knot group can be presented using one relator (in particular, torus knots).*

Proof. Adapt the proof for Corollary 3.3. ∎

4. Directions for future work. In the context of quandles this work has to do with homomorphisms from the fundamental quandle of the knot to the dihedral quandles ([7, 13]). We organize these homomorphisms into equivalence classes. In future work we plan to generalize this work to other classes of target quandles, other than the dihedral quandles.

References

[1]   A.-L. Breiland, L. Oesper, L. Taalman, *p-coloring classes of torus knots*, Missouri J. Math. Sci. 21 (2009), 120–126.

[2]   K. Brown, K. O'Neil, L. Taalman, *Counting m-coloring classes of knots and links*, found at http://educ.jmu.edu/˜taalmala/PME_brown_oneil_taal.pdf.

[3]   R. Crowell, R. Fox, *Introduction to Knot Theory*, Dover Publications, 2008.

[4]   M. Elhamdadi, J. MacQuarrie, R. Restrepo, *Automorphism groups of quandles*, J. Algebra Appl. 11 (2012), 1250008, 9 pp.

[5]   R. H. Fox, *A quick trip through knot theory*, in: Topology of Three-Manifolds and related topics, Prentice-Hall, Englewood Cliffs, NJ 1962, 120–167.

[6]   S. Jablan, R. Sazdanović, *LinKnot. Knot Theory by Computer*, Ser. Knots Everything 21, World Scientific, River Edge, NJ 2007.

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

[8]   L. H. Kauffman, *On Knots*, Ann. of Math. Stud. 115, Princeton Univ. Press, Princeton 1987.

[9]   L. H. Kauffman, *Knots and Physics*, Ser. Knots Everything 1, 53, World Scientific, River Edge, NJ, 1991, 1994, 2001, 2013.

[10] L. H. Kauffman, P. Lopes, *On the minimum number of colors for knots*, Adv. in Appl. Math. 40 (2008), 36–53.

[11] W. B. R. Lickorish, *An Introduction to Knot Theory*, Grad. Texts in Math. 175, Springer, New York 1997.

[12] P. Lopes, *Quandles at finite temperatures* I, J. Knot Theory Ramifications 12 (2003), 159–186.

[13] S. V. Matveev, *Distributive groupoids in knot theory*, Mat. Sb. (N.S.) 119 (1982), 78–88; English transl.: Math. USSR-Sb. 47 (1984), 73–83.

[14] J. Przytycki, 3-*coloring and other elementary invariants of knots*, in: Knot Theory (Warsaw, 1995), Banach Center Publ. 42, Polish Acad. Sci. Inst. Math., Warsaw 1998, 275–295.

[15] K. Reidemeister, *Knotentheorie*, Chelsea Pub. Co., New York 1948; Originally published in 1932 – Julius Springer, Berlin.

[16] D. Rolfsen, *Knots and links*, AMS Chelsea Publishing, 2003.

[17] H. Seifert, *Über das Geschlecht von Knoten*, Math. Ann. 110 (1935), 571–592.

[18] H. J. S. Smith, *On systems of linear indeterminate equations and congruences*, Philos. Trans. R. Soc. Lond. 151 (1861), 293–326.

[19] M. Wada, *Group invariants of links*, Topology 31 (1992), 399–406.

[20] S. Winker, *Quandles, knots invariants and the n-fold branched cover*, Ph.D. Thesis, Univ. of Illinois at Chicago, 1984.