Legendrian Knots and First Order Theorem Provers

T. V. H. Prathamesh (Joint work with Dheeraj Kulkarni)

15-11-2017

Background

Background

- Automated theorem provers, especially the first-order logic based theorem provers, are usually used to prove or negate mathematical statements.

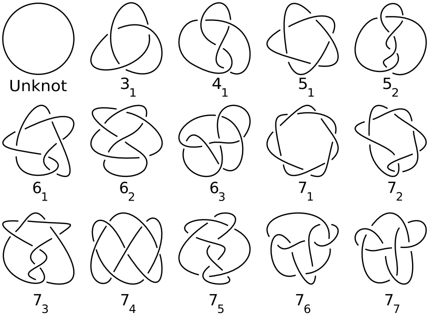
Background

- Automated theorem provers, especially the first-order logic based theorem provers, are usually used to prove or negate mathematical statements.
- In this talk, we look at how they proved effective in constructing a new topological invariant called Legendrian racks.

Background

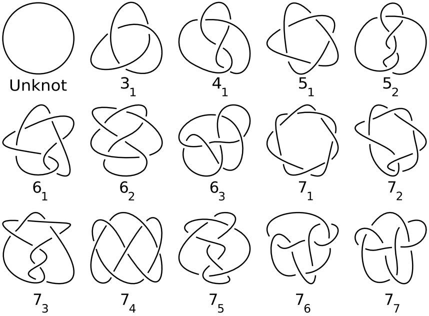
- Automated theorem provers, especially the first-order logic based theorem provers, are usually used to prove or negate mathematical statements.
- In this talk, we look at how they proved effective in constructing a new topological invariant called Legendrian racks.
- Legendrian racks are an invariant of Legendrian knots, an object of study in contact topology.

Knot



(Image source: Wikipedia)

Knot



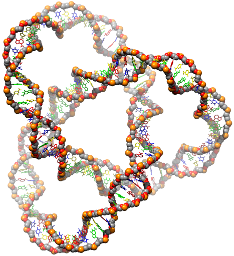
(Image source: Wikipedia)

Definition (Formal Definition)

A knot K is the image of a smooth, injective map $h : S^1 \to \mathbb{R}^3$ such that, $h'(\theta) \neq 0$ for all $\theta \in S^1$.

Why study knots

DNA Structures



Quantum Knots

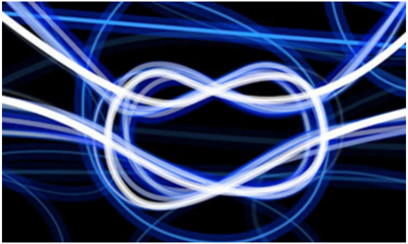
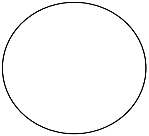


Image source(s): thinglink.com, edx.org

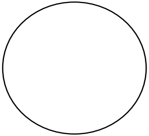
Question: **What do we study about knots?**

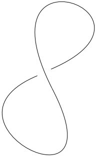
When are two knots (or links) regarded as same or different?

When are two knots (or links) regarded as same or different?

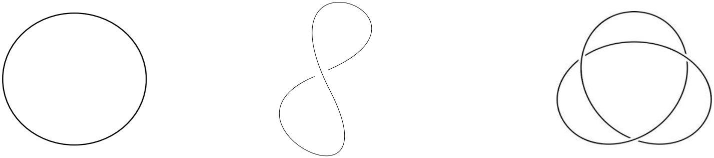


When are two knots (or links) regarded as same or different?

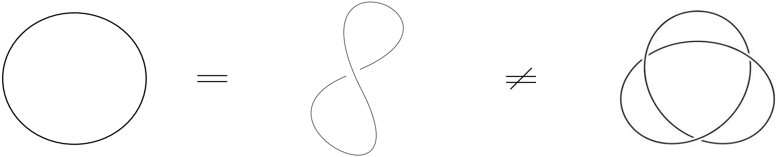




When are two knots (or links) regarded as same or different?



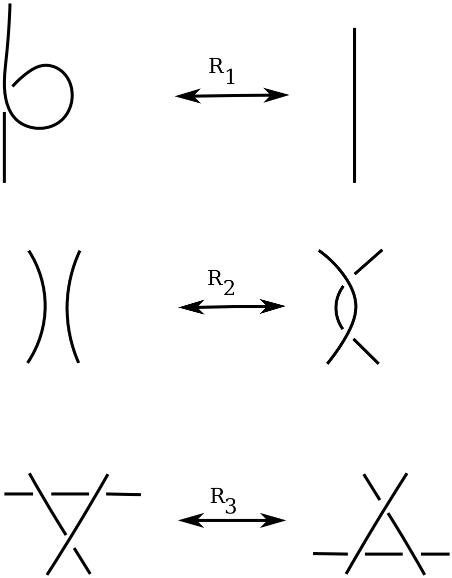
When are two knots regarded as same or different?



Knot Equivalence

- Two knots are said to be the same if one can be obtained from another without involving any cutting and pasting.
- The formal definition is in terms of 'ambient isotopy'.
- In practise, we use a 'combinatorial' version of equivalence, called Reidemeister moves.

Reidemeister moves



How do show in/equivalence of two knots?

- Run a knot recognition algorithm.
  - Drawbacks: Complexity is exponential in number of crossings and very few implementations available.
- Compute an invariant. If the values differ, they are different.
  - Drawback: Already tried for most cases. Complexity bounds of the difficult invariants are not reliably known.
- Use an automated theorem prover [Fish, Lisista (2014)].
  - Drawback: Early stages of research, no new results have been derived using this method.

How does one achieve the above for knots?

Topological Objects

Quandles

Combinatorial/Algebraic Structures

How does one achieve the above for knots?

Topological Objects

↓ Quandles

Combinatorial/Algebraic Structures

↓ First Order Logic

Automated Theorem Provers

Some definitions

- Left Self Distributivity:
  $\forall x.\forall y.\forall z.\ (x * y) * z = (x * z) * (y * z)$.
- Left Inverse: $\forall y.\forall z.\exists! x.\ z = (x * y)$.
- Idempotence: $\forall x.\ x * x = x$.

Some definitions

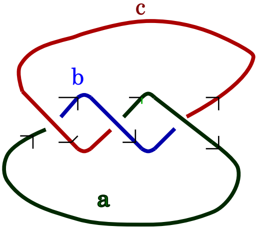
- Left Self Distributivity:
  $\forall x.\forall y.\forall z.\ (x * y) * z = (x * z) * (y * z)$.
- Left Inverse: $\forall y.\forall z.\exists! x.\ z = (x * y)$.
- Idempotence: $\forall x.\ x * x = x$.

Definition

- A **rack** $(R, *)$ is a model of the left self distributive and left inverse axioms.
- A **quandle** is an idempotent rack.
- **Remark:** We can use z/y to denote x in the left inverse axiom.

Knots and Quandles

Knot



- $a * c = b$.
- $b * a = c$.
- $c * b = a$.

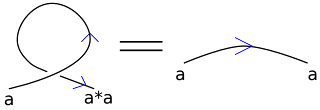
Quandle

- $(S, *)$.
- Generators: Strands.
- Generating Relations: Crossings.
- $(S, *)$:
  1. Closed under $(*)$.
  2. Left self-distributive.
  3. Left inverse property.
  4. Idempotent

Knots and Quandles

Knot

- Left self distributivity to third Reidemeister move.
- Left inverse corresponds to second Reidemeister move.
- Idempotence corresponds to third Reidemeister move.



Quandle

- $(S, *)$.
- Generators: Strands.
- Generating Relations: Crossings.
- $(S, *)$:
  1. Closed under $(*)$.
  2. Left self-distributive.
  3. Left inverse property.
  4. Idempotent

Automated Theorem Proving and Quandles

- The quandle corresponding to the unknot is the trivial quandle.
- Checking if a given knot is an unknot, equals checking triviality of the quandle.
- This can be achieved by an ATP for FOL.

Dheeraj asked:

Question: Can Automated theorem provers help distinguish Legendrian knots?

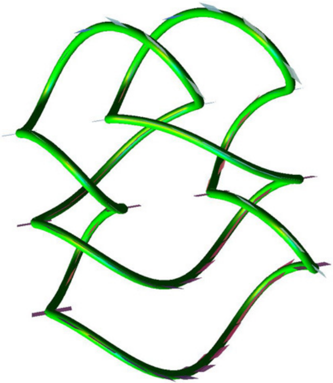


Image Source: Lenny Ng

Legendrian Knots

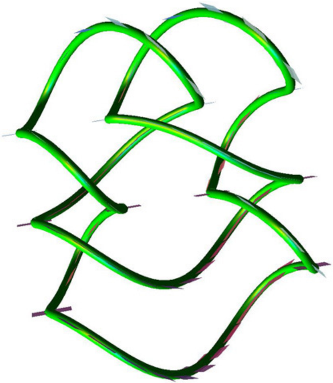


Image Source: Lenny Ng

- Legendrian knots occur in contact geometry.

Legendrian Knots

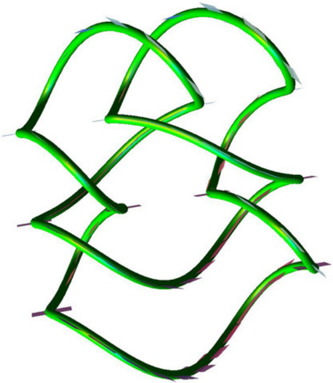


Image Source: Lenny Ng

- Legendrian knots occur in contact geometry.
- They help distinguishing geometric structures called contact manfolds.

Legendrian Knots

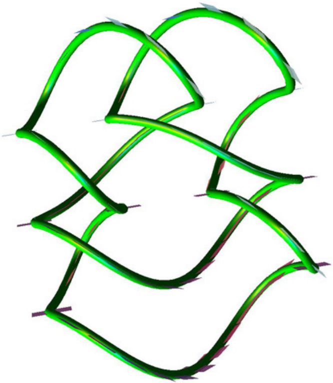


Image Source: Lenny Ng

- Legendrian knots occur in contact geometry.
- They help distinguishing geometric structures called contact manfolds.
- Contact manifolds arise out of optics and related PDE's.

Legendrian Knots

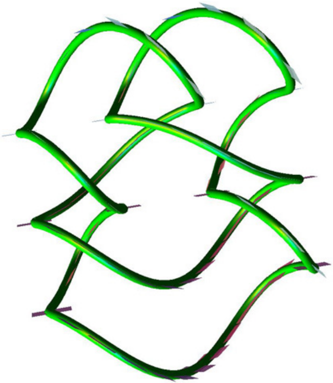


Image Source: Lenny Ng

- Legendrian knots occur in contact geometry.
- They help distinguishing geometric structures called contact manfolds.
- Contact manifolds arise out of optics and related PDE's.
- They are odd dimensional analogues of 'symplectic manifolds'.

Legendrian Knots

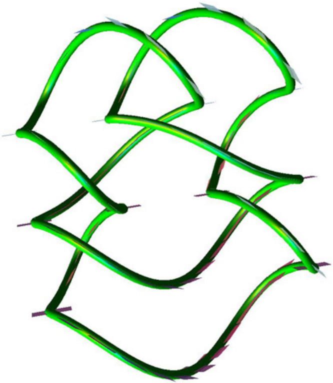
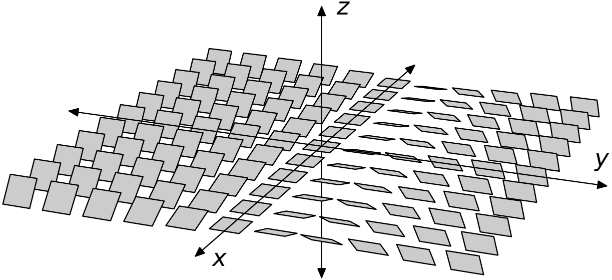


Image Source: Lenny Ng

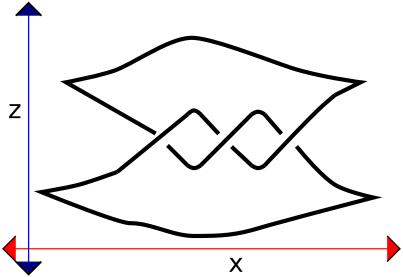
- Legendrian knots occur in contact geometry.
- They help distinguishing geometric structures called contact manfolds.
- Contact manifolds arise out of optics and related PDE's.
- They are odd dimensional analogues of 'symplectic manifolds'.
- Legendrian knots can be understood as knots with conditions on tangency.

Standard Contact Form on $\mathbb{R}^3$

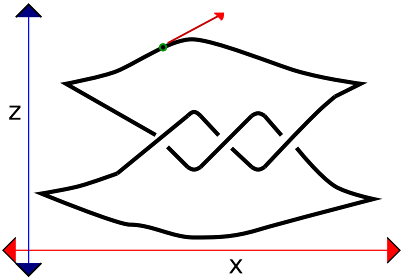
- Point : $(x,\ y,\ z)$
- Embedded Plane: $\{(u,\ v,\ y \cdot u) \mid u, v \in \mathbb{R}\}$



Only admissible paths in such a space, are those whose tangents at each lie in the associated embedded plane.

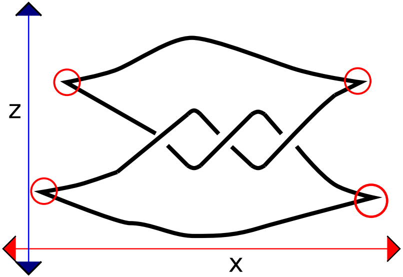


- $y = dz/dx$.
- No vertical tangencies in the front projection.
- Vertical tangencies are replaced by cusps.
- Only one kind of crossing is present.
- Knot Eq $\prec_{weaker}$ Legendrian knot Eq.



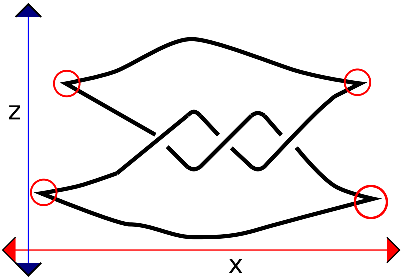
- $y = dz/dx$.
- No vertical tangencies in the front projection.
- Vertical tangencies are replaced by cusps.
- Only one kind of crossing is present.
- Knot Eq $\prec_{weaker}$ Legendrian knot Eq.

Legendrian Knots



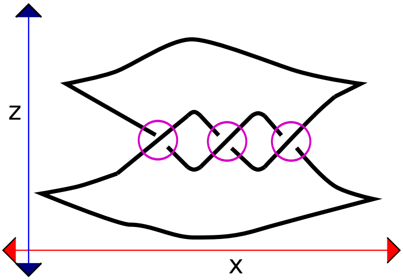
- $y = dz/dx$.
- No vertical tangencies in the front projection.
- Vertical tangencies are replaced by cusps.
- Only one kind of crossing is present.
- Knot Eq $\prec_{weaker}$ Legendrian knot Eq.

Legendrian Knots



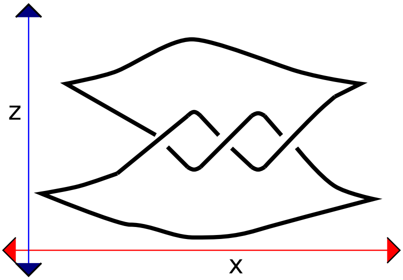
- $y = dz/dx$.
- No vertical tangencies in the front projection.
- Vertical tangencies are replaced by cusps.
- Only one kind of crossing is present.
- Knot Eq $\prec_{weaker}$ Legendrian knot Eq.

Legendrian Knots



- $y = dz/dx$.
- No vertical tangencies in the front projection.
- Vertical tangencies are replaced by cusps.
- Only one kind of crossing is present.
- Knot Eq $\prec_{weaker}$ Leg knot Eq.

Legendrian Knots



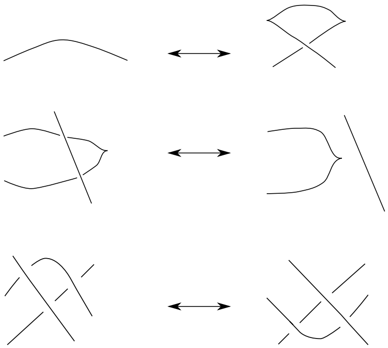
- $y = dz/dx$.
- No vertical tangencies in the front projection.
- Vertical tangencies are replaced by cusps.
- Only one kind of crossing is present.
- Knot Eq $\prec_{weaker}$ Legendrian knot Eq.

When are two Legendrian knots *same*?

- Equivalence between Legendrian knots is formally defined in terms of *Legendrian isotopy*. The definition involves derivatives and ambient isotopy.

- It can be pictorially understood using Legendrian Reidemeister moves.

Legendrian Reidemeister moves

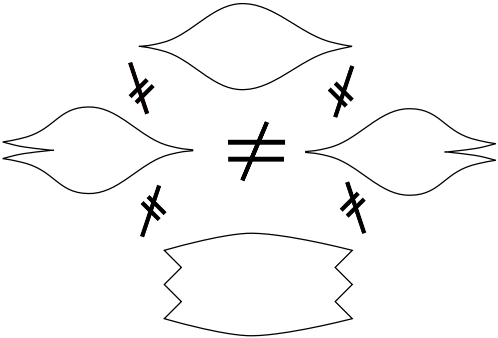


Legendrian knots and knots

- Legendrian knot equality $\Rightarrow$ knot equality
- The converse **does not** hold true

Legendrian knots and knots

- Legendrian knot equality $\Rightarrow$ knot equality
- The converse **does not** hold true



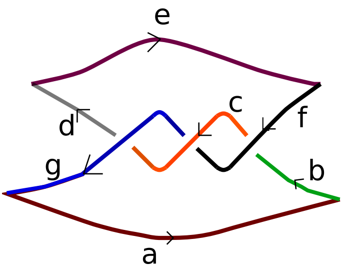
Distinguishing Legendrian Knots

- Few knot invariants: Chekanov DGA, Rotation number, Tb number Et Al.
- Some of them can be computed using regular computer programs. Though not sufficiently high number of Legendrian knots are classified.
- However, none of these invariants are implementable in an Automated Theorem Prover.

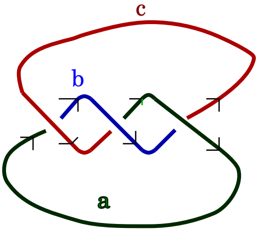
Motivating Task: To find quandle like invariants of Legendrian knots.

We discovered such a class of invariants, which we call Legendrian racks.

Legendrian Knot

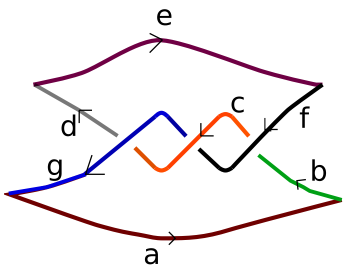


(Classical) Knot



Legendrian Knots and Legendrian Racks

Legendrian Knot



- $b * f = c$.
- $b = a^{n+1}$.

Legendrian racks

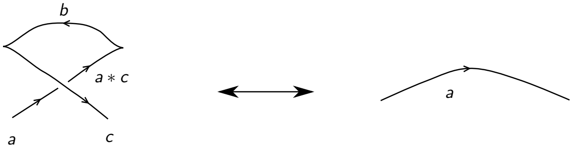
- $\{(LR_n, *)\}$
- Generators: Strands.
- Generating Relations: Crossings + Cusps.
- $(LR_n, *)$:
  1. Closed under $(*)$.
  2. Left self-distributive.
  3. Left inverse property.
  4. $\forall x.\ x^{(2n+2)} = x$.

How did we discover it

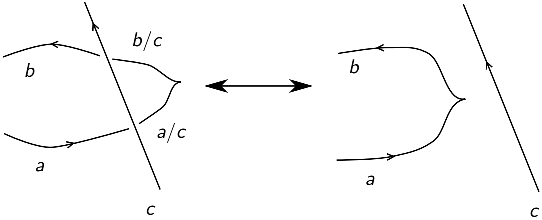
How did we discover it

Legendrian Reidemeister moves were formalized as first-order logic axioms in the language - $(*, /, U, D)$.

Legendrian Reidemeister moves were formalized as first-order logic axioms in the language - $(*, /, U, D)$.



$$U(a * c, b) \wedge D(b, c) \longleftrightarrow (a = c) \wedge (b = c)$$



$$U(a, b) \longleftrightarrow U(a/c, b/c)$$

A note on the axioms

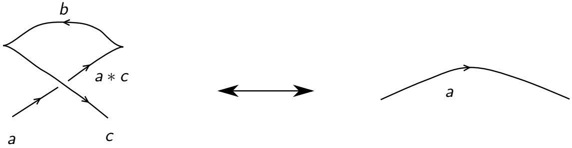
- To each Legendrian knot, we associate the canonical model of these axioms.
- These axioms consisted of rack axioms + axioms for Legendrian Reidemeister moves. The idempotence axioms does not hold true.
- The third Legendrian Reidemeister move does not involve predicates and follows from the rack axioms.
- There were a net total of 18 axioms to account for various geometric possibilities.

We ran a few experiments on Prover9, to check the following facts:

- $U(a, b) = D(a, b)$
- $U(a, b) \longrightarrow (a = b)$.

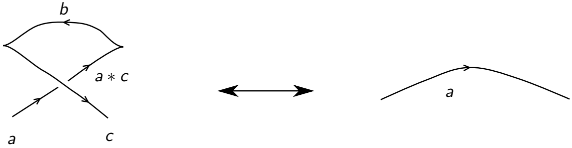
Both of these returned TRUE, which implies that the structure did not detect 'cusps'.

Revisiting axioms



$$U(a * c, b) \wedge D(b, c) \iff (a = c) \wedge (b = a^{\square})$$

Revisiting axioms

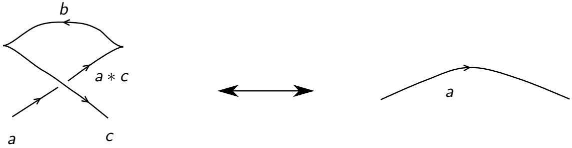


$$U(a * c, b) \wedge D(b, c) \iff (a = c) \wedge (b = a^{\square})$$

New axiom (schema):

$$U_n(a * c, b) \wedge D_n(b, c) \iff (a = c) \wedge (b = a^n)$$

Revisiting axioms



$$U(a * c, b) \wedge D(b, c) \iff (a = c) \wedge (b = a^{\square})$$

New axiom (schema):

$$U_n(a * c, b) \wedge D_n(b, c) \iff (a = c) \wedge (b = a^n)$$

The experiments were repeated for values of $n = 1, ..., 10$.

Results

- $U_n(a, b) = D_n(a, b)$.
- $U_n(a, b) \longrightarrow (a = b)$.

Results

- $U_n(a, b) = D_n(a, b)$.
- $U_n(a, b) \longrightarrow (a = b)$.

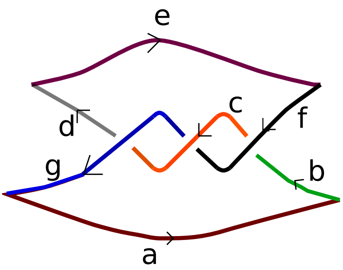
Results and observations:

- The first case always returned TRUE. Thus orientation is not detected.
- The second case was FALSE, except when n is of the form 2^k.

Experiment: $U_n(a, b) \wedge D_n(b, a) \implies b = a$.

- Above holds true for all tested n.
- In the proof, we noticed the following result $U_n(a, b) \longleftrightarrow (b = a^n)$.
- By carefully going through proofs for values of n, we were able to extract general proofs of the above results $\forall n \in \mathbb{N}$.
- We subsequently reworked the axioms by substituting for $U_n(a, b)$.

Legendrian Knot



- $b * f = c$.
- $b = a^{n+1}$.

Legendrian racks

- $\{(LR_n, *)\}$
- Generators: Strands'.
- Generating Relations: Crossings + Cusps.
- $(LR_n, *)$:
  1. Closed under $(*)$.
  2. Left self-distributive.
  3. Left inverse property.
  4. $\forall x.\ x^{(2n+2)} = x$.

Quandles and Legendrian Racks

`Quandles`

- Generators: Strands.
- Generating Relations: Crossings.
- $(S, *)$:
  1. closed under $(*)$.
  2. Left self-distributive.
  3. Left inverse property.
  4. Idempotent
- $K \to (Q(K), *)$.
- Comlete invariant.

`Legendrian Racks`

- Generators: Strands'.
- Generating Relations: Crossings + Cusps.
- $(LR_n, *)$:
  1. Closed under $(*)$.
  2. Left self-distributive.
  3. Left inverse property.
  4. $\forall x.\ x^{(2n+2)} = x$.
- $LK \to \{(LR_n(LK), *)\}_{n \in \mathbb{N}}$.
- Not a comlete invariant.

Quandles and Legendrian Racks

Quandles

- Generators: Strands.
- Generating Relations: Crossings.
- $(S, *)$:
  1. closed under $(*)$.
  2. Left self-distributive.
  3. Left inverse property.
  4. Idempotent
- $K \rightarrow (Q(K), *)$.
- Complete invariant.

Legendrian Racks

- Generators: Strands'.
- Generating Relations: Crossings + Cusps.
- $(LR_n, *)$:
  1. Closed under $(*)$.
  2. Left self-distributive.
  3. Left inverse property.
  4. $\forall x.\ x^{(2n+2)} = x$.
- $LK \rightarrow \{(LR_n(LK), *)\}_{n\in\mathbb{N}}$.
- Invariant, but not a complete invariant.

Proof of invariance

Theorem

For each $n \in \mathbb{N}$, LR_n is an invariant of Legendrian rack moves.

Proof.

Check for each Legendrian Reidemeister move. We get a set of identities, which are proved by a combination of induction and symbolic computations. □

Remark

Most of the proofs obtained again involved using automated theorem provers for specific cases, and then subsequently generalized the automatically generated proofs.

Detecting different Legendrian unknots

Input: Generating relations of various Legendrian unknots.
Conjecture: Triviality of the rack LR_n.

Output: Finite model counterexamples were generated, when number of strands did not equal 2^k, and for values of LR_n, where $(n, s_L) > 1$ (s_L is the minimum number of strands).

The finite models generated on closer look, revealed a pattern:

- There was a link between values of n, for which counterexamples were generated, and number of strands.
- Cardinality of the models was always a prime number..
- They were equal to a known example of racks, called the coloring racks $\{(C_n, *)\}$.
- Cardinality related to a known invariant called the Thurston-Bennequin number, tb.

Classifying Legendrian unknots

Theorem

If two Legendrian knots have the same tb number, each n-Legendrian rack is isomorphic.

Theorem

Given two Legendrian unknots L_1 and L_2 , such that there exists an odd prime p and $k \in \mathbb{N}$, such that:

- $p^k | tb(L_1)$,
- $p^k \not| tb(L_2)$,

then $\exists n.\ LR_n(L_1) = LR_n(L_2)$.

Proof.

There exists a surjective homomorphism in the first instance to C_{p^k}, which does not hold true in the second case. □

Further Questions

- As of yet, little is known about these invariants in more general cases..
- Is the word problem decidable in a Legendrian rack?
- Is the isomorphism problem decidable?
- Term rewriting related questions: Existence of unique normal forms, completion...
- Relationship with other known invariants, for more general cases.

Thank You