

A combinatorial approach to knot recognition

Andrew Fish¹, Alexei Lisitsa², and David Stanovský^{3*}

1. School of Computing, Engineering and Mathematics, University of Brighton, UK
2. Department of Computer Science, The University of Liverpool, UK
3. Department of Information Systems and Mathematical Modeling, International IT University, Almaty, Kazakhstan & Department of Algebra, Faculty of Mathematics and Physics, Charles University, Prague, Czech Republic

Abstract. This is a report on our ongoing research on a combinatorial approach to knot recognition, using coloring of knots by certain algebraic objects called quandles. The aim of the paper is to summarize the mathematical theory of knot coloring in a compact, accessible manner, and to show how to use it for computational purposes. In particular, we address how to determine colorability of a knot, and propose to use SAT solving to search for colorings. The computational complexity of the problem, both in theory and in our implementation, is discussed. In the last part, we explain how coloring can be utilized in knot recognition.

1 Introduction

Knot recognition is a central problem in computational knot theory. Given two *knots* (closed loops in space without self-intersection), or rather their descriptions (such as their diagrams, Gauss codes, etc.), are they *equivalent* in the sense that there is an ambient isotopy (informally, a continuous deformation of space) transforming one knot into the other?

Although it all started with Kelvin's hypothesis that different elements are differently knotted vortices of ether [20], most of the work on knot recognition is a typical mathematical endeavour, with little care paid to potential applications. Nevertheless, current real life motivation to study knots exist: for example, some molecules, such as DNA, can occur knotted, and their chemical or biological properties depend on the way they are knotted (it is reported that certain antibiotics exploit topological properties of DNA). See [1, Section 7] or [4] for details and other applications of knots in biology, chemistry and physics.

Knot theory, since its beginnings in late 19th century, has used mostly geometric and topological methods, often supported by an algebraic framework (algebraic topology, homological algebra, polynomials). This is somewhat surprising, since tame knots can be considered as finite graph-like structures (see [18] for more ideas in this direction); the tameness condition is imposed to rule out pathological cases. An entirely new approach appeared in foundational papers by Joyce [12] and Matveev [17] where certain algebraic structures, called

* Partially supported by the GAČR grant 13-01832S.

quandles, were introduced and used to obtain a complete invariant (up to reverse mirroring), called the knot quandle. While their motivation was to capture the essential part of the knot group, their works paved the way to introduce an extensive class of combinatorial knot invariants, based on coloring of arcs by (finite) quandles.

The present paper is an initial report on our project to turn the coloring method into a practical computational tool for knot recognition. In the first part (Section 3), we summarize the mathematical theory necessary to understand the algorithms. The ideas are old, but dispersed around various sources; our contribution is a compact self-contained presentation of the material. Then, we discuss how to find a coloring, computationally. A theoretical framework and the complexity of the problem is addressed in Section 4.1. To search for a coloring in practice, we propose to use SAT solving. This idea seems to be new and our initial experiments are reported in detail in Section 4.2 which is the core of the paper. In the last part, we explain how coloring can be utilized for knot recognition (Section 5), building upon earlier ideas of [6,8].

Readers not familiar with basic notions of knot theory are recommended to take a fine crash course on Wikipedia¹. A standard textbook reference is [1]. By an *unknot* we mean any knot equivalent to the trivial knot, a simple circle in space. Informally, unknots are knots that can be untangled. Non-specialists are recommended to read the article [10] to learn what is so hard about unknotting unknots.

All knots in the text are assumed to be tame and oriented. For computational purposes, knots are presented in the form of diagrams, which are regular planar projections, so that the only singularities of the projection are transverse double points, and these bear additional information about the relative height of strands at every crossing. The size of a knot diagram then refers to the number of crossings, which determines, for instance, the size of its Gaussian code or other diagram encodings. Greek letters α, β, γ will be used for knot arcs, and latin letters a, b, c for colors.

2 Classical approach to knot recognition

Mathematicians have been working on the knot recognition problem for more than a century, yet are nowhere near a satisfactory solution. The standard approach is based on calculating *invariants*, properties shared by equivalent knots. Classical invariants use various algebraic constructions to code some of the topological properties of a knot. Typical examples are polynomial invariants, for instance:

- The *Alexander polynomial*. It can distinguish most small knots, yet there are infinitely many knots with trivial Alexander polynomial (hence indistinguishable from the unknots). A polynomial time algorithm, fast in practice, exists (based on calculation of a determinant of a sparse matrix).

¹ http://en.wikipedia.org/wiki/Knot_theory

- The *Jones polynomial* and several common generalizations of the Jones and Alexander polynomials. They tend to distinguish even more knots, yet it is not known whether they distinguish unknots. Better performance comes for a price: calculating (or even approximating) the Jones polynomial is known to be $\#P$ -hard.
- The currently fashionable *Khovanov homology* is the “categorification” of the Jones polynomial. It provably distinguishes unknots, but is even harder to calculate in practice.

Among other classical methods, let us mention the *knot group*, the fundamental group of the knot complement, which informally describes the “holes” the knot creates in space. While fairly powerful in theory (for instance, it does distinguish unknots), it is not directly useful for calculations, since there is no algorithm to handle the isomorphism problem for finitely presented groups.

From what we have said so far, it would not even be clear whether knot recognition is algorithmically decidable. However, it was shown to be decidable by Haken in 1962, by an algorithm which was considered impractical for implementation. The complexity of knot recognition is an interesting and widely open problem.

Even the special case of *unknot recognition* (formally, given a knot, is it equivalent to an unknot?) is not fully understood, although there has been significant progress over the past 20 years. At the moment, unknot recognition is known to be both in the NP and coNP complexity classes (coNP assuming the Generalized Riemann Hypothesis, GRH). A polynomial-time checkable certificate of unknottedness was found by Hass, Lagarias and Pippenger [9], using the theory of normal surfaces. A more natural certificate, a polynomial length sequence of Reidemeister moves that untangles an unknot, has been conjectured for a long time, but was only proved to exist by Lackenby [15] very recently (however, it provides no clue for how to find that short sequence efficiently). On the other hand, a polynomial-time certificate for knottedness was proved to exist by Kuperberg [14], assuming GRH, taking the Kronheimer-Mrówka representation of the knot group over the group $SL(2, \mathbb{C})$ and using GRH to project it to a representation over a finite field of a sufficiently small size.

3 Combinatorial approach to knot recognition

A combinatorial approach to knot theory is possible, following Reidemeister, since two knots are ambient isotopic if and only if they have diagrams which differ by a finite sequence of local diagram rewrite rules called Reidemeister moves. Thus, invariants of knots can be constructed as invariants of knot diagrams which do not change under the Reidemeister moves.

3.1 Coloring knots

One of the first invariants ever considered was *tricolorability*: color the arcs of a knot diagram with three colors in a way that, at every crossing, the three

strands have either the same, or three different colors. Every knot admits three *trivial colorings*, with all arcs painted in the same color. A knot diagram is called tricolorable if it admits a non-trivial tricoloring. It is not difficult to show that tricolorability is invariant with respect to Reidemeister moves, and so it is a property of knots (not just their diagrams) which is invariant with respect to knot equivalence. More generally, the number of non-trivial tricolorings of a knot K , $\text{col}_3(K)$, is an invariant.



Fig. 1. Tricolored trefoil and five-colored figure-eight.

Figure 1 shows an example of a non-trivial tricoloring. Tricolorability is not a terribly good invariant: for instance, it cannot distinguish the figure-eight knot from an unknot, as the figure-eight knot admits no non-trivial tricoloring.

More generally, one can consider *Fox n -colorings*, using colors $0, 1, \dots, n-1$, and the rule that, for every crossing, the sum of the colors of the two lower strands equals twice the color of the bridge, modulo n . The number $\text{col}_n(K)$ of non-trivial n -colorings is an invariant, which is easily calculated using linear algebra and the Chinese Remainder Theorem. Figure 1 shows an example of a non-trivial 5-coloring of the figure-eight knot (only four colors are used, but, importantly, the arithmetic is modulo 5). Notice that Fox 3-coloring is the same thing as tricoloring.



Fig. 2. Labeled crossing.

There is an common framework for these and other arc coloring invariants. Let C be a set (of colors) and $*$ a binary operation on C . A *coloring* of a knot diagram is a mapping f assigning to every arc a color from C in a manner that, for every crossing with arcs labeled α, β, γ as in Figure 2, the equation

$$f(\alpha) * f(\beta) = f(\gamma) \quad (\text{E})$$

is satisfied. A coloring is called trivial if it only uses one color. For example, tricolorability uses a set C with $|C| = 3$ and the operation defined by $a * a = a$ for every $a \in C$ and $a * b$ equal to the third color whenever $a \neq b$. Fox n -coloring uses $C = \{0, 1, \dots, n-1\}$ and $a * b = 2a - b \bmod n$.

Let $\text{col}_Q(D)$ denote the number of non-trivial colorings of the knot diagram D by the algebraic structure $Q = (C, *)$. Not every algebraic structure provides an invariant. The following theorem determines such instances.

Theorem 1. *Let $Q = (C, *)$ be an algebraic structure over a set C with a binary operation $*$ satisfying the following conditions for every $a, b, c \in C$:*

- (1) $a * a = a$ (idempotence);
- (2) there is a unique $x \in C$ such that $a * x = b$ (unique left division);
- (3) $a * (b * c) = (a * b) * (a * c)$ (left self-distributivity).

Then col_Q is a knot invariant.

The algebraic structures satisfying conditions (1), (2), (3) are called *quandles*. (We use the *left* notation for quandles.)

Theorem 1 is a consequence of the theory developed in [12,17]. Here is a sketch of the direct proof.

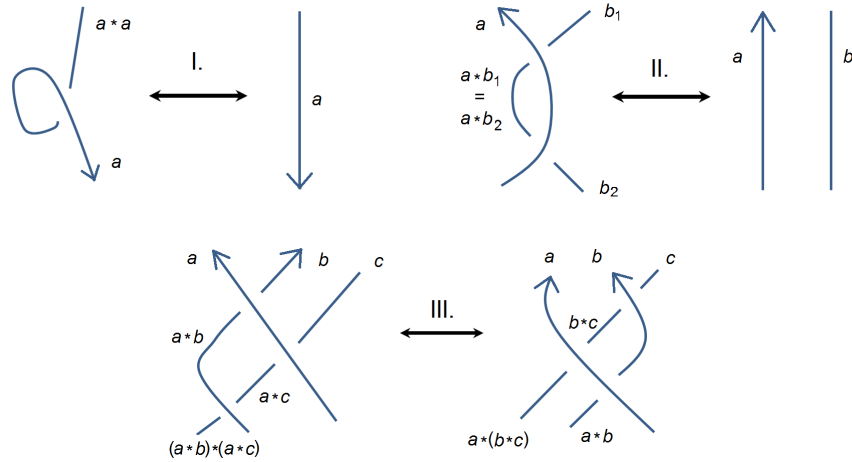


Fig. 3. Reidemeister moves and invariance of coloring.

It is sufficient to show that col_Q is invariant with respect to the three Reidemeister moves, i.e., if two diagrams D, D' differ by a single move, the number of non-trivial colorings remains the same. We prove that every coloring of D corresponds uniquely to a coloring of D' that uses identical colors for arcs outside the scope of the move, including those crossing the move's borderline.

For the type I move, there are two options for the orientation. For the downwards orientation as in Figure 3, assume the color of the lower arc in the lefthand picture is a . Then, the color of the upper arc is $a * a$. Using (1), we have $a * a = a$, hence every coloring of the lefthand diagram colors both arcs in the same color, and thus corresponds to a unique coloring of the righthand diagram. For the upwards orientation, the upper arc has a color x such that $a * x = a$. Using (2), this color is uniquely determined, and using (1), $x = a$, and the same argument proves the case.

For the type II move, there are two options for the orientation, again. For the upwards orientation as in Figure 3, assume the colors of the border arcs in the lefthand picture are a, b_1, b_2 , respectively. Then, the color of the middle arc is $a * b_1 = a * b_2$, hence uniquely determined by a, b_1, b_2 . Moreover, using (2), we have $b_1 = b_2$. Hence every coloring of the lefthand diagram corresponds to a uniquely determined coloring of the righthand diagram. Thanks to (1), non-trivial colorings correspond mutually. A similar argument proves the downwards orientation.

For the type III move as in Figure 3, assume the colors of the top arcs be a, b, c , respectively. The colors of the remaining arcs are uniquely determined as in the picture. To obtain the same color for the left bottom arc, we use condition (3). For the other three orientations, we proceed similarly; condition (2) is needed for unique solutions as in case I.

Looking at the proof sketch, we see that the three axioms of quandles relate very well to the three Reidemeister moves. Invariance with respect to type II moves uses precisely condition (2), and invariance with respect to types I and III moves uses precisely conditions (1) and (3), respectively, in some cases under the assumption of unique left division. The converse statement, that *quandles are the only structures providing arc coloring invariants of knots*, is also true in certain way, but the precise statement and a proof is beyond the scope of the present paper.

3.2 Quandles

A natural question arises: what really are quandles? The answer is not yet fully understood, but in the most important case, of so called *algebraically connected quandles*, it is. We will briefly summarize the theory in the next paragraph. Readers with no background in group theory can safely skip it and continue reading about the examples of quandles below.

A quandle $Q = (C, *)$ is algebraically connected if the permutation group generated by the left translations $L_a(x) = a * x$ is transitive on C . It is not difficult to prove that colors used in a coloring generate an algebraically connected subquandle [19, Section 5.2], hence, without loss of generality, we can consider only Q -colorings with a connected Q . Such quandles were studied in detail in several papers, the strongest results were obtained recently in [11]. The main theorem states that connected quandles are in 1-1 correspondence to certain configurations in transitive groups: every connected quandle on a set C is uniquely determined by a pair (G, ζ) where G is a transitive group on C and ζ is

a central element of the stabilizer G_e such that $\langle \zeta^G \rangle = G$ (uniqueness up to the choice of e); an isomorphism theorem is available. Using the theory of [11], and a library of transitive groups of degree n , one can easily enumerate all connected quandles of size n up to isomorphism. Currently, such a library is available for $n \leq 47$.

Let us introduce three important classes of quandles.

A quandle $Q = (C, *)$ is called *affine* if there is an abelian group $G = (C, +)$ (informally, an addition on the set of colors) and an automorphism φ such that $a * b = a - \varphi(a) + \varphi(b)$ for every $a, b \in C$ (informally, $*$ is an affine combination of colors). For example, Fox n -coloring uses the affine quandle with $G = \mathbb{Z}_n$ and $\varphi(x) = -x$. An affine quandle is connected if and only if the mapping $x \mapsto x - \varphi(x)$ is onto.

Given a group G and a conjugacy class C in G , then $(C, *)$ with $a * b = aba^{-1}$ is called a *conjugation quandle* over G . Conjugation quandles may or may not be connected.

A quandle is called *simple* if it has no proper homomorphic images (other than itself and the trivial one). Finite simple quandles with $|C| > 2$ are always connected and were characterized in [2,13]: they are either affine, or arise from a finite simple group using a sort of parametrized conjugation operation on its orbit of transitivity; the construction can be used to create a large list of simple quandles. Within the framework of [11] (see the description above), simple quandles are recognized as those where every factor of G is cyclic and the centralizer of ζ is contained in G_e [2]; the message is that it is computationally easy to verify whether a given quandle is simple.

3.3 Colorability and simple quandles

If $\text{col}_Q(K) > 0$, we say that the knot K is *Q-colorable*. Now, Q -colorability is also an invariant, which is easier to calculate than $\text{col}_Q(K)$: one only has to establish that $\text{col}_Q(K) > 0$, whereas the actual number of colorings, $\text{col}_Q(K)$, is often rather big due to the high symmetry of quandles [6], and finding all of them can be computationally costly.

The following observation suggests that if we only care about colorability (and not the actual number of colorings), we can restrict to simple quandles.

Lemma 1. *Let K be a knot which is colorable by a finite quandle Q . Then K is colorable by a finite simple quandle Q' such that $|Q'| \leq |Q|$.*

Proof. Consider a non-trivial coloring f of K by Q . Let Q'' be the subquandle of Q generated by all colors used in the coloring f . Indeed, f is a coloring of K by Q'' . Let α be a maximal congruence of Q'' . Then the factor, $Q' = Q''/\alpha$, is a finite simple quandle (because α is maximal). Consider the composition $f' = \pi \circ f$ where π is the natural projection $Q'' \rightarrow Q'$. Then f' is a non-trivial coloring of K by Q' . Equation (E) follows from the fact that π is a homomorphism: for every crossing as in Figure 2, $f'(\alpha) * f'(\beta) = \pi(f(\alpha)) * \pi(f(\beta)) = \pi(f(\alpha) * f(\beta)) = \pi(f(\gamma)) = f'(\gamma)$. If f' was trivial, then all colors used by f were in one block, B ,

of α . Since congruence blocks are subquandles and Q'' is generated by all such colors, $B = Q''$, hence α was the total congruence $Q'' \times Q''$, a contradiction.

4 Finding a coloring

Given a quandle Q and a knot K , a natural question is “how do we calculate $\text{col}_Q(K)$, the number of non-trivial Q -colorings?” For simplicity, let us focus on the decision problem of Q -colorability: “does there exist a non-trivial Q -coloring of K ?”, i.e. can we decide if $\text{col}_Q(K) > 0$. We will always assume a knot K is presented as a diagram, and we let $|K|$ denote the number of crossings of the diagram.

4.1 Theory

Naturally, this problem is in the complexity class NP: given an assignment of colors to arcs, it is easy to check whether it is a non-trivial Q -coloring. To find a coloring, one has to solve a system of equations over the quandle Q : for every crossing as in Figure 2, we have the equation $x_\alpha * x_\beta = x_\gamma$, where $x_\alpha, x_\beta, x_\gamma$ are variables that determine the colors of the arcs α, β, γ . This can be viewed as an instance of the Constraint Satisfaction Problem (CSP): arcs are variables, Q is the domain, and the equations are the constraints. In general, CSP is an NP-complete problem (SAT is a special instance of CSP). But how hard are the knot coloring instances? In particular, how hard is Q -colorability for a fixed quandle Q ? How hard is Q -colorability for a fixed knot K ?

One can try a simple brute force search: to every one of $|K|$ arcs, assign one of $|Q|$ colors, and check whether this is a non-trivial coloring; we are handling $|Q|^{|K|}$ assignments. For a fixed knot K , this gives a polynomial time algorithm with respect to $|Q|$, but this is impractical for larger knots. Can we do with a better exponent than $|K|$?

Given a braid representation of K , with n strands (the smallest possible n is called the *braid index* of K), the brute force search is only required to assign colors to the initial n arcs, since the colors of the remaining arcs are uniquely determined; hence, we only handle $|Q|^n$ assignments. Whilst this provides a dramatic improvement in practice, the algorithm is still exponential-time with respect to $|K|$ (leaving aside conversion into braid representation). See [6] for a more detailed description and experimental results.

Universal algebra provides a different point of view on coloring. We are solving a system of $|K|$ equations over the quandle Q . The complexity of equation solving over general algebraic structures has been studied extensively. In our case, it follows from general results of Larose and Zádori [16] that the problem of solving a general system of equations over a quandle Q is polynomial-time if and only if Q is affine, and it is NP-complete otherwise. Consequently, colorability by affine quandles (and Fox coloring in particular) is easy. Nevertheless, it does not mean that colorability by non-affine quandles is hard, because the systems of equations arising from knot coloring have a very special form! It is an

interesting open problem whether a polynomial time algorithm for Q -colorability exists for every quandle Q .

We are not aware of any other theoretical results applicable to the complexity of quandle colorings.

4.2 Practice

The only attempt to calculate quandle colorings on a larger scale we know about is reported in [6]. Their implementation was tested on all knots with at most 12 crossings, their performance graph exhibits a fast growth of running time with respect to $|Q|$.

We propose a more efficient approach to knot coloring: a reduction to the Boolean Satisfiability Problem, SAT. Fix a connected quandle $Q = (\{1, \dots, q\}, *)$ and a knot diagram K with $|K| = n$, with arcs numbered $\alpha_1, \dots, \alpha_n$. We consider nq boolean variables $v_{i,c}$ that determine whether the arc α_i has the color c . We need to satisfy the following constraints:

- Every arc has a unique color: the obvious description uses the clauses

$$v_{i,1} \vee \dots \vee v_{i,q} \quad \text{and} \quad \neg v_{i,c} \vee \neg v_{i,d}$$

for every $i = 1, \dots, n$ and $c = 1, \dots, q$, $d = c + 1, \dots, q$.

- Not all arcs have the same color: the obvious description uses, for every $c = 1, \dots, q$, the clause

$$\neg v_{1,c} \vee \dots \vee \neg v_{n,c}.$$

- Crossing equations (E): for every crossing, with a bridge α_i over the strands α_j to the right and α_k to the left, we use q^2 formulas of the form

$$(v_{i,c} \wedge v_{j,d}) \rightarrow v_{k,c*d}.$$

An important ingredient is basic symmetry breaking: since connected quandles are homogeneous, we can assume that the arc α_1 has color 1. (If we were counting the number of colorings, and not just checking colorability, then we could recover $\text{col}_Q(K)$ by multiplying the answer by $|Q|$).

We implemented the procedure, employing a standard SAT-solver MiniSat 1.14. For our experiments, we used the family

SQ. of all 354 simple quandles of size ≤ 47 , indexed in accordance to size,

(the reason is explained in Lemma 1); and the following three families of knots:

12A. all 1288 alternating knots with crossing number 12 (taken from [5]),

T2. $(2, n)$ -torus knots with $n = 11, 21, 31, \dots, 91$,

T3. $(3, n)$ -torus knots with $n = 14, 20, 26, \dots, 98$.

(Torus knots are some of the best known and easiest to implement, potentially infinite, families of knots.) Figures 4-7 present performance graphs with respect to various parameters.

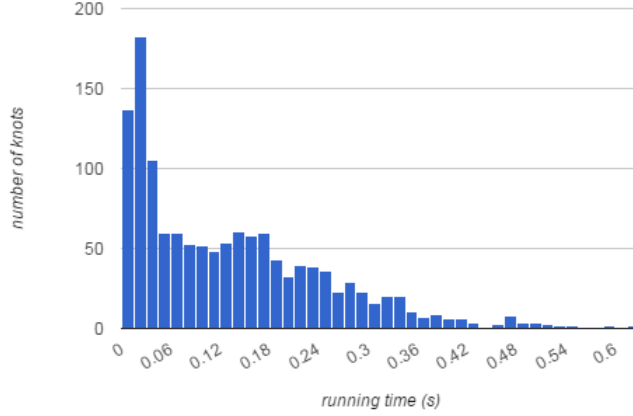


Fig. 4. Distribution of running times (in seconds) for the **12A** family, averaged over all quandles in **SQ**.

First of all, we must stress that neither the number of crossings, nor the braid index, are the most relevant knot parameters with respect to running time. Figure 4 shows the distribution of running times for the family **12A**. Whilst most knots are colored quickly, there are several “slow” knots, with the record being held by the knot with KnotInfo [5] code 12a.1092, see Figure 8. We were unable to identify any possible reason that makes this particular knot harder than others. Also notice the high noisiness of the performance graphs for the $(3, n)$ -torus knots in Figure 5. Yet again, it is not merely the number of crossings that determines the running time.

For the **T3** family, the average running time fluctuates more than the median running time. This suggests that the peaks are caused by a few very long computations, while a “random” coloring job runs relatively fast. For example, for the $(3, 92)$ -torus knot, which is the last but one node on the right graph in Figure 5, the running times for most quandles are no more than a few seconds, but the few exceptions run for a few hundreds of seconds. Perhaps this is an indication that while it is fast to determine Q -colorability on average, it could be hard in the worst case.

Both graphs in Figure 5 suggest that the dependence of median running time with respect to knot size is roughly linear for torus knots. This is not surprising, and probably far from the general case because (k, n) -torus knots have a fixed braid index k , for every n , and so a brute force search in the spirit of [6] runs in linear time with respect to n , by choosing k initial colors and running along the torus producing the remaining coloring values. Nevertheless, in the **T3** case, it seems the SAT solver has a hard time to recognize the braids, and therefore, the running times fluctuate.

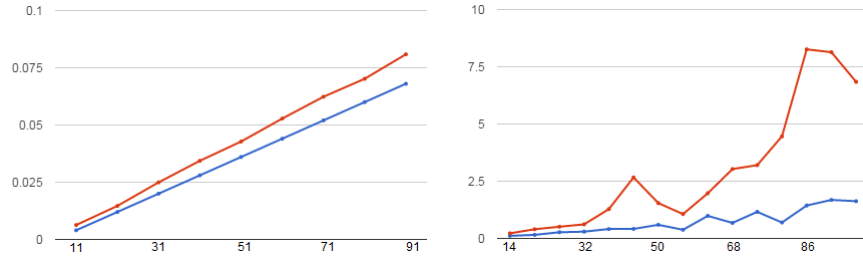


Fig. 5. Average (red, top line) and median (blue, bottom line) running times (s) over all quandles in SQ , with respect to knot size for knots in T_2 (on the left) and T_3 (on the right), respectively.

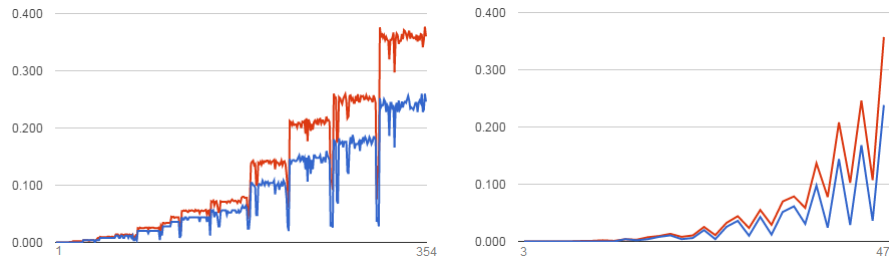


Fig. 6. Average (red, top line) and median (blue, bottom line) running times (s) over knots in $12A$, with respect to quandle index (on the left), and quandle size (on the right), respectively.

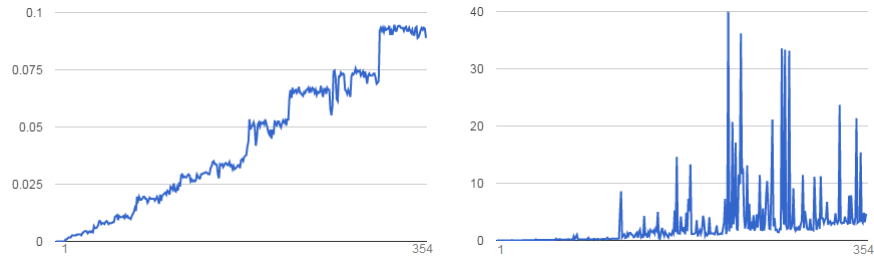


Fig. 7. Average running times (s) over knots in T_2 (on the left) and T_3 (on the right), respectively, with respect to quandle index.

The graphs in Figures 6 and 7 indicate the time complexity with respect to quandle index and quandle size (by index, we mean the position in the list **SQ**). Looking at the lefthand graphs, addressing the **12A** and **T2** knots, we observe a staircase behavior. It tells that quandles of equal size have similar running times. For **12A** knots, we observe occasional deep drops. These are precisely the positions of non-affine quandles, which are, on average, much faster than the affine ones. This is somewhat surprising, since, in theory, non-affine quandles are the harder ones (see Section 4.1). The reason might be a higher symmetry of affine quandles, invisible to MiniSat, together with its inability to employ the fast coloring algorithm.

For **T3** knots (Figure 7, right), the situation is different: the graph is much noisier and the majority of the peaks are at non-affine positions. While non-affine quandles seem faster in “random” cases, they also provide the majority of very long running times.

Observing the growth of running time with respect to quandle index, we see it is somewhat faster than linear, but certainly subquadratic. What about the dependence with respect to quandle size, $|Q|$? Since the number of simple quandles of size n appears to grow roughly linearly with n (this is only an empirical observation based on the family **SQ**, we have no formal arguments yet), we shall add one to the degree. Figure 6 confirms the idea. Since all affine simple quandles have prime power size, and all non-affine simple quandles have size divisible by at least two primes, the right graph reflects the drops and peaks of the left graph.

We can draw the following conclusion. Even a simple implementation, using an obsolete solver and no fine tuning, is competitive, outperforming the brute-force search considerably. Our programs and computation data are available at our website².

5 Recognizing knots and unknots

5.1 Proving inequivalence

Let K_1, K_2 be two knots. If we find a quandle Q such that $\text{col}_Q(K_1) \neq \text{col}_Q(K_2)$ (or, in particular, such that K_1 is Q -colorable and K_2 is not), we can conclude that K_1 and K_2 are not equivalent. Large libraries of connected quandles can be created using the methods described in Section 3.2. For instance, it is feasible to compile the complete list of connected quandles up to size 47, the complete list of conjugation quandles over any group with hundreds of elements, the complete list of affine quandles of any size in the order of thousands.

An interesting experiment is described in [6]. All knots with at most 12 crossings can be distinguished (up to mirror image) using a list of 26 finite quandles, the largest having 182 elements. Most pairs of knots are distinguished using a fairly small quandle, and therefore relatively quickly. More details and other interesting findings can be found in [6].

² <http://www.karlin.mff.cuni.cz/~stanovsk/quandles>

Unfortunately, no upper bound is known for the size of a quandle that distinguishes two inequivalent knots, and it is not even known whether a finite quandle is sufficient. In particular, it is not known whether coloring provides a decision procedure for knot recognition.

5.2 Recognizing unknots

In [8], the first two named authors proposed to use automated theorem proving on knot quandles for unknot recognition, i.e., for the decision of whether a given knot is equivalent to an unknot. Here we present the idea in terms a quandle coloring in a somewhat reshaped manner. The method is based on Theorem 2, which is collected from several works.

Theorem 2. *The following are equivalent for a knot K :*

- (1) K is knotted (i.e., not an unknot).
- (2) There is a quandle Q such that $\text{col}_Q(K) > 0$.
- (3) There is a finite quandle Q such that $\text{col}_Q(K) > 0$.
- (4) There is a finite simple quandle Q such that $\text{col}_Q(K) > 0$.
- (5) There is a conjugation quandle Q over the group $SL(2, p)$, for a prime p , such that $\text{col}_Q(K) > 0$.

The equivalence of (1) and (2) was proved in [12,17]. The equivalence of (2) and (3) was proved in [7]. The equivalence of (3) and (4) follows from Lemma 1. The equivalence of (1) and (5) is a translation of Kuperberg’s certificate of knottedness [14] into the language of quandles (this part of Kuperberg’s result is independent of GRH which is only needed to guarantee that p is small enough). Notice that the implication (2) \Rightarrow (1) follows from Theorem 1: the trivial knot has only one arc, hence admits only trivial colorings; since col_Q is an invariant, so does any unknot.

Theorem 2 turns quandle coloring into a decision procedure for unknot recognition: given a knot on input, we run two independent algorithms (ideally in parallel), one seeking for a certificate of knottedness, the other for unknotting. For knottedness, it is sufficient to find a non-trivial coloring; condition (3) says it is sufficient to consider finite colorings, and conditions (4) and (5) suggest particular families of finite quandles to try. For unknottedness, it is sufficient to *prove* that no non-trivial coloring exists, and automated theorem proving provides a tool to do so.

Detailed experiments with the proposed decision procedure will be reported in a subsequent paper. To certify knottedness, for example, the family **SQ** of simple quandles of size ≤ 47 is sufficient for all **12A** knots and for many larger knots. Certification running times are competitive against state-of-the-art in knot recognition. The unknottedness certification has been tested on various famous “hard unknots” with a positive outcome, see [8] for details.

Efficiency of the knottedness certification heavily relies on efficiency of the coloring procedure used. Nevertheless, for a particular knot, the complexity of the two problems seems to be related only loosely: for example, the slowest knot reported in Section 4.2 is tricolorable (see Figure 8), hence certified very quickly.

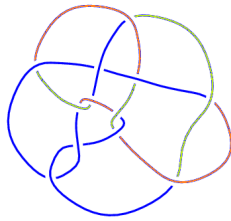


Fig. 8. Tricolored knot with KnotInfo [5] code 12a_1092.

5.3 Classic vs. combinatorial

We believe that many classical results in knot theory can be explained in terms of coloring, perhaps in a more systematic or conceptually cleaner form. A few sample results can be found in [6, Section 7]. A different kind of example has been mentioned earlier in our paper: Kuperberg’s certificate of knottedness is a prime p and a non-commutative representation of the knot group over $SL(2, p)$, which is the same thing as a non-trivial coloring by a conjugation quandle over $SL(2, p)$ (the Wirtinger presentation of the knot group uses arcs as generators and conjugation relations analogous to condition (E) for every crossing).

Here is another, perhaps more important, example. The Alexander invariant is essentially the same thing as coloring by affine quandles. We refer to [3] for a precise statement, and we state formally a result related to Theorem 2.

Theorem 3. *The following are equivalent for a knot K .*

- (1) K has a non-trivial Alexander polynomial.
- (2) There is a finite affine quandle Q such that $\text{col}_Q(K) > 0$.
- (3) There is a finite simple affine quandle Q such that $\text{col}_Q(K) > 0$.

The theorem can be used to considerably improve efficiency of search for inequivalence certificates. Let K_1, K_2 be two knots. First, we calculate their Alexander polynomials Δ_1, Δ_2 (a fast algorithm exists). If $\Delta_1 \neq \Delta_2$, the knots are inequivalent. Else, continue as before. If we only test for Q -colorability (such as in the knottedness certificate described in the previous subsection), we can exclude all affine quandles from the search. This can result in a considerable cut of the search space: for instance, out of the 354 simple quandles with at most 47 elements, only 23 are non-affine.

6 Conclusion

We presented a new approach to knot recognition, based on coloring the arcs of a knot by certain algebraic objects. Unlike most of the classical invariants, finding a coloring is a combinatorial problem, amenable to a (smart) exhaustive search. The coloring method is provably a decision procedure for recognizing unknots,

and works very well in practice for general knot recognition, too. In both cases, most instances of inequivalence are certified very quickly.

The obvious future work is a careful analysis of the parameters of the decision procedure (efficient SAT encoding, choice of the quandle family, heuristics in the spirit of Theorem 3) to improve efficiency of knottedness certification in practice. To extend the method towards general knot recognition, a generalization of Theorem 2 is much needed.

References

1. C. Adams, *The knot book: an elementary introduction to the mathematical theory of knots*. Amer. Math. Soc., 1994.
2. N. Andruskiewitsch and M. Graña, *From racks to pointed Hopf algebras*. Adv. Math. 178/2 (2003), 177–243.
3. Y. Bae, *Coloring Link Diagrams by Alexander Quandles*. J. Knot Theory Ramifications, 21/10 (2012), 1250094.
4. D. Buck, E. Flapan (eds), *Applications of Knot Theory*. Proc. of Symposia in Applied Mathematics, Amer. Math. Soc., 2009.
5. J. C. Cha, C. Livingston, *KnotInfo: Table of knot invariants*. <http://www.indiana.edu/~knotinfo>
6. W. E. Clark, M. Elhamdadi, M. Saito, T. Yeatman, *Quandle colorings of knots and applications*. J. Knot Theory Ramifications 23/6 (2014), 1450035.
7. W. E. Clark, M. Saito, L. Vendramin, *Quandle coloring and cocycle invariants of composite knots and abelian extensions*. <http://arxiv.org/abs/1407.5803>
8. A. Fish, A. Lisitsa, *Detecting Unknots via Equational Reasoning, I: Exploration*. In: Intelligent Computer Mathematics - International Conference, CICM. Lecture Notes in Computer Science 8543 (2014), 76–91.
9. J. Hass, J. Lagarias, N. Pippenger, *The computational complexity of knot and link problems*. J. ACM 46 (1999) 185–211.
10. A. Henrich, L. Kauffman, *Unknotting Unknots*. Am. Math. Monthly, 121/5 (2014), 379–390.
11. A. Hulpke, D. Stanovský, P. Vojtěchovský, *Connected quandles and transitive groups*. To appear in J. Pure Appl. Algebra, <http://arxiv.org/abs/1409.2249>
12. D. Joyce, *Classifying invariant of knots, the knot quandle*. Journal of Pure and Applied Algebra, 1982, 23, 37–65.
13. D. Joyce, *Simple quandles*. J. Algebra 79 (1982), 307–318.
14. G. Kuperberg, *Knottedness is in NP, modulo GRH*. Adv. Math. 256 (2014), 493–506.
15. M. Lackenby, *A polynomial upper bound on Reidemeister moves*. To appear in Annals Math., <http://arxiv.org/abs/1302.0180>
16. B. Larose, L. Zádori, *Taylor terms, constraint satisfaction and the complexity of polynomial equations over finite algebras*. Internat. J. Algebra Comput. 16/3 (2006), 563–581.
17. S. V. Matveev, *Distributive groupoids in knot theory*. Math. USSR - Sbornik 47/1 (1984), 73–83.
18. S. Nelson, *The combinatorial revolution in knot theory*. Notices Amer. Math. Soc. 58/11 (2011), 1553–1561.
19. T. Ohtsuki, *Problems on invariants of knots and 3-manifolds*. In: Geom. Topol. Monogr. 4, 377–572, Geom. Topol. Publ., Coventry, 2002.
20. D. S. Silver, *Knot theory's odd origins*. American Scientist 94 (2006), 158–165.