Automated Reasoning for Tangles with Quantum Verification Applications

Andrew Fish and Alexei Lisitsa

University of Liverpool

SYCO 2024, Birmingham, 15.04.2024

Outline

- Origins: automated reasoning for knotted objects and quantum verification via tangles
- Tangles, Quandles, Pointed Quandles and Automated Reasoning
- Automated proving and disproving for isotopy checking
- Conclusion and Future Work

Origins

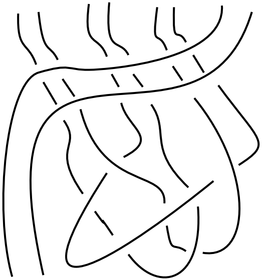
- **Automated reasoning for knots**
  - Andrew Fish and Alexei Lisitsa. *Detecting unknots via equational reasoning, I: exploration.* CICM 2014, LNCS 8543 , pages 76–91, 2014 **FL 2014**
  - Andrew Fish, Alexei Lisitsa, David Stanovsky, and Sarah Swartwood. *Efficient knot discrimination via quandle coloring with SAT and -Sat.* ICMS 2016, LNCS 9725, pages 51–58, 2016 **FLSS 2106**
- **Verification of Quantum programs via Tangles**
  - David J. Reutter and Jamie Vicary. *Shaded tangles for the design and verification of quantum circuits.* Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, 475(2224):20180338, 2019. **RV 2019**

Definition

An *oriented tangle diagram* T is a generic immersion of a union of a finite number of unit intervals and unit circles, in a disc in $\mathbb{R}^2$

A tangle diagram is *ordered* if we have a fixed ordering of the endpoints.

Isotopy respecting ordering of fixed points is a natural equivalence relation on oriented and ordered diagrams

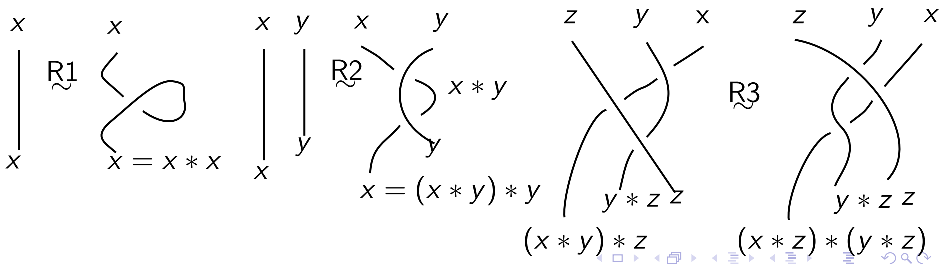


Involutory Quandles

Definition

An involutory quandle is an algebraic structure, that is a set Q with an operation $*$ satisfying the following properties

1. $x * x = x$
2. $(x * y) * y = x$
3. $(x * y) * z = (x * z) * (y * z)$.



Pointed involutory quandles and strong ismorphism

Definition

A pointed involutory quandle $\langle Q, *, a_1, \dots a_n \rangle$ is an involutory quandle $\langle Q, * \rangle$ equipped with a sequence of distinguished elements $a_1, \dots, a_n \in Q$. A pointed involutory quandle $\langle Q, *, a_1, \dots a_n \rangle$ is called *g-pointed* if interpretations of constants $a_1, \dots, a_n$ form a generating set for Q.

Definition

Two pointed involutory quandles $\langle Q_1, *_1, a_1, \dots a_n \rangle$ and $\langle Q_2, *_2, b_1, \dots b_m \rangle$ are strongly isomorphic if $n = m$, $a_i \equiv b_i$ for $i = 1, \dots n$, where $\equiv$ denotes syntactic equality, and there is an involutory quandle isomorphism $i : \langle Q_1, *_1 \rangle \rightarrow \langle Q_2, *_2 \rangle$ such that $i([a_i]) = [b_i]$.

- For a tangle T and a set S, a mapping $c : arc(T) \to S$ is called a *colouring* of T by elements of S.
- With any tangle T and any c of T we can associate an involutory quandle presentation
  $IQ(T, c) = \langle G, R \rangle$ where
  - $G = Im(c)$ is the set of generators determined by the image under c of the set of arcs of T, and
  - R is a set of defining relations, defined as follows. For each crossing t of T, the set R contains a defining relation $a_i * a_j = a_k$, where a_i is the colour of an incoming under-crossing arc of t, a_j is a colour of over-crossing arc of t, and a_k is a colour of outgoing under-crossing arc of t

Fully reduced presentations and end colorable tangles

Fully reduced involutory quandle presentation $IQ^r(T, c)$ **:**

- the generators are distinct colours of external arcs of T;
- the colours of all internal arcs are uniquely determined by involutory quandle operation repeatedly applied to the colours of external arcs.

We make two observations:

- It is not necessarily the case that for every T there exists a fully reduced presentation $IQ^r(T, c)$.
- For a tangle T and a colouring c, $IQ(T, c)$ and $IQ^r(T, c)$ present isomorphic involutory quandles.

Definition

A tangle T is called *end-colourable* if $IQ^r(T, c)$ exists for some c, and *end-coloured* if each end arc has been assigned a colour (which are sufficient to deduce the colours of the rest of the arcs of T).

Proposition

Two $g-$pointed involutory quandles $\langle Q_1, *_1, a_1, \dots a_n \rangle$ and $\langle Q_2, *_2, a_1, \dots a_n \rangle$ given by presentations $\langle G, R_1 \rangle$ and $\langle G, R_2 \rangle$, with $G = \{a_1, \dots, a_n\}$, are strongly isomorphic if and only if

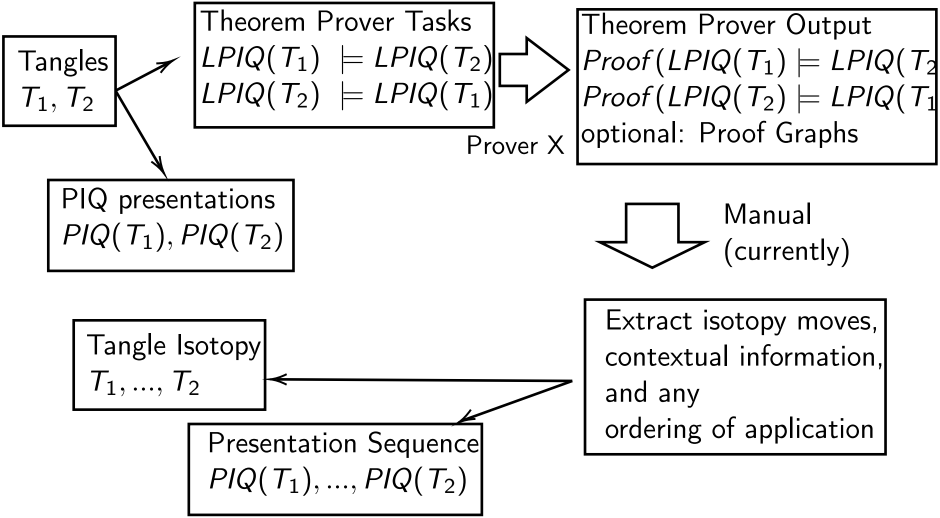
- $AX_{IQ} \cup R_1 \vdash R_2$ *and* $AX_{IQ} \cup R_2 \vdash R_1$.

Proposition

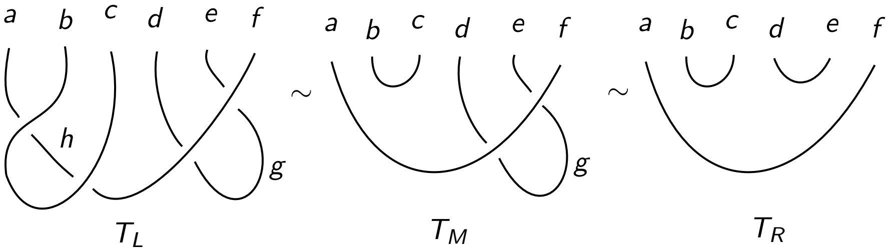
If two ordered and end-coloured tangles $\langle T, e_1, \dots e_{2n} \rangle$ and $\langle T', e'_1, \dots e'_{2n} \rangle$ are isotopic then the $g-$pointed involutory quandles presented by $IQ^r(T, c)$ and $IQ^r(T', c')$ are strongly isomorphic.

Thus, Proposition 2 associates the checking of isotopy of end-coloured tangles to the checking of strong isomorphism of associated pointed involutory quandles, which taken together with Proposition 1, further reduces it to automated reasoning tasks.

General Methodology



Detailed worked example (RV 2019)

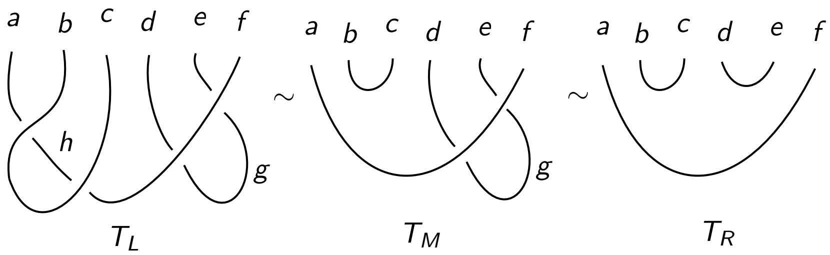


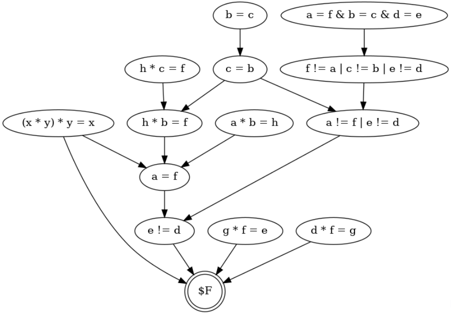
$\sim$ $\sim$

```
%Assumptions arising from $T_L$.
a*b=h.
h*c=f.
b=c.
d*f=g.
g*f=e.
```

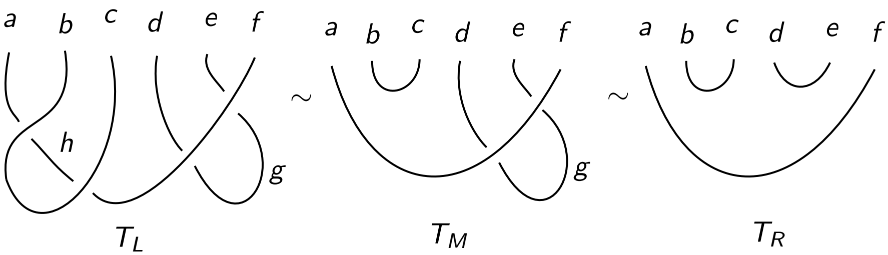
```
% Involutory quandle axioms
x * x = x.
(x * y) * y = x.
(x * y) * z = (x * z) * (y * z).

%Goals arising from $T_R$.
a=f & b=c & d=e.
```

Proof graph and Reidemeister Moves





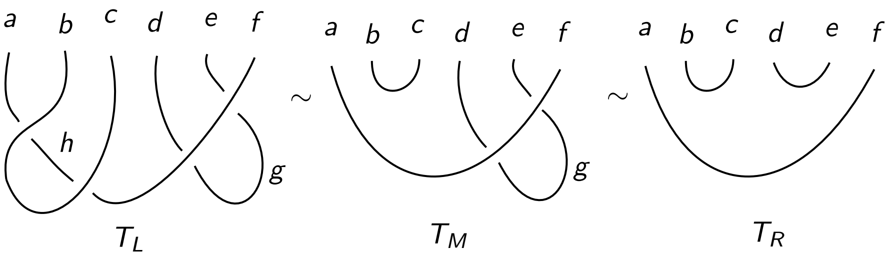
The same example, End-label encoding

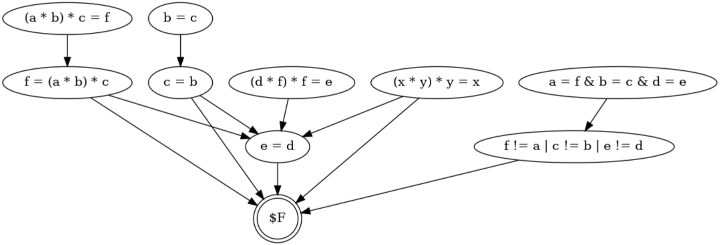


ProverX, $\Rightarrow$

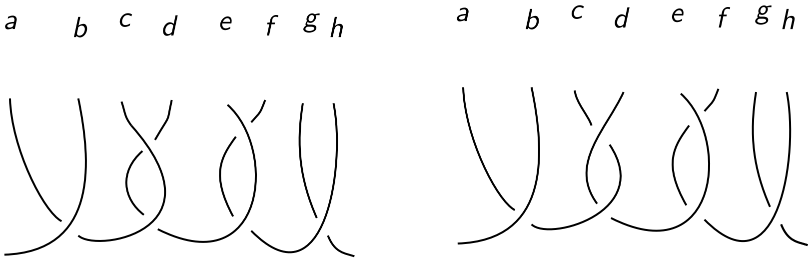
```
1 a = f & b = c & d = e # label(non_clause) # label(goal).  [goal].
3 (x * y) * y = x.  [assumption].
6 (a * b) * c = f.  [assumption].
8 b = c.  [assumption].
10 (d * f) * f = e.  [assumption].
```

Proof graph and RMs





Disproving for non-isotopy

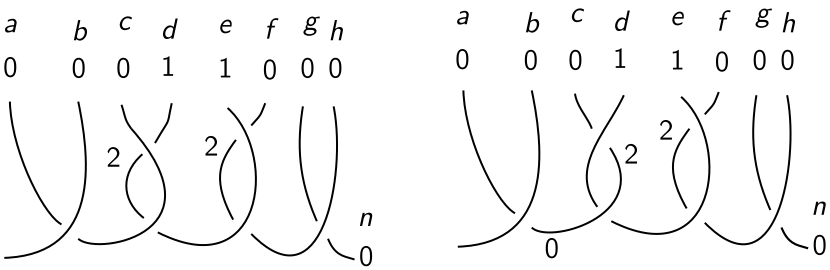


(RV 2019)

Task:

$$a * b = c \wedge (d * c) * c = e \wedge (f * e) * e = h \wedge b = m \wedge g * h = n$$

$$\nvdash \ (a * b) * d = c \wedge d * (a * b) = e \wedge (f * e) * e = h \wedge b = m \wedge g * h = n$$



Mace4:

```
interpretation( 3, [number = 1,seconds = 0], [
    function(*(_,_), [
        0,0,0,
        2,1,1,
        1,2,2]),
    function(a, [0]), function(b, [0]), function(c, [0]),
    function(d, [1]), function(e, [1]), function(f, [0]),
    function(g, [0]), function(h, [0]), function(m, [0]), function(n, [0])]
```

Conclusions & Future work

- Automated reasoning can assist in establishing isotopy of tangles (theorem proving)
- Automated reasoning can be used to show non-isotopy of tangles (theorem disporving)
- Taking tangle abstraction of quantum programs/circuits AR can be used for verification

Conclusions & Future work

- Automated reasoning can assist in establishing isotopy of tangles (theorem proving)
- Automated reasoning can be used to show non-isotopy of tangles (theorem disporving)
- Taking tangle abstraction of quantum programs/circuits AR can be used for verification
- Future work
  - automation of RMs extraction from proofs
  - characterisation of when proofs guarantee isotopy
  - are finite countermodels always sufficient to show non-isotopy?

Thank you! Any questions?