Proceeding of

The 5th Mini Workshop on Knot Theory

edited by
Byung Hee An

July 2020

Preface

The 5th Mini Workshop on Knot theory was held at *Maison Glad Jeju* in the beautiful Jeju island, Korea from July 19 to 23. There were 18 participants from all around Korea including Seoul, Daegu, Pohang, Jeonju, Gyeongju and Jeju. Most of the participants are in early career such as students, post-docs, and assistant professors.

The academic program consisted of two lecture series of three talks given by Youngjin Bae at KIAS and Seungsang Oh at Korea University, and six individual lectures. Among these twelve lectures, this proceeding contains eleven articles which are either full paper versions or extended abstracts, and one presentation slide.

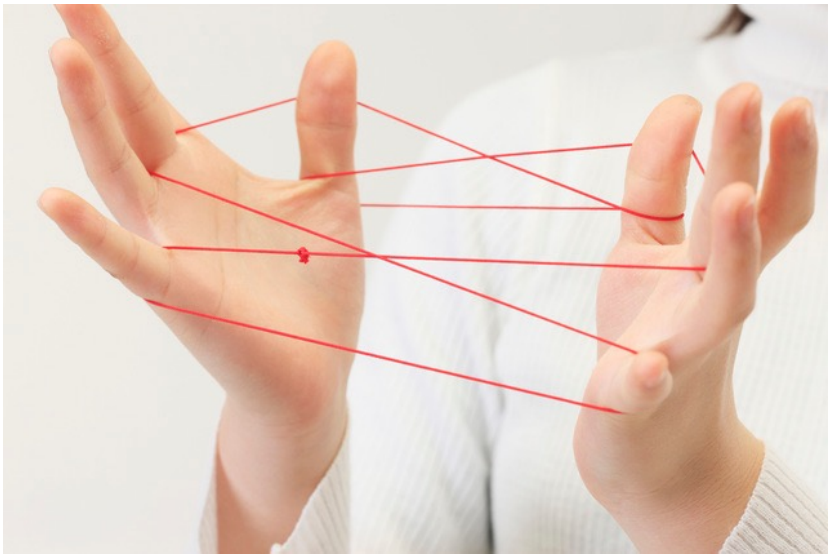
The workshop was mainly supported by National Research Foundation of Korea, the mid-career researcher programs, 'Legendrian, Fukaya category, and Mirror symmetry' led by Byung Hee An and Youngjin Bae, and 'Research on arc presentations of knots and its applications' led by Hwa Jeong Lee. The workshop was also partly supported by the Conference Supporting Program of Kyungpook National University.

Last but not least, we thank all participants and speakers for making the workshop a great success. We hope this workshop will continue in future.

July 31, 2020
Byung Hee An

The 5th Mini Workshop on Knot Theory

July 19 – 23, 2020



Minicourse Lectures

Youngjin Bae | KIAS

Seungsang Oh | Korea University

Invited Speakers

Youngjin Cho | KAIST

Hyoungjun Kim | Ewha Womans University

Jung Hoon Lee | Jeonbuk National University

Sungjong No | Kyonggi University

Minkyoung Song | IBS-CGP

Hyungkee Yoo | Korea University

Organizers

Byung Hee An | Kyungpook National Univ.

Hwa Jeong Lee | Dongguk Univ. - Gyeongju

Contact

anbyhee@knu.ac.kr
hjwith@dongguk.ac.kr
https://geometry.knu.ac.kr/conferences/MWKnot/

Venue

Maison Glad Jeju, Jeju, Korea

KNU KYUNGPOOK NATIONAL UNIVERSITY

NRF National Research Foundation of Korea

dongguk UNIVERSITY gyeongju

Table of Contents

Preface iii

Workshop Poster v

Table of Contents vii

List of Organizers ix

List of Participants xi

Part 1. Series Lectures 1

Lecture 1. Introduction to Legendrian knot theory 3
Contact manifolds, Legendrian submanifolds, and their classical invariants
Youngjin Bae 3
Non-classical invariant of Legendrian knots and their computations I
Youngjin Bae 9
Non-classical invariant of Legendrian knots and their computations III
Youngjin Bae 15

Lecture 2. Mathematics in Blockchains 19
Mathematics in Blockchains I
Seungsang Oh 19
Mathematics in Blockchains II
Seungsang Oh 23
Mathematics in Blockchains III
Seungsang Oh 27

Part 2. Individual Lectures 31

Invited Talks 33
The structure of automorphism groups of CLTTF Artin groups
Youngjin Cho 33
Bipartite intrinsically knotted graphs with 23 edges
Hyungjun Kim*, Thomas Mattman and Seungsang Oh 41
Primitive disks and intersection pattern
Sangbum Cho, Yuya Kora and Jung Hoon Lee* 49
Stick numbers of Montesinos knots
Hwa Jeong Lee, Sungjong No* and Seungsang Oh 57
Lower central series and homology cylinders
Minkyoung Song 63
Minimally knotted spatial cubic graphs with two vertices
Hyungkee Yoo 69

Commemorative Photographs 77

List of Organizers

The 5th Mini Workshop on Knot Theory

Maison Glad Jeju, Jeju, Korea
July 19 – 23, 2020

Organizers

- Byung Hee An (Kyungpook National University)
- Hwa Jeong Lee (Dongguk University-Gyeongju)

Sponsered by

- Department Of Mathematics Education, Kyungpook National University
- Department Of Mathematics Education, Dongguk University-Gyeongju
- National Research Foundation of Korea
  - Grant No. : 2019R1A2C1005506
  - Grant No. : 2020R1A2C1A01003201

List of Participants

Byung Hee An 안병희	Kyungpook National University anbyhee@knu.ac.kr
Youngjin Bae 배영진	Korea Institute for Advanced Study yjbae@kias.re.kr
Youngjin Cho 조영진	Korea Advanced Institute of Science and Technology y_cho@kaist.ac.kr
Hyungjun Kim 김형준	Ewha Womans University kimhjun@ewha.ac.kr
Seonjung Kim 김선중	Korea University todndi88@korea.ac.kr
Sungwoon Kim 김성운	Jeju National University sungwoon@jejunu.ac.kr
Hwa Jeong Lee 이화정	Dongguk University-Gyeongju hjwith@dongguk.ac.kr
Jung Hoon Lee 이정훈	Jeonbuk National University junghoon@jbnu.ac.kr
Sangyop Lee 이상엽	Chung-Ang University sylee@cau.ac.kr
Sungjong No 노성종	Kyonggi University sungjungno@kgu.ac.kr
Sangrok O 오상록	Korea Advanced Institute of Science and Technology tossnight@gmail.com
Seungsang Oh 오승상	Korea University seungsang@korea.ac.kr
Hyowon Park 박효원	Handong University park.hyowon@gmail.com
Juno Seo 서준호	Korea Advanced Institute of Science and Technology juno19@kaist.ac.kr
Minkyoung Song 송민경	Institute for Basic Science, Center for Geometry and Physics mksong@ibs.ac.kr
Seungyeop Yang 양승엽	Kyungpook National University seungyeop.yang@knu.ac.kr
Byungyong Yoo 유병용	Korea University yugane1211@korea.ac.kr
Hyungkee Yoo 유형기	Korea University lpyhk727@korea.ac.kr

Part 1

Series Lectures

LECTURE 1

Introduction to Legendrian knot theory

CONTACT MANIFOLDS, LEGENDRIAN SUBMANIFOLDS, AND THEIR CLASSICAL INVARIANTS

YOUNGJIN BAE

Abstract. Legendrian knot theory naturally arise in the study of submanifolds in a 3-dimensional contact manifold. The theory has its own interest of classification and geography. Moreover, it plays an essential role in the study of 3-dimensional contact manifold, construction of 4-dimensional Weinstein manifold and give a new relation to the smooth knot theory. We start the Legendrian knot theory by investigating the classical Legendrian knot invariants.

In the second part, we study Legendrian singular links up to contact isotopy. Using a special property of the singular points, we define the singular connected sum of Legendrian singular links. This concept is a generalization of the connected sum and can be interpreted as a tangle replacement, which provides a way to classify Legendrian singular links. Moreover, we investigate several phenomena only occur in the Legendrian setup.

Legendrian knots have been a prominent part of three dimensional contact topology for a long time. All contact manifolds can be constructed from the standard contact structure on S^3 through Legendrian knot surgery operations. Legendrians distinguish contact structures: for example the famous tight versus overtwisted dichotomy can be interpreted in terms of Legendrian knots. A fundamental problem in the theory of Legendrian knots is the classification problem: completely characterize Legendrian knots up to the natural equivalence relation, Legendrian isotopy. This is finer than the classification of smooth knots, as follows from the existence of two "classical" invariants of Legendrian knots, the Thurston–Bennequin number, tb and rotation number, rot.

Throughout this article, we consider Legendrian knots in the standard contact 3-manifold $(\mathbb{R}^3, \xi = \ker(dz - ydx))$. A knot $\Lambda : S^1 \to \mathbb{R}^3$ is called *Legendrian* if $T_p\Lambda \in \xi_p$ for all $p \in \Lambda$.

By the Legendrian condition it is enough to know two coordinates among three coordinates. There are two famous and meaningful projections, the front and Lagrangian projection:

$$\pi_{\mathrm{F}} : \mathbb{R}^3 \to \mathbb{R}^2 : (x, y, z) \mapsto (x, z);$$
$$\pi_{\mathrm{L}} : \mathbb{R}^3 \to \mathbb{R}^2 : (x, y, z) \mapsto (x, y).$$

We are interested in equivalence classes of Legendrian knots under Legendrian isotopy, which means smooth isotopy through Legendrian knots. This Legendrian isotopy can be interpreted as Reidemeister moves I, II, and, III in the front projection as depicted in Figure 1. The classical invariants can be computed in a combinatorial way in terms of the front projection:

$$tb(\Lambda) = \#\{\diagup\!\diagdown, \diagdown\!\diagup, \} - \#\{\diagup\!\diagdown, \diagdown\!\diagup, >\};$$
$$rot(\Lambda) = \frac{1}{2}\left(\#\{<, >\} - \#\{<, >\}\right).$$

A Legendrian singular link of degree m with n-component is the image of an immersion of n-copies of S^1 into S^3 whose tangent vectors are contained in the contact structure (S^3, ξ_{std}) which

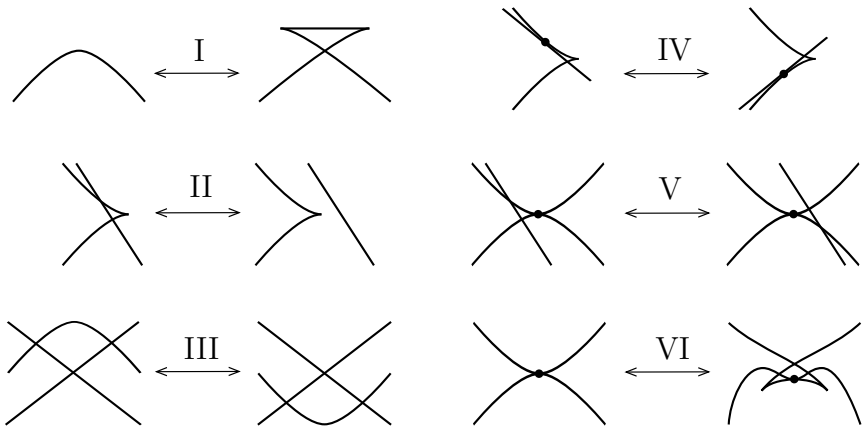


FIGURE 1. Reidemeister moves for $\mathcal{LSK}$

has m transverse double points as its only singularities. Legendrian singular links are discussed as a theme of Vassiliev type invariants, and appeared to give an algorithm for producing possible Lagrangian projections of Legendrian knots. To the best of the authors' knowledge, Legendrian singular links have not yet been studied in their own right.

The h-principle says that the study of Legendrian singular links up to Legendrian regular homotopy reduces to a homotopic theoretic question, thus there can be no interesting phenomena from the perspective of contact topology. We instead study Legendrian singular links up to (ambient) contact isotopy, which preserves transversality and the Legendrian property at each singular point. See Figure 1.

The degree of a given Legendrian singular link can be reduced via *resolutions*[1] as usual for singular links. So Legendrian singular links ($\mathcal{LSK}$) can be reduced to singular links ($\mathcal{SK}$) via the *forgetful map* $\|\cdot\|$, which takes the underlying singular link type, and to Legendrian links ($\mathcal{LK}$) via resolutions $\mathcal{R}$ with the following commutative diagram of various link theories:

$$\begin{array}{ccc} \mathcal{LSK} & \xrightarrow{\mathcal{R}} & \mathcal{LK} \\ {\scriptstyle \|\cdot\|}\downarrow & & \downarrow{\scriptstyle \|\cdot\|} \\ \mathcal{SK} & \xrightarrow{\mathcal{R}} & \mathcal{K} \end{array}$$

We investigate various invariants for $\mathcal{LSK}$ including Thurston-Bennequin number, rotation number, and the resolutions with supporting examples and argue that $\mathcal{LSK}$ is not a straightforward combination of $\mathcal{LK}$ and $\mathcal{SK}$. The other is to develop a useful tool, called *singular connected sum*, and show that it distinguishes a particular pair of Legendrian singular links that can not be distinguished in $\mathcal{LK}$ under any resolution or in $\mathcal{SK}$ under $\|\cdot\|$.

The above two goals are deeply related to a special property of the singular points of Legendrian singular links. Specifically, through contact isotopy, one can keep track of the relative position of two tangent vectors at each singular point by the co-orientation of the contact structure ξ_{std} on S^3. This allows to define an *order* at each singular point which is equivariant under contact isotopy.

Moreover this property enables us to define the notion of connected sum at singular points. We define a *singular connected sum* $(L_1, p_1) \otimes (L_2, p_2)$ by simultaneously performing connected sums on two pairs of arcs near singular points p_i of L_i.

THEOREM 0.1. *For a given pair of Legendrian singular links L_1, L_2 with singular points p_1, p_2, the singular connected sum $(L_1, p_1) \otimes (L_2, p_2)$ is well-defined.*

[1]Sometimes called 'smoothing' in the literature.

THEOREM 0.2. *Let L be a Legendrian singular link and S be a separating sphere for L inducing a decomposition $L = (L_1, p_1) \otimes (L_2, p_2)$. Then this decomposition is well-defined up to order-preserving contact isotopy of S with respect to L.*

There are rigid phenomena in terms of the singular connected sum and the decomposition which will be discussed in a subsequent paper. It is worth remarking that neither the singular connected sum nor the decomposition are well-defined in $\mathcal{SK}$.

On the other hand, a singular connected sum is the same as the replacement of a singular point $p_1 \in L_1$ with a specific singular Legendrian tangle obtained from (L_2, p_2), and *vice versa*. Indeed, the idea of Legendrian tangles and their replacement is already discussed in the literatures although their approaches are slightly different from ours. There is a diagrammatic interpretation of the singular connected sum as well, which allows us to handle the operation in a convenient way.

As an application of the singular connected sum, we have the following theorem which implies that $\mathcal{LSK}$ is more than the *pull-back* of $\mathcal{LK}$ and $\mathcal{SK}$ in the commutative diagram above.

THEOREM 0.3. *There exist two Legendrian singular links sharing all classical invariants, Legendrian link types of all resolutions, and invariants from the orders, which are not contact isotopic to one another.*

For a given $L \in \mathcal{LSK}$ of degree k one can obtain a double $\mathcal{D}(L)$, a Legendrian link in $\#^{k-1}(S^2 \times S^1)$, by a *multiple singular connected sum* of L with itself. Thanks to the work of Ekholm-Ng, we can assign a Legendrian contact homology algebra of $\mathcal{D}(L)$ to L, as an algebraic invariant of L.

Furthermore, the resolutions can be regarded as special cases of tangle replacements, and each resolution has a unique inverse operation, called a *splicing*, under certain splitting conditions. These splicings provide full descriptions of Legendrian singular links with certain singular link types.

Bibliography

[ABKim] B. An, Y. Bae, S. Kim, *Legendrian singular links and singular connected sums*, J. Symplectic Geom. **16** (2018), 885–930.

NON-CLASSICAL INVARIANT OF LEGENDRIAN KNOTS AND THEIR COMPUTATIONS I

YOUNGJIN BAE

Abstract. We discuss a non-classical invariant of Legendrian knot, so-called Legendrian differential algebra or Chekanov-Eliashberg algebra. The geometric and combinatorial construction of Legendrian DGA invariant will be introduced. Also we will see that how this invariant distinguishes the pair of Legendrian knot with the same classical Legendrian invariants.

In the second part, we define a differential graded algebra for Legendrian graphs and tangles in the standard contact Euclidean three space. This invariant is defined combinatorially by using ideas from Legendrian contact homology. The construction is distinguished from other versions of Legendrian contact algebra by the vertices of Legendrian graphs. A set of countably many generators and a generalized notion of equivalence are introduced for invariance. We show a van Kampen type theorem for the differential graded algebras under the tangle replacement. Our construction recovers many known algebraic constructions of Legendrian links via suitable operations at the vertices.

Even though the history of *non-classical* invariants of Legendrian knots is only 20 years, its impact to relative area is huge and fundamental. There are now a number of non-classical invariants including its categorical generalization. The first of these, and in many regards the most important, is Legendrian contact homology(LCH), introduced by Chekanov [Che02] and Eliashberg [Eli98]. Note that LCH is a Legendrian analogue of Lagrangian intersection Floer homology.

In the past 20 years, LCH has been shown to be a powerful invariant of Legendrian knots, but it also has revealed a beautiful internal structure and deep connections with smooth topology and symplectic geometry. Our goal in this paper is to present a fairly thorough overview of Legendrian contact homology, and the network of ideas radiating from it, in the setting where the theory is most fully developed: for Legendrian knots in the standard contact structure in $\mathbb{R}^3$.

Legendrian DGA is a tensor algebra generated by Reeb chords. Here the Reeb chord is an integral curve of Reeb vector field, which is canonically determined by the contact 1-from, starting and ending at the Legendrian we want to investigate. After giving a grading system by using the Lagrangian Grassmannian, we define a differential on the graded algebra by counting a J-holomorphic disks satisfying Lagrangian boundary condition, Reeb chords asymptotic conditions.

Directly comparison between the Legendrian contact homology of two Legendrian knots is in general very difficult. Chekanov introduced augmentations and used them to *linearize* Legendrian contact homology in $\mathbb{R}^3$ producing an invariant that is much easier to use to distinguish between Legendrian knots than the full DGA.

Legendrian graphs are used in the proof of the famous Giroux correspondence theorem and recently appeared in the study of arboreal singularities as 1-dimensional Legendrians with singularities. They have been studied by several groups in their own right, especially in the spirit of classification. The goal of this article is to extend the curve counting idea to Legendrian graphs in the standard contact $\mathbb{R}^3$.

The main issue is how to deal with the singularities, i.e., the vertices of the Legendrian graph. The crucial feature of the construction of a DGA for Legendrian graphs is that we associate a set of countably many generators, Reeb chords, for each vertex of the Legendrian graph. There is geometric motivation for such an assignment. Instead of considering a Legendrian with singularities, let us consider a bordered manifold $S^3 \setminus k\mathring{B}^3$, where $\mathring{B}^3$ is an open 3-ball and k is the number of vertices of our Legendrian graph. Edges in a Legendrian graph are replaced by properly embedded Legendrian arcs in $S^3 \setminus k\mathring{B}^3$. By admitting a certain standard model near the boundary we have a Reeb orbit for each boundary component which yields infinitely many Reeb chords. A DGA with infinitely many generators was discussed by Ekholm-Ng where the authors considered Legendrian links in the boundary of a subcritical Stein 4-manifold. Note that these two constructions are deeply related both geometrically and algebraically.

The second issue is about the grading of the DGA. For Legendrian knots, there is a canonical construction of a potential function, which is unique up to translation and induces a $\mathbb{Z}$ or $\mathbb{Z}/(r)$-grading. Similarly, the gradings on n-component links are given by componentwise potential functions which have $(n-1)$ degrees of freedom up to translation. We generalize this construction further to Legendrian graphs by considering *edgewise* potential functions. Then each edge contributes one to the degree of freedom for grading and exactly one of them is reduced by the translation action as in the link case. To have a well-defined grading on our DGA, we consider Legendrian graphs with potential instead of Legendrian graphs alone.

The last important issue is about invariance with respect to Legendrian isotopy, or Reidemeister moves for Legendrian graphs. The stable-tame isomorphism, a notion of equivalence between DGAs, works well when a pair of generators emerges or cancels out. Such a phenomenon typically appear when we perform the Legendrian Reidemeister move (II) on Legendrian links in the standard contact $\mathbb{R}^3$. When there is a m-valent vertex in a Legendrian graph, however, the Legendrian Reidemeister move (IV$_*$) forces us to develop the notion of algebraic equivalence which cares about the birth and death of m generators. To remedy this problem, we suggest the notion of *peripheral structures* and *generalized stabilizations*. With this terminology, we have

THEOREM 0.1. *Let $\mathcal{L} = (\Lambda, \mathfrak{P})$ be a Legendrian graph with potential. Then there is a pair $(\mathcal{A}_\mathcal{L}, \mathcal{P}_\mathcal{L})$ consisting of a DGA $\mathcal{A}_\mathcal{L} := (A_\Lambda, |\cdot|_\mathfrak{P}, \partial)$ and a canonical peripheral structure $\mathcal{P}_\mathcal{L}$.*

THEOREM 0.2. *The pair $(\mathcal{A}_\mathcal{L}, \mathcal{P}_\mathcal{L})$ up to generalized stable-tame isomorphisms is an invariant for $\mathcal{L}$ under the Legendrian Reidemeister moves for Legendrian graphs with potential. In particular the induced homology $H_*(\mathcal{A}_\mathcal{L}, \partial)$ is an invariant.*

The DGA construction can be generalized to *Legendrian tangles* and we consider the operation given by replacing a Darboux neighborhood of a vertex with suitable Legendrian tangle, which yields a van Kampen type theorem for DGAs.

Legendrian links in a bordered manifold and their associated DGAs were first considered by Sivek via combinatorial methods. The main statement there was also a van Kampen type theorem for Legendrian links in the standard contact $\mathbb{R}^3$. Note that their construction has at most two borders, and it can be interpreted as a Legendrian graph with one or two vertices in our terminology. Our construction of a DGA generalizes that of Sivek's as follows:

THEOREM 0.3. *Let $\mathcal{L}$ be a Legendrian graph(or tangle) with potential having a m-valent vertex, $\mathcal{T}$ be a Legendrian m-tangle with potential, and $\mathcal{L} \amalg_{\Phi_v} \mathcal{T}$ be a tangle replacement with respect to a gluing Φ_v. Then we have a following commutative diagram of DGAs:*

$$\begin{array}{ccc} \mathcal{I}_m & \xrightarrow{\mathbf{p}_\infty} & \mathcal{A}_\mathcal{T} \\ {\scriptstyle \mathbf{p}_v}\downarrow & & \downarrow \\ \mathcal{A}_\mathcal{L} & \xrightarrow{\mathbf{w}_v} & \mathcal{A}_{\mathcal{L}\amalg_{\Phi_v}\mathcal{T}} \end{array}$$

Here $\mathcal{I}_m$ is a DGA for the m-valent vertex v with peripheral structures $\mathbf{p}_v$ and $\mathbf{p}_\infty$, and $\mathbf{w}_v$ is defined by evaluating $\mathbf{p}_\infty$ for the image $\mathbf{p}_v(\mathcal{I}_m)$.

Moreover, there is a canonical inclusion from Sivek's DGA diagram to the above DGA diagram.

On the other hand, Legendrian links can be considered as Legendrian graphs having bivalent vertices only which are smooth at each vertex. Conversely, we define an operation, called *smoothing*, on a bivalent vertex of a given Legendrian graph, which can be used to define an associated DGA for the result. Then via this operation, we can recover Chekanov-Eliashberg's DGA and Ng's DGA.

THEOREM 0.4. *Let $\mathcal{K} = (\Lambda, \mathfrak{P})$ be a Legendrian circle with $(\mathbb{Z}/2rot(\mathcal{K}))$-valued potential consisting of one bivalent vertex v and one edge. Suppose that two half-edges are opposite and have the same potential. Then there is a DGA isomorphism*

$$\mathcal{A}^{\mathsf{sm}}_{\mathcal{K}}(v) \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z}) \to \mathcal{A}^{\mathsf{CE}}_{\mathcal{K}},$$

where $\mathcal{A}^{\mathsf{CE}}_{\mathcal{K}}$ is the Chekanov-Eliashberg DGA over $\mathbb{Z}/2\mathbb{Z}$ for the Legendrian knot obtained from $\mathcal{K}$.

Let $\mathcal{L} = (\Lambda, \mathfrak{P})$ be a Legendrian graph with $\mathbb{Z}$-valued potential whose underlying graph is a disjoint union of circles. Suppose that each component has only one bivalent vertex whose two half-edges are opposite and have the same potential. Then there is a DGA isomorphism

$$\mathcal{A}^{\mathsf{sm}}_{\mathcal{L}} \to \mathcal{A}^{\mathsf{Ng}}_{\mathcal{L}},$$

where $\mathcal{A}^{\mathsf{Ng}}_{\mathcal{L}}$ is the $\mathbb{Z}$-graded Chekanov-Eliashberg DGA over $\mathbb{Z}[\mathsf{t}_1^{\pm 1}, \cdots, \mathsf{t}_m^{\pm 1}]$ for the Legendrian m-component link $\mathcal{L}$ generalized by Ng.

Even though we only consider a combinatorial description for pseudo-holomorphic disks in the rest of the article, the main idea of the construction of our DGA and of the proof of the invariance come from the geometric picture sketched above. This model is inspired by the standard local model for Legendrians in boundaries of Weinstein 1-handles. Indeed, we need half of that standard model. We have the following relation in this regard:

THEOREM 0.5. *Let $\mathcal{L}$ be a Legendrian graph with $2m$ vertices and Φ be a m-pair of gluings of vertices such that the gluing $\mathcal{L}_\Phi$ is a Legendrian link in $\#^m(S^1 \times S^2)$. Then the DGA $\mathcal{A}_{\mathcal{L}}$ is generalized stable-tame isomorphic to the DGA $\mathcal{A}^{\mathsf{EN}}_{\mathcal{L}_\Phi}$ defined by Ekholm and Ng.*

For a given Legendrian link in S^3, there is a construction of a Weinstein domain obtained by attaching a cotangent cone (or Weinstein two handle) along the neighborhood of the given Legendrian link. To extend this construction to a Legendrian graph Λ, we need additional data on Λ, a *smoothing* $\mathcal{S}$ at each vertex and *base points*.

Note that these additional data determine a neighborhood of Λ, *a Legendrian ribbon* R, with preferred Legendrian cycles $\{\Lambda_i\}_{i\in I}$. Now it is possible to mimic the construction for the Legendrian graph, and note that the resulting Weinstein domain, say $\mathcal{W}$, depends on the ribbon R, not the starting Legendrian Λ. So it is natural and important to consider algebraic invariants for the ribbon structure which can be extracted from Λ equipped with the above additional data.

THEOREM 0.6. *Let $(\mathcal{L}, \mathcal{S})$ be a based Legendrian graph with potential and smoothing. For each pair of cycles (Λ_i, Λ_j), there exists a chain complex $\mathcal{A}_{\mathcal{L}_\mathcal{S}}(\Lambda_i, \Lambda_j)$, which is a ribbon equivalence invariant up to (zig-zags of) quasi-isomorphisms.*

In particular, the homology group $H_*(\mathcal{A}_{\mathcal{L}_\mathcal{S}}(\Lambda_i, \Lambda_j))$ is an invariant up to isomorphism under ribbon equivalence.

There are two distinguished Lagrangians in $\mathcal{W}$. One is the Lagrangian skeleton of $\mathcal{W}$ and the other is its symplectic dual, the union of the corresponding cocore disks $D_\Lambda = \{D_i\}_{i\in I}$. We propose a relation between the partially wrapped Floer cohomology of the dual of the Lagrangian skeleton and the newly constructed chain complexes in the following theorem.

THEOREM 0.7. *There is an A_∞ quasi-isomorphism between the partially wrapped A_∞ algebra $CW^*(D_\Lambda, D_\Lambda)$ and $\mathcal{A}_{\mathcal{L}_\mathcal{S}}(\Lambda,\Lambda) = \bigoplus_{i,j} \mathcal{A}_{\mathcal{L}_\mathcal{S}}(\Lambda_i,\Lambda_j)$ which extends the quasi-isomorphisms between the chain complexes $CW^*(D_i, D_j)$ and $\mathcal{A}_{\mathcal{L}_\mathcal{S}}(\Lambda_i,\Lambda_j)$.*

The above conjecture implies that $\mathcal{A}_{\mathcal{L}_\mathcal{S}}(\Lambda_i,\Lambda_j)$ in the above can be interpreted as a combinatorial computation on the A-side of mirror symmetry proposed by Kontsevich. It seems interesting to make a comparison between our method and other approaches including the theory of microlocal sheaves, the infinitesimal Fukaya category, and the study of holonomic $\mathcal{D}$-modules. At the end of this article we give explicit computations of the algebra $\mathcal{A}_{\mathcal{L}_\mathcal{S}}(\Lambda_i,\Lambda_j)$ for an arboreal singularity in Nadler's list.

Bibliography

[AB] B. An, Y. Bae, *A Chekanov-Eliashberg algebra for Legendrian graphs*, J. Topol. **13** (2020), 777–869.

NON-CLASSICAL INVARIANT OF LEGENDRIAN KNOTS AND THEIR COMPUTATIONS III

YOUNGJIN BAE

Abstract. Another source of non-classical Legendrian invariant is the idea of generating families for Legendrian knots. This idea induces a combinatorial description of ruling invariants which is easily computable. Moreover, this ruling type invariant and is intimately related to the DGA invariant for Legendrian knots.

In the second part, we define ruling invariants for even-valence Legendrian graphs in standard contact three-space. We prove that rulings exist if and only if the DGA of the graph in the previous one has an augmentation. We set up the usual ruling polynomials for various notions of gradedness and prove that if the graph is four-valent, then the ungraded ruling polynomial appears in Kauffman–Vogel's graph version of the Kauffman polynomial. Our ruling invariants are compatible with certain vertex-identifying operations as well as vertical cuts and gluings of front diagrams. We also show that Leverson's definition of a ruling of a Legendrian link in a connected sum of $S^1 \times S^2$'s can be seen as a special case of ours.

Ruling invariants for Legendrian knots and links were introduced by Chekanov and Pushkar, and independently by Fuchs. The motivation comes from a *generating family*, which is a family of functions whose critical values give the front of a Legendrian knot. Rulings can be used to distinguish smoothly isotopic Legendrians even if share the same Thurston–Bennequin number and rotation number, such as Chekanov's famous pair of Legendrians of knot type 5_2. For that reason we call ruling invariants *non-classical*.

There is another non-classical construction, the so called Chekanov–Eliashberg DG-algebra, originating from a relative version of contact homology, i.e., holomorphic curve techniques. The homology of the DG-algebra is invariant under Legendrian isotopy and also distinguishes the above pair of Legendrians via a method called linearization of DG-algebras.

There is a deep relation between the two approaches: the existence of a ruling and the linearizability of the DG-algebra, i.e, the existence of a so called augmentation, are equivalent. This is established by Fuchs, Fuchs–Ishkhanov, and Sabloff and extended by Leverson.

On the other hand, the so called ungraded ruling polynomial, which is a weighted (by genus) count of all rulings, appears as a certain sequence of coefficients of the Kauffman polynomial. These are leading coefficients when the upper bound for the Thurston–Bennequin number given by the Kauffman polynomial is sharp, and otherwise all zeros. (Hence the ungraded ruling polynomial is in fact a classical invariant; to access the full power of rulings, one has to narrow their counts to only $\mathbb{Z}$-graded ones.)

Legendrian graphs have been studied using classical invariants. Recently they have also drawn attention as singular Legendrians appearing in the study of Lagrangian skeleta of Weinstein manifolds. The first two authors developed a DG-algebra invariant for Legendrian graphs via a careful consideration of the algebraic issues that arise near the vertices of graphs.

In this article, we extend the definition of ruling from Legendrian links to Legendrian graphs. Of course, the main issue will be to analyze the behavior of each ruling near the vertices. We restrict ourselves to Legendrian graphs with only even-valent vertices and demand that the ruling at each vertex be parametrized by the set of perfect matchings of the incident edges. In

other words, we regard a Legendrian graph as a set of Legendrian links (with markings) which can be obtained by resolutions of vertices, indexed by a perfect matching at each vertex.

With this extension, we show the equivalence between the existence of (ρ-graded) rulings and of (ρ-graded) augmentations for Legendrian graphs.

THEOREM 0.1. *Let L be a bordered Legendrian graph. Then a ρ-graded normal ruling for L exists if and only if a ρ-graded augmentation for the DG-algebra $\mathcal{A}(\mathsf{L})$ exists.*

Kauffman and Vogel introduced a polynomial invariant for four-valent graphs embedded in $\mathbb{R}^3$ which generalizes the two-variable Kauffman polynomial of links. We also show that the ungraded ruling polynomial can be realized as a certain sequence of coefficients of this topological graph invariant.

THEOREM 0.2. *Let L be a regular front projection of a four-valent Legendrian graph. The ungraded ($\rho = 1$) ruling polynomial $R_1(\mathsf{L})$ for L is the same as the coefficient of $a^{-\mathbf{tb}(\mathsf{L})-1}$ (a^{-1}, resp.) in the shifted Kauffman–Vogel polynomial $z^{-1}F_{\mathsf{L}}$ (unnormalized polynomial $z^{-1}[\mathsf{L}]$, resp.) after replacing A and B with $(z-1)$ and -1, respectively.*

Bibliography

[ABKa] B. An, Y. Bae, T. Kálmán *Ruling invariants for Legendrian graphs*, arXiv:1911.08668.

LECTURE 2

Mathematics in Blockchains

MATHEMATICS IN BLOCKCHAINS I

SEUNGSANG OH

Abstract. 블록체인은 거대한 분산 공개 장부이며, 그 장부 안에 포함된 개별 거래는 모두 디지털 서명이 붙어 있어서 은행이나 다른 제 3자의 개입이 없어도 진본임을 보증할 수 있다. 거래 당사자간의 신뢰 확보를 위해 중앙 기관을 필요로 하지 않는 탈중앙화를 달성한 최초의 스프트웨어 기술이다. 여기에는 작업 증명이라는 수학적 계산 작업과 경제 관점에서의 논리를 통해 위,변조가 사실상 불가능한 구조를 갖게 되어, 그 안에 기록된 거래들은 은행같은 중앙의 보증 기관이 없이도 신뢰할 수 있는 거래로서 확정될 수 있다. 이번 강의를 통해서 우리는 블록체인의 핵심 개념인 분산 공개 장부, 해시함수, 전자서명, 작업증명(PoW), 채굴(보상), 블록의 생성 및 전파, 블룸 필터, 이중지불 문제, 완료된 거래정보의 변경 불가 등에 대해서 배운다.

1. 4차 산업혁명과 블록체인, 그리고 비트코인

1.1. 4차 산업혁명 4차 산업혁명(Fourth Industrial Revolution)은 정보통신 기술(ICT)의 융합으로 이루어지는 차세대 산업혁명으로 핵심은 *빅 데이터(Big Data)*, *인공지능(AI)*, *사물인터넷(IoT)*, 로봇공학, 무인 운송 수단(무인 항공기, 무인 자동차), 3D 프린팅, 나노 기술과 같은 7대 분야에서 새로운 기술 혁신이다.

1.1.1. *4차 산업혁명에 따른 플랫폼 차원의 변화* 과거 우리 사회 인프라와 규제는 중앙집권적인 형식으로, 비암호화된 허브 앤 스포크[1] 데이터베이스 구조로 인해 관리 비용이 많이 들고 사이버 공격에 쉽게 노출되었다. 이를 해결하기 위해 시스템을 *분산구조*로 전환할 필요가 있는데, 그 핵심 기술이 *암호화*와 *분산장부*이다.

1.1.2. *4차 산업혁명의 인프라로서의 블록체인* 블록체인은 *탈중앙화*(Decentralization), *비용*(Efficiency), *보안성*(Sequrity), *투명성*(Transparency) 등 뛰어난 장점으로 4차 산업혁명의 신성장 산업을 발전시키는데 있어 신뢰성을 강화하고 효율성을 제공할 수 있는 기반 기술이다. [2]

1.2. 블록체인(Blockchain). 블록체인은 데이터 위·변조를 방지하기 위한 분산 컴퓨팅 기술 기반의 원장(Ledger) 관리 기술이다. P2P 방식을 기반으로 소규모 데이터들이 체인 형태로 연결되어 형성된 '블록'이라는 분산 데이터 저장 환경에 관리 대상 데이터를 저장함으로써, 누구도 임의로 수정할 수 없으나 누구나 열람할 수 있도록 하는 기술이다.

블록에는 해당 블록이 생성되기 전에 사용자들에게 전파되었던 모든 거래 내역이 기록되어 있고, 새로 생성된 이 블록은 P2P 방식으로 모든 사용자에게 똑같이 전파되어 거래 내역에 대한 임의 조작이 불가능하다. 각 블록은 생성된 날짜와 이전 블록에 대한 연결고리를 가지고 있으며, 블록들의 집합을 블록체인이라 한다.

블록체인 기술은 비트코인과 이더리움을 비롯한 대부분의 암호화폐 거래에 사용된다. 암호화폐의 거래과정은 탈중앙화된 전자장부에 기록되기 때문에 블록체인 소프트웨어를 실행하는 사용자들의 컴퓨터에서 서버가 운영되어, 중앙에 존재하는 은행 없이 개인 간의 자유로운 거래가

[1]허브 앤 스포크(hub-and-spoke): 각각의 출발지(Spoke)에서 발생하는 물량을 중심 거점(Hub)으로 모으고, 중심 거점에서 물류를 분류하여 다시 각각의 도착지(Spoke)로 배송하는 형태가 마치 바퀴의 중심축(Hub)과 바퀴살(Spoke)의 모습을 연상케 한다고 해서 지어진 이름.

[2]2015년 세계경제포럼의 미래예측리포트 '기술전환점과 사회적 충격'은 2027년에는 전 세계 GDP의 10%가 블록체인 화폐로 보관될 것을 예측.

가능하다. 특이한 것은, 사토시 나카모토는 블록체인을 먼저 개발하고 그것을 비트코인에 적용한 것이 아니라, P2P 방식 전자 화폐 시스템인 비트코인을 개발하면서 발생하는 문제를 해결하기 위해 블록체인을 개발했다는 점이다.

1.3. 비트코인(Bitcoin). 비트코인은 블록체인 기술을 기반으로 만들어진 최초의 온라인 암호화폐로, 통화를 발행하고 관리하는 중앙 장치가 존재하지 않는 구조를 가지고 있다.

비트코인 창시자는 사토시 나카모토(Satoshi Nakamoto)라는 필명을 쓰는 개인 또는 팀으로 알려져 있다. 더욱이 나카모토는 비트코인을 2009년 1월에 출시하고 약 1년 후 자취를 감춰버렸다.

비트코인의 거래는 P2P 기반 분산 데이터베이스에 의해 이루어지며, 공개 키 암호 방식 기반으로 개인들 간에 자유롭게 송금 등의 금융거래를 할 수 있게 설계되어 있다. 비트코인은 지갑 파일의 형태로 저장되며, 각 지갑에 부여된 고유주소를 기반으로 거래가 이루어진다.

모든 거래 기록은 분산 데이터베이스에 저장하는데, 용량을 줄이기 위해 머클트리(Merkle tree)가 사용된다. 또한, 일련의 작업증명(Proof of Work)을 통해 이중지불(double-spending)을 방지한다.

거래장부는 전 세계적인 범위에서 여러 사용자들의 서버에 분산하여 저장하기 때문에 해킹이 불가능하다. SHA-256 기반의 암호 해시 함수를 사용한다.

1.4. 이더리움(Ethereum). 이더리움은 블록체인 기술을 기반으로 스마트 컨트랙트(smart contract) 개념을 처음 구현한 분산 컴퓨팅 플랫폼이자 운영 체제다. 비탈릭 부테린(Vitalik Buterin)이 17세에 비트코인 매거진을 만든후, 18세에 이더리움을 개발, ICO로 200억을 모아 2015년에 출시하였다. [3]

비트코인이 결제나 거래 관련 시스템, 즉 화폐로서의 기능에 집중하는 반면, 이더리움은 화폐로서의 기능 외에, 계약서, SNS, 이메일, 전자투표 등의 추가 정보를 블록체인에 기록할 수 있는 다양한 애플리케이션을 투명하게 운영할 수 있게 확장하였다.

댑(dApp)이라는 분산 애플리케이션(Decentralized Application)은 누구나 만들고 사용할 수 있는 플랫폼이다. 또한, 이더리움을 사물 인터넷(IoT)에 적용하면 기계 간 금융 거래도 가능해진다. [4]

2. 블록체인의 핵심은 분산 공개 장부다.

2.1. 분산 공개 장부 A가 B에 백만원을 송금할때, A가 은행사이트에 접속해서 잔액을 확인한 후, B의 계좌정보와 공인인증서 비밀번호를 입력하고 송금 버튼을 누르면, A의 잔액에서 백만원이 차감되고, B의 잔액에 백만원이 더해진다. 송금거래에 필요한 모든 과정은 은행에서 확인, 수행, 기록하며, 원장은 외부로 공개되지 않는다.

그래서 은행은 단일실패지점(single point of failure)이 될 수 있다. 즉, 은행의 서버가 오작동하거나 기록들이 사라지면 심각한 문제가 발생한다. 컴퓨팅 분야에서 단일실패지점 문제를 해결하는 보편적인 방법은 다중화이다. 은행도 이러한 위험을 낮추기 위해 거래내용을 복제해서 분산처리하고, 보안장비와 보안담당 직원을 배치하는데 많은 비용을 사용한다.

블록체인(퍼블릭 블록체인)은 이 문제를 완전히 다른 각도로 바라본다. 거래정보(transaction)를 모두에게 공개하여 누구나 읽고 생성하며, 사본을 저장하고 동기화시킨다. 거대 다중화로 기록 손실을 원천적으로 막기 때문에 블록체인은 거대한 분산 공개 장부가 된다. 또한, 블록체인은 암호이론을 이용하여 기록의 위·변조까지 막는다.

블록체인은 P2P[5] 기반 분산 네트워크를 사용하여 트랜잭션과 블록의 데이터를 모든 구성원이 100% 동일하게 공유한다.

---

[3]이 기술로 부테린은 신기술 분야의 노벨상이라고 불리는 '월드 테크놀로지 어워드'에서 페이스북 창업자인 마크 저커버그를 제치고 IT 소프트웨어 수상자로 뽑혔다.

[4]예를 들어 고장난 청소로봇이 정비로봇에 돈을 내고 정비를 받고, 청소로봇은 돈을 벌기 위해 정비로봇의 집을 청소하는 것도 가능해진다

[5]P2P(peer-to-peer network 동등 계층간 통신망)는 소수의 서버에 집중하기보다는 망구성에 참여하는 기계들의 계산과 대역폭 성능에 의존하여 구성되는 통신망이다. 각 노드들(peer nodes)이 서로 클라이언트와 서버 역할을 동시에 하기 때문에 클라이언트-서버 모델과는 구별된다.

2.1.1. *풀* 노드 모든 블록체인 정보를 수집하고 저장하는 노드로, 새로운 블록을 추가하기 위해 블록검증을 수행하고, 요청 받는 블록정보나 새롭게 검증된 블록 들을 저장 및 관리한다.

2.1.2. *라이트* 노드 블록체인에 참여하여 거래를 수행하는 노드로, 모든 블록정보를 가지고 있지 않고 개별 거래에 대한 트랜잭션을 확인하기 위해 단순지불검증 (Simple Payment Verify, SPV)를 수행한다. 거래를 검증하기 위해 라이트 노드가 풀 노드에게 블록정보를 요청하며, 라이트 노드는 머클트리를 통해 이 거래가 검증된 거래인지를 확인한다.

3. 블록체인과 블록의 구조

3.1. 블록체인 블록체인은 암호 화폐의 거래가 공개적으로 기록되는 디지털 장부인 블록들로 이루어진 링크드 리스트다.

사토시 나카모토가 생성한 최초 블록(genesis block)부터 현재까지 모든 불록들을 삭제를 하지 않으면서 시간순서로 블록해시 체인으로 연결되어 있다.

MATHEMATICS IN BLOCKCHAINS II

SEUNGSANG OH

Abstract. 블록체인은 거대한 분산 공개 장부이며, 그 장부 안에 포함된 개별 거래는 모두 디지털 서명이 붙어 있어서 은행이나 다른 제 3자의 개입이 없어도 진본임을 보증할 수 있다. 거래 당사자간의 신뢰 확보를 위해 중앙 기관을 필요로 하지 않는 탈중앙화를 달성한 최초의 스프트웨어 기술이다. 여기에는 작업 증명이라는 수학적 계산 작업과 경제 관점에서의 논리를 통해 위,변조가 사실상 불가능한 구조를 갖게 되어, 그 안에 기록된 거래들은 은행같은 중앙의 보증 기관이 없이도 신뢰할 수 있는 거래로서 확정될 수 있다. 이번 강의를 통해서 우리는 블록체인의 핵심 개념인 분산 공개 장부, 해시함수, 전자서명, 작업증명(PoW), 채굴(보상), 블록의 생성 및 전파, 블룸 필터, 이중지불 문제, 완료된 거래정보의 변경 불가 등에 대해서 배운다.

1. 암호화 해시함수와 머클트리

1.1. 암호화 해시함수 해시함수(hash function)는 임이의 길이를 갖는 메시지를 입력받아 다음 성질의 해시값을 출력한다.

- 어떤 입력값에도 항상 고정된 길이의 해시값을 출력한다.
- 눈사태 효과: 입력 값의 아주 일부만 변경되어도 전혀 다른 해시값을 출력한다.
- 출력된 해시값을 토대로 입력값을 유추할 수 없다.

암호 알고리즘과는 달리 해시함수는 키를 사용하지 않으므로 같은 입력에 대해서는 항상 같은 출력이 나온다. 이러한 성질은 메시지의 오류나 변조를 탐지할 수 있는 무결성을 제공하기 위해 사용된다.

해시 테이블이라는 자료구조에 사용해서 정렬을 하지 않고도 빠른 데이터 검색용 소프트웨어에도 사용된다.

해시값으로는 입력값을 유추할 수 없기에 암호용으로 사용되는데, 이 경우 다음에 대한 안전성을 가져야 한다.

- *역상 저항성*(preimage resistance): 주어진 해시값을 생성하는 입력값을 찾는 것이 계산상 어렵다.
- *제 2 역상 저항성*(second preimage resistance): 해시값을 바꾸지 않으면서 입력값의 변경은 계산상 어렵다.
- *충돌 저항성*(collision resistance): 같은 해시값을 생성하는 두 개의 입력값을 찾는 것이 계산상 어렵다.

해시함수의 성능은 입력 영역에서의 해시 충돌 확률로 결정된다. 입력값 범위보다 해시값 범위가 좁기 때문에 드물게 충돌이 일어난다. 이런 어쩔 수 없는 충돌을 제외하고 의도적으로 충돌을 계산해 낼 수 없어야 한다.

1.2. 블록체인에서의 해시함수

1.2.1. *SHA256 해시함수(Secure Hash Algorithm).* 미국 국가안보국에서 1993년 설계하고 국가표준으로 지정. 해시값은 32byte 크기의 64문자열(0~f의 16진수 사용)이고, $2^{256} \approx 10^{77}$ 종류의 해시를 생성할 수 있다. 참고로, 32byte는 256bit이므로 크기가 2^{256}이고, 16진수 64문자열도 16^{64}이다. 이 해시함수를 무차별 대입으로 깨려면 약 10^{77}번의 계산을 해야하므로 현실적으로는 불가능하다.

- 안녕하세요. $\Longrightarrow$ 8B118D6741F7CFA1A7EE246D0DDA39F2F00BF9FD207B4E6C7FAD87A15434A513
- 안녕하세요 $\Longrightarrow$ 6DCE5BB85644D4E531F29E06EA28024324E949BFBBDE472C0CFD04B4EEF03D65
- 블록체인은 P2P 방식을 기반으로 소규모 데이터들이 체인 형태로 연결되어 형성된 '블록'이라는 분산 데이터 저장 환경에 관리 대상 데이터를 저장해서, 누구도 임의로 수정할 수 없으나 누구나 열람할 수 있도록한다. $\Longrightarrow$ 82FA4923FFFCE2F1343DD372450CD103A4559913186C517406A6F7ABE65D4A2C

- 비트코인 주소: RIPEMD160(SHA256(public key)) 사용자의 public key 사용
- 트랜잭션(거래정보) 해시: SHA256(SHA256(transaction data)) 각 트랜잭션마다
- 머클트리 해시: SHA256(SHA256(concat(tx1 hash, tx2 hash))) 블록에 소속될 전체 트랜잭션의 해시값을 순서대로 2개 쌍으로 묶어서 해시값들을 구한 후 최종 머클루트를 구함
- 블록 해시: SHA256(SHA256(blockheader 80bytes)) 블록헤더 전체에 대하여 계산

1.3. 머클트리와 머클루트 머클루트는 블록이 보유하고 있는 거래내역들의 해시값을 가장 가까운 거래내역끼리 쌍을 지어 해시화하고, 쌍을 지을수 없을 때까지 이진 트리 형태로 이 과정을 반복했을 때 얻게 되는 최종 해시값이다.

특정 거래내역을 증명하기 위해 방대한 거래내역들을 조회할 필요가 없이, 32byte의 해시값 하나로 검증을 간편하고 확실하게 할수있다. 블록체인은 모든 거래 내역을 저장한 풀노드와 일부만을 처리해 보관하는 라이트 노드를 분리해 거래 처리 속도를 높이는데, 라이트 노드는 이 머클루트들만 저장한다.

거래 내역 일부에 작은 변화가 있으면 상위 해시값이 모두 변환되기 때문에, 각 거래내역의 정보들이 변경·삭제·삽입 되었는지에 대한 유효성 검사가 가능하다. 위 두 가지 장점으로 인해 저사양이 기기들의 네트워크 접근성이 용이하고 동시에 보안성도 높아서, 탈중앙화를 통한 네트워크 안정성을 향상 할수다.

2. 채굴: 작업증명 (PoW) 과 보상

2.1. 작업증명(Proof of Work, PoW). 특정 조건을 만족할 때까지 *난스값*(nonce)을 변화시켜가면서 블록해시들을 구하고, 조건을 만족하는 블록해시가 구해지면 이것으로 유효한 블록이 생성된다. 결국 작업 증명의 핵심은 난스값을 구하는 것이다.

입력값은 블록헤더에 있는 6가지 정보이고, 이중에 오직 난스값만 고정값이 아니다. 난스값을 무작위로 계속 바꿔가면서 계산한 해시값이 어떤 target보다 작아지면 새로운 블록의 블록해시값으로 확정이 되고, 그 때의 난스값이 그 블록의 난스값이 되면서 작업증명이 끝난다.

2.2. 채굴 난이도(Difficulty). 블록해시가 target보다 낮게 나오도록 하는 난스값을 찾는 것이 작업증명이다. 채굴 난이도에서는 블록헤더 정보에서 bits라는 값으로 조절하여 난스값 계산의 어려운 정도를 정한다. [1]

난이도는 2,016개 블록을 생성하는 평균 채굴시간이 20,160분(2주)이 걸리도록 자동 조정되어 블록체인 전체에 걸쳐 일률적으로 적용된다. 컴퓨팅 성능이 좋아지거나 채굴자들의 수가 늘어나서 블록 생성이 빨라지면, 정해진 주기에 따라 난이도가 높아져서 결국에는 유효한 난스값을 찾아 작업증명을 하는데 평균적으로 10분이 소요되도록 한다.

2.3. Bits에서 target과 난이도 계산 방법 4byte 크기의 *bits*로 64byte 크기의 *target*을 만드는 방법은, 먼저 bits를 16진수 8문자열(0x~표기)로 바꾼 후, 앞의 두자리 수와 뒤에 6자리 수를 다음 공식처럼 대입한다.

- bits: 388618029 = 0x*17*29D72D

[1] 난이도 수치인 bits에서 요구하는 target이 '000000000000000C84...F33A'라면(16진수 64문자열), 블록해시가 더 작게 나올 확률은 앞에 0이 15개가 있으므로 $\frac{1}{16^{15}} \approx \frac{1}{10^{18}}$이다. 대략 10^{18}번 정도 반복해서 블록해시를 계산해야 난스값을 찾게된다.

- target: 0x29D72D*2**(8*(0x*17*−3)) = 0x29D72D×16^{40}
  = 0x 0000 0000 0000 0000 0029 D72D 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

*난이도*는 나카모토가 생성한 genesis block의 Bits의 난이도(difficulty_1_target)와 현재의 난이도의 비율이다.

- difficulty_1_target: 0x*1D*00FFFF = 0x 0000 0000 FFFF 0000 0000 0000 0000 ⋯ 0000 0000 0000 0000
- difficulty = difficulty_1_target/current_target = 6,727,225,469,722.53 (10진수로 변환해서 계산)

다음 난이도 계산 방법

- new_difficulty = old_difficulty × (20,160분)/(마지막 2016블록의 실제소요시간) ⟵ $\left[\frac{1}{4}, 4\right]$로 큰 변화 제한
- new_target: difficulty_1_target/new_difficulty ≈ 0x 0000 0000 0000 0000 00C5 9D27 090B 029C ⋯ A90B
  ⇒ 0x 0000 0000 0000 0000 00C5 9D27 0000 0000 ⋯ 0000
- new_bits: 398826791 = 0x*17*C59D27

2.4. 채굴(mine)과 보상 *채굴*은 작업증명과 보상을 합친 개념으로 일반인들이 비트코인을 쉽게 이해할 수 있도록 만든 용어다. 난스값을 구하는 채굴 작업은 방대한 해시 계산이 필요하기에 고가의 GPU 장치와 막대한 전기 비용이 든다.

*보상*은 자발적 참여를 위해 채굴자에게 주는 일정량의 비트코인과 해당 블록 내의 모든 거래 수수료의 합이다. 블록 채굴에 대한 보상은 비트코인 체계의 핵심이고, 보상이 없다면 시스템 자체가 작동하지 않는다. 새로 발행되는 비트코인이 채굴자의 지갑에 입금되는 거래가 채굴자가 구성한 블록의 첫 거래가 된다.

비트코인은 총 2100만 개로 한정되있고, 이러한 희소가치가 시장 가격에 큰 영향을 미친다. 보상으로 주어지는 비트코인은 2009년 1월 50BTC로 시작해, 블록이 21만개 채굴될 때마다 절반으로 줄어들며, 세 번째 반감기인 2020년부터는 블록당 6.25BTC가 발행된다. 반감기는 10분마다 1블록이 생성되므로 약 4년 걸린다.

시간이 지날수록 지급되는 비트코인은 줄어들지만 비트코인 가치가 커져서 실질 보상액은 오히려 늘어난다. 하지만 대략 2032년 이후, 보상이 1BTC보다 적어지면 거래 수수료는 채굴자의 중요한 수입원이 된다. 채굴 업무에 이전 같은 매력을 느낄 수 있을지는 불투명해져서 비트코인이 심각한 위협에 처할수도 있다.

채굴은 매 10분마다 전세계에서 단 한번 이루어지기 때문에 성공 확률이 지극히 적다. 그래서 채굴자들끼리 채굴 풀(mining pool)을 형성해서 난스값을 찾는 계산 작업을 분담하고, 해당 풀에서 채굴에 성공하여 코인을 보상받으면 풀에 참가한 각자의 배분 기준에 의해 나누어 가지는 방식으로 채굴 시장이 운영된다.

MATHEMATICS IN BLOCKCHAINS III

SEUNGSANG OH

Abstract. 블록체인은 거대한 분산 공개 장부이며, 그 장부 안에 포함된 개별 거래는 모두 디지털 서명이 붙어 있어서 은행이나 다른 제 3자의 개입이 없어도 진본임을 보증할 수 있다. 거래 당사자간의 신뢰 확보를 위해 중앙 기관을 필요로 하지 않는 탈중앙화를 달성한 최초의 스프트웨어 기술이다. 여기에는 작업 증명이라는 수학적 계산 작업과 경제 관점에서의 논리를 통해 위,변조가 사실상 불가능한 구조를 갖게 되어, 그 안에 기록된 거래들은 은행같은 중앙의 보증 기관이 없이도 신뢰할 수 있는 거래로서 확정될 수 있다. 이번 강의를 통해서 우리는 블록체인의 핵심 개념인 분산 공개 장부, 해시함수, 전자서명, 작업증명(PoW), 채굴(보상), 블록의 생성 및 전파, 블룸 필터, 이중지불 문제, 완료된 거래정보의 변경 불가 등에 대해서 배운다.

1. 전자서명(Digital sign)

전자서명은 *데이터 해싱*, *서명*, *검증*으로 이루어져 있다.

타원곡선 전자서명[1] 기반으로 서명자의 개인키(private key)와 공개키(public key)를 이용한 서명과 검증 알고리즘을 통해 데이터의 *무결성*, 서명자의 *진위성*, 서명자의 서명 *부인 방지* 등을 보장 한다.[2]

1.1. 데이터 해싱과 공개키 암호화 방식

- 데이터 해싱: 해싱 알고리즘을 통해 주어진 데이터를 고정된 길이로 다이제스트 된 해시값으로 변환한다.
- 서명: 서명자 A는 해시된 메시지와 A의 개인키로 전자서명을 생성하고 공개한다. 전자서명은 각 메시지 내용과 직접 관련있어, 손으로 쓴 서명과 달리 특정 메시지의 고유한 디지털 지문 역할을 한다.
- 검증: 일반 사용자는 공개된 전자서명과 A의 공개키로 메세지를 복원한 후에 원본을 해싱한 해시값과 비교하여, 원본 내용이 A에 의해 작성되었는지를 검증한다. 서명자만이 공개키에 상응하는 개인키를 갖고 있기 때문에, 해당 전자서명의 진위성을 보장 받을수 있다.

1.2. 디지털 서명은 왜 중요한가요?.

- 데이터 무결성: 메시지가 수정되면 전자서명이 변경되기 때문에, 전송되는 동안 변경되지 않았음을 검증한다.
- 진위성: 서명자 A의 개인키가 안전하게 보관되는 한, 수신자는 전자서명이 A에 의해 생성되었음을 검증한다. 개인키가 안전하게 보관되지 않은 경우, 다른 사람이 A의 코인을 마음대로 사용할 수 있다.
- 부인 방지: 서명자 A의 개인키가 어떤 특정 이유로 노출되지 않는 이상, A는 앞으로는 서명 사실을 부정할 수 없다.

[1]타원곡선 암호시스템은 기존이 암호시스템에 비해 단위 비트당 키 길이가 작고 속도가 빠르기에, 휴대 통신기기에 용이하게 적용된다.

[2]공개키 암호화 방식은 암호화와 복호화에 같은 키를 사용하는 대칭키 암호화 방식과 다르며, 지금의 전자서명이나 인터넷 암호화 통신을 가능하게 만든 1등 공신으로, 인터넷 전자상거래를 가능하게 했다.

2. 블록의 생성 및 전파 - 블룸 필터

2.1. 단일 거래정보의 전파 블록체인의 분산공개장부는 P2P로 연결되어 블록체인 네트워크를 형성하고 있는 여러 노드에 복사되어 있다. 하나의 거래정보(transaction) 발생시, 즉시 네트워크에 분산되어 있는 수많은 노드에 전파된다.

F가 지갑앱으로 C에게 1.6BTC (수수료 0.001BTC) 보내면, 지갑앱은 블록체인 네트워크 상의 노드 A에 거래정보를 F의 전자서명과 함께 전송한다. 노드 A는 먼저 해당 거래의 유효성을 전자서명을 사용해 검증한 후, 그 거래를 아직 블록 생성 작업이 시작되지 않은 후보 블록에 추가하고 인접한 다른 노드에 전파한다. 거래정보를 받은 다른 노드들도 동일하게 여러 노드에게 전파해서 결국 블록체인 네트워크 전체 노드에 전파된다.

비트코인 지갑은 송수금 거래를 가능하게 해주는 클라이언트 소프트웨어이며, 거래정보를 블록체인 네트워크에 전파해야하므로 블록체인 네트워크의 노드이기도 하다. 하지만, 지갑앱은 작업증명 계산을 하지 않기 때문에 블록체인의 모든 거래정보를 저장하지 않는다.

비트코인의 블록은 약 10분마다 하나씩 생성된다. 어떤 거래가 확정 되려면 그 거래가 포함된 블록이 생성되어야 하므로 약 10분 정도가 소요된다. 엄밀하게는 거래 수수료에 따라 10분 이상이 소요되는 거래가 있을 수도 있다.

2.2. 블록의 생성 및 전파 블록에 거래 정보가 채워지면 노드는 블록을 생성한다. 이때 캐나다에 있던 노드와 호주에 있던 노드는 상당히 멀리 떨어져 있으므로, 각 블록에 담겨 있는 거래의 내용과 순서는 아래와 같이 서로 다를 수 있다.

새로 만들어질 블록은 가장 마지막에 생성된 파랑블록 다음에 추가된다. 캐나다와 호주의 노드들이 거의 동시에 난스값을 찾아서 빨강블록과 초록블록을 생성하게 되면, 생성 후 그림과 같이 전파된다.

캐나다 노드의 인접 노드에서는 전달받은 빨강블록의 난스값을 가지고 블록해시를 다시 계산해서 그 값이 정말로 target보다 작은지를 검증한 후에, 자신이 가지고 있던 파랑블록에 빨강블록을 추가한다. 호주 노드에 인접한 노드에서도 마찬가지 방식으로 기존의 파랑노드에 초록노드가 추가한다. 이러한 방법으로 빨강블록과 초록블록은 전 세계에 분산되어 있는 노드들에게 전파된다.

포르투갈에 있는 노드에는 빨강블록이 먼저 전파되면, 늦게 도착하는 초록블록은 무시된다. 러시아에 있는 노드는 초록블록을 추가한 후, 다시 가장 먼저 난스값을 구해서 새로 분홍블록을 생성해서 초록블록 다음에 추가하고 인접 노드에 전파했다. 포르투갈에 있던 노드에는 파랑블록 다음에 빨강블록이 추가되어 있는 상태였는데, 파랑블록과 초록블록에 이어진 새로운 분홍블록을 전달받는다. 그로인해 포르투갈에 있던 노드에는 다른 내용의 빨강블록과 초록블록에 의한 블록체인의 분기가 발생한다.

블록체인의 분기가 발생해서 충돌할 때, 더 많은 작업증명이 수행되어 길이가 긴 블록을 선택한다. 그래서 포르투갈 노드에 더 긴 블록체인을 가진 분홍블록이 전파되는 순간, 빨강블록은 파랑블록에서의 연결이 끊어지고 고아가 된다.

블록 생성은 10여분이 소요될 정도로 연산량이 큰 작업으로, 두 블록이 거의 동시에 생성되어 분기가 발생할 가능성은 적다. 그리고 길이가 같은 블록체인이 충돌하더라도 머지않아 블록체인의 길이가 달라져서 분기에 의한 충돌이 곧바로 해소된다. 실제로 길어야 3개 이내에서 블록체인의 분기에 의한 충돌이 해소된다.

하지만 일시적으로나마 이런 분기 상태가 발생할 수 있기 때문에, 실제 거래 상황에서는 어떤 거래를 포함한 블록이 뒤에 3∼5개의 블록이 더 추가된 후에야 그 거래가 최종적으로 유효한 것으로 확정한다. 일시적으로 분기가 발생하더라도 그 이후로 3∼5개의 블록이 추가되는 과정에서 분기 상태가 해소되고 결국 하나의 블록체인만 남기 때문이다.

2.3. 블룸 필터(Bloom filter). 빨강블록에 있던 거래 중에서 초록블록에 포함되지 않았던 거래 T가 있을 수 있다. 그럼 빨강블록이 고아가 되면 거래 T는 결국 유실되는 것이 아닐까? 아니다. 거래 T가 초록블록에 포함되지 않았기에, 초록블록에 이어 생성되는 분홍블록 또는 그 이후의 블록에서도 거래 T는 아직 블록체인에 포함되지 않은 것으로 취급되며, 결국 새로운 블록에 추가된다.

*블룸 필터*는 한 트랜잭션이 블록체인의 블록에 속해 있는지 확인하는 효율적인 방법이다. 원소가 집합에 속하는지 여부를 검사하는데 사용되는 확률적 자료 구조로, 1970년 Burton Bloom이 고안했다.

블룸 필터의 특징은 원소가 집합에 속한다고 판단했는데 실제로는 속하지 않는 긍정 오류의 발생은 가능하되, 반대로 원소가 집합에 속하지 않는 것으로 판단했는데 실제로는 속하는 부정 오류의 발생은 불가능하다. 또한, 집합에 원소를 추가하는 것은 가능하나, 삭제하는 것은 불가능하다. 집합 내 원소의 숫자가 증가할수록 긍정 오류 발생 확률도 증가한다.

블룸 필터는 m비트 크기의 비트 배열 구조를 가진다. 또한 블룸 필터는 k가지의 서로 다른 해시함수를 사용하며, 각 해시함수는 입력된 원소에 대해 m가지의 값을 균등한 확률로 출력해야 한다.

블룸 필터는 집합에 원소를 추가하는 명령어와 원소가 속하는지를 검사하는 명령어를 지원하고, 원소를 삭제하는 명령어는 존재하지 않는다. 원소를 추가할 때는 원소의 k가지의 해시값을 계산한 다음, 각 해시값에 대응하는 비트를 1로 설정한다. 원소를 검사할 때도 k가지의 해시값을 계산해서 각 해시값에 대응하는 비트값을 읽은 후, 모든 비트가 1인 경우 속한다고 판단하며, 나머지는 속하지 않는다고 판단한다.

블룸 필터 $(m = 18, k = 3)$에 세 원소 x, y, z가 추가되어 있다. w의 세 해시값 중에서 블룸 필터 값이 0인 경우가 존재하기 때문에, 해당 값은 집합에 속하지 않는다고 판단할 수 있다.

3. 이중지불 문제 및 완료된 거래정보의 변경 불가

3.1. 이중지불 문제 디지털은 복사가 가능하므로 이중 지불이라는 문제가 있다. 특히 블록체인은 수많은 노드에 복제되는 방식이므로 더욱 심각하다.

일단 동일한 기기에 담긴 지갑에서는 지불하는 순간 잔액이 줄어들어 0이 되면 이중지불을 할 수 없다. 그래서 이중지불은 물리적으로 떨어진 두 개의 지점에서 가능하다.

예를들어, 장부가 복제되어 있으므로 캐나다나 호주도 내 잔액은 동일하게 10만원 일때, 캐나다에서 A에게 10만원을 보내고, 거래정보가 아직 도달하지 않은 호주에서 B에게 10만원을 보내면 어떻게 될까? 이중지불이 실행된 후, 두 거래정보는 블록체인 네트워크를 타고 전파되다가 어디에선가 반드시 만나게 되고, 그 지점에 먼저 도달한 거래는 유효한 거래로 인정되지만 늦게 도달한 거래는 이미 잔액이 0인 상태에서 10만원을 보내게 되므로 무효한 거래로 버려지게 된다.

이중지불된 거래 중 하나는 결국에는 무효화되는 방식으로 이중지불 문제가 해결된다. 이러한 이중지불 문제는 비트코인이 등장 이전까지는 오랫동안 해결하지 못한 어려운 문제였다. 그래서 이중지불이 쉽게 일어나 출처도 모르는 코인이 많이 생성되곤 했다.

3.2. 완료된 거래정보의 변경 불가 각 거래정보의 해시값은 머클트리를 통해 머클루트 해시값에 사용되고, 결국 해당 거래가 포함된 블록의 블록해시값에 사용되어서 영향을 미친다. 이 블록해시는 다음 블록 M이 생성될때 '이전 블록해시'로 저장되어 블록 M의 블록해시값에 사용된다.

따라서, 어떤 거래정보가 변경되면 그 거래정보가 포함된 블록의 블록해시를 새로 계산해야 하고, 그래야 유효한 블록으로 수정되어진다. 연이어 그 다음 블록들의 블록해시가 계속 새롭게 계산되어져야하고, 결국은 새로 수정된 블록들이 완성된다.

만약 어떤 악의적인 노드가 이전의 블록 M의 거래정보를 변경할 목적으로, 블록 M을 무시하고 새로운 블록을 다시 채굴한다고 하자. 그러는 사이에 이미 다른 선의의 노드들은 거래정보가 변경되지 않은 원래의 블록체인에 이어서 평균 10분 간격으로 새로운 블록들을 계속해서 붙여나가고 있다. 즉, 악의적인 노드의 블록체인이 완성되어도 블록체인의 길이는 다른 선의의 노드들이 보유한 블록체인의 길이보다 짧을 수 밖에 없고, 결국 두 블록체인이 만나는 순간 길이가 짧은 블록체인은 버려지게 된다.

혹 악의적인 노드의 연산 능력이 충분히 빨라서 블록체인의 길이가 정상 블록체인보다 더 길어지게 된다면, 이렇게 되는 순간 악의적인 노드에 의해 변경된 거래정보가 유효한 거래 정보로서 전체 블록체인 네트워크에 퍼지게 되며 과거 거래정보의 변경이 성공하게 된다. 이를 *51% 공격*이라고 한다.

하지만 경제적인 관점에서 생각해보면 발생할 가능성이 없다. 일단, 거래 정보가 변경될 수 있다는 사실이 알려지게 되면 블록체인의 신뢰는 깨지게 된다. 만약 악의적인 노드가 오랫동안 가장 큰 연산 능력을 가지고 있었다면, 악의적인 노드가 생성한 블록이 많을 것이고 그에 따른 보상액도 많이 보유하고 있을텐데, 블록체인의 신뢰가 붕괴되면 큰 피해를 보는 쪽은 오히려 자신이기 때문에 거래정보를 변경할 경제적 동기가 없다. 따라서, 경제적으로 이익을 볼 수 없는 거래 정보의 변경은 사실상 발생하지 않게 된다.

3.3. 비잔틴 장군의 딜레마 비트코인의 놀라운 점은 관리주체가 없는데도 위조화폐나 시세조작 등의 문제가 발생없이 작동하는 점이다. 이는 비트코인이 비잔틴 장군의 딜레마(*분산화 컴퓨팅*에서 발생할 수 있는 *신뢰와 합의*의 문제에 대한 우화) 대한 해결책을 구현한 것이기 때문이다. [3]

비잔틴 장군의 딜레마: 배신자의 존재에도 불구하고 옳은 지휘관들이 동일한 공격 계획을 세우기 위해서 얼마만큼 존재해야 하며, 어떤 규칙을 따라 교신해야하는지에 대한 문제다.

- 비잔틴 시대에 적군의 성을 둘러싼 영지를 차지하고 있는 비잔틴 장군들이 있다.
- 적군의 성을 차지하기 위해서는, 장군들은 같은날 같은시간에 동시에 과반수 이상의 군대로 공격하면 된다.
- 장군들 중에는 전투에 승리하는것을 원치않는 배신자가 포함되어있지만 누구인지 알수가 없다.
- 장군들간의 연락은 반드시 1대1로 통신병을 통해서만 가능하고, 다수간에 동시연락을 할수가 없다.

비트코인에서는 마지막 거래를 단순한 방법으로 확정한다. (사토시 나카모토의 논문에 제시됨)

- 10분이 걸리는 블록 생성을 가장 먼저 성공한 컴퓨터에게 장부 확정의 권리를 부여한다.
- 나머지 컴퓨터의 절반 이상이 그 사실을 확인하는 순간 거래가 인정되는 구조이다.
- 이것을 조작하려면 한 사람이 네트워크의 절반 이상을 장악(51% 공격)해야 하는데 현실적으로 불가능하다.

3.4. 블록체인의 핵심 거대한 분산 공개 장부이며, 그 장부 안에 포함된 개별 거래는 모두 전자서명이 같이 있어서 은행이나 다른 제 3자의 개입이 없어도 진본임을 검증할 수 있다. 즉, 거래 당사자간의 신뢰 확보를 위해 중앙 기관을 필요로 하지 않는 탈중앙화(Decentralization)를 달성한 최초의 소프트웨어 기술이다.

전 세계에 노드들이 분산 되어 있어서 어느 한 지점에 장애나 공격이 발생하더라도 블록체인이라는 네트워크 전체는 문제 없이 계속 진행된다.

작업 증명이라는 수학적 계산 작업과 경제 관점에서의 논리를 통해 위·변조가 불가능한 구조를 갖고 있다.

분산 환경에 전파되는 과정에서 분기가 발생시, 가장 길이가 긴 블록체인을 유효한 것으로 선택한다.

비트코인은 화폐에 한정되어 있지만, 이더리움 등 최근 개발되고 있는 암호화폐 들은 블록 체인 위에서 당사자간의 계약을 프로그램으로 실행시킬 수 있는 탈중앙화 플랫폼을 지향하고 있다. 블록 체인이 탈중앙화 플랫폼의 바탕이 되기 때문에 세상을 바꿀 수 있는 기술이라고 평가받는 것이다.

4차 산업의 핵심기술은 인공지능과 빅데이터인데, 분명 한 가지가 더 있다면 블록체인이다. 확산되는 공유경제 속에서 데이터 및 자산 거래의 신뢰성을 제공하여 거래의 효율성을이룰수 있기 때문이다.

[3]이 딜레마는 1982년 레슬리 램포트 등 3명의 컴퓨터 공학자들이 마이크로소프트 의뢰로 수행한 연구 논문을 통해 이슈화 되었는데, 아이러니 하게도 논문에서는 불가능함을 증명하였다.

Part 2

Individual Lectures

Invited Talks

THE STRUCTURE OF AUTOMORPHISM GROUPS OF CLTTF ARTIN GROUPS

YOUNGJIN CHO

Abstract. We obtain a presentation of the automorphism group of a CLTTF Artin group. In fact, it is generated by inversions, partial conjugations, graph automorphisms, and partial reflections. The complication due to the non-uniqueness of defining graphs is managed by surprisingly simple automorphisms called partial reflections. Relations are basically given by conjugation actions of one type of automorphisms to the other.
*This work is a part of the dissertation theses of the author.

1. Introduction

Let Γ be a simple graph such that every edge e carries an integer label $m_e \geq 2$. An *Artin group* A_Γ with a defining graph Γ is generated by vertices of Γ and related by

$$\underbrace{sts\cdots}_{m_e} = \underbrace{tst\cdots}_{m_e}$$

for each edge e joining s and t. A set of generators is called that of *Artin generators* if a defining graph can be recovered by using them as vertices. For example, the 4-strand braid group is an Artin group defined by the triangle with edge labels 2, 3, 3. If all edge labels are 2, A_Γ is called a *right-angled Artin group*. An Artin group is *rigid* if it has a unique defining graph, or equivalently, if a set of Artin generators is sent to any other set of Artin generators by an automorphism of the Artin group. Right-angled Artin groups [**5**] and Artin groups of finite type [**1**] are known to be rigid. In general, Artin groups need not be rigid.

From now on, a graph Γ is edge-labeled and $V(\Gamma)$ and $E(\Gamma)$ denote the set of vertices and the set of edges, respectively. Suppose that for a graph Γ, $V(\Gamma)$ has disjoint subsets U and V such that V generates Artin subgroup A_V of finite type and each vertex in $V(\Gamma) - (U \cup V)$ that is adjacent to a vertex in U is adjacent to every vertex in V by an edge labeled 2. In [**2**], authors propose a typical way of obtaining a new defining graph from Γ under this circumstance. Recall that there is a unique element λ in A_V, which is the longest element in the associated Coxeter group, such that the conjugation by λ permutes elements of V. A new set S' of Artin generators is obtained from $V(\Gamma)$ by replacing elements of U by their conjugates by λ and then S' determines a new defining graph Δ that is called a *twist* of Γ on U along V. In fact Δ is obtained from Γ by replacing each edges joining a vertex u in U and a vertex v in V by a new edge joining u and $\lambda v \lambda^{-1}$. We may identify $V(\Delta)$ with $V(\Gamma)$ since only edges are altered. There is an obvious isomorphism : $A_\Gamma \to A_\Delta$ called a *twist isomorphism*, that sends each $v \in V$ to $\lambda v \lambda^{-1}$ and fixes other generators. It is a conjecture that two defining graphs of an Artin group are *twist-equivalent*, that is, related via a series of twists.

There have been extensive researches on automorphism groups of free abelian groups, free groups, and more generally, right-angled Artin groups. There are also many complete results on automorphism groups of some Artin groups of finite type. Nielsen automorphisms or Whitehead

automorphisms on free groups can be adapted to form a set of generators of automorphism groups when they are appropriate. They are usually classified as one of the following types: permutations of generators, inversions, transvections, and partial conjugations. For right-angled Artin groups, peak reduction arguments can be employed to obtain a complete set of relations among generators [**3, 4**].

In this article we find a presentation of the automorphism group $\mathrm{Aut}(A_\Gamma)$ of a CLTTF Artin group A_Γ. A difficulty lies on handling twist isomorphisms that obviously influence the automorphism group. Another difficulty is the fact that a (label-preserving) graph isomorphism $: \Gamma_1 \to \Gamma_2$ does not induce an automorphism on A_Γ in general even though Γ_1 and Γ_2 are twist-equivalent to Γ. This is because an automorphism is defined on a fixed presentation of A_Γ. We overcome these by introducing a group $\mathrm{Iso}(\Gamma)$ consisting of equivalence classes of graph isomorphisms among graphs twist-equivalent to Γ and its subgroup of partial reflections.

2. A short exact sequence for $\mathrm{Aut}(A_\Gamma)$

Let Γ be a CLTTF graph. Then two kinds of inversions are automorphisms of A_Γ. The *global inversion* sending s to s^{-1} for all vertices s is always an automorphism. If t is a vertex of valence 1 and the incident edge with ends s, t has an even label, there is an automorphism, called a *leaf inversion*, that sends t to $(sts)^{-1}$ and fixes others. Let $\mathrm{Inv}(A_\Gamma)$ denote the subgroup of A_Γ generated by the global inversion and leaf inversions. Then $\mathrm{Inv}(A_\Gamma) \cong (\mathbb{Z}/2\mathbb{Z})^{k+1}$ where k is the number of vertices of valence 1.

A partial conjugation can be an automorphism of A_Γ or a twist isomorphism when Γ splits along T, that is, $\Gamma = \Gamma' \cup \Gamma''$ and $T = \Gamma' \cap \Gamma''$ for full subgraphs Γ' and Γ'' of Γ where T is an edge or a vertex. Let g be an element of the centralizer of the subgroup A_T in A_Γ. A *partial conjugation* on Γ' is an automorphism sending v to gvg^{-1} for $v \in V(\Gamma')$ and fixing others. In the degenerate case that Γ'' is a vertex s, a partial conjugation becomes an inner automorphism that is a conjugation by s. Let $\mathrm{PC}(A_\Gamma)$ denotes the subgroup of $\mathrm{Aut}(A_\Gamma)$ generated by partial conjugations.

In addition, if T is an edge $\{s, t\}$ of an odd label m or its end vertex s in the above splitting, let λ be the m-fold product $st \cdots s$. Then the conjugation by λ switch s and t. Let Δ be the twist of Γ on $V(\Gamma') - \{s, t\}$ along $\{s, t\}$. Then the partial conjugation that conjugates generators in $V(\Gamma') - \{s, t\}$ by λ and fixes other generators gives a twist isomorphism $: A_\Gamma \to A_\Delta$. Two graphs are *twist-equivalent* if they are related by a finite sequence of twits. John Crisp showed that all defining graphs of A_Γ are twist-equivalent if Γ is CLTTF [**2**], which we do not use in this article. We always assume that every graph twist-equivalent to Γ has the same set of vertex labels determined by Γ. These two kind of partial conjugations generates a set $\mathrm{PT}(\Gamma)$ of morphisms in the category of Artin groups defined by graphs twist-equivalent to Γ. In another words, $\mathrm{PT}(\Gamma)$ is generated by $\mathrm{PC}(A_\Gamma)$ and twist isomorphisms under composition.

Given a defining graph Γ, consider the set of all (edge-label preserving) graph isomorphisms $: \Gamma_1 \to \Gamma_2$ for graphs Γ_1 and Γ_2 twist-equivalent to Γ. Two graph isomorphisms are equivalent if they agree as functions on the sets of vertices, that is, $\alpha \sim \beta$ if $\alpha(v) = \beta(v)$ for all $v \in V(\Gamma)$. Let $\mathrm{Iso}(\Gamma)$ be the set of equivalent classes. We can think of a class in $\mathrm{Iso}(\Gamma)$ as a bijection on $V(\Gamma)$ that can be realized by a graph isomorphism among graphs twist-equivalent to Γ and its representative is a realization. Thus $\mathrm{Iso}(\Gamma)$ forms a group under composition. Given a class in $\mathrm{Iso}(\Gamma)$ and a graph Δ_1 twist-equivalent to Γ, there is a unique graph isomorphisms $: \Delta_1 \to \Delta_2$ that represents the class since Δ_1 and the bijection on vertices forces edges of Δ_2 to turn the bijection into a graph isomorphism.

An isomorphism $\varphi : A_\Gamma \to A_\Delta$ is *inversion-free* if the exponent sum of the word $\varphi(v)$ is 1 for all $v \in V(\Gamma)$. An inversion-free isomorphism sends each vertex of Γ to a conjugate of a vertex of Δ. For an isomorphism φ, there is a unique $\iota \in \mathrm{Inv}(A_\Gamma)$ such that $\varphi \circ \iota$ is inversion-free. A *chunk* in Γ is a maximal full subgraph of Γ that does not split any more along an edge or a vertex. Since

vertices in a chunk are conjugated by the same product of words under partial conjugations in $\mathrm{PT}(\Gamma)$, it is natural to expect that an inversion-free automorphism of A_Γ conjugates vertices in a chunk by a fixed group element. This prediction is verified by Chunk Invariance Lemma introduced and proved by John Crisp in [**2**].

LEMMA 2.1 (Chunk Invariance Lemma [**2**]). *For an inversion-free isomorphism $\varphi : A_\Gamma \to A_\Delta$ and each chunk C of Γ, there is an element $a \in A_\Delta$ such that the restriction of $a^\# \circ \varphi$ to the subgroup A_C is induced from a (label-preserving) graph isomorphism $: C \to D$ where $a^\#$ is the conjugation by a and D is a chunk in Δ.*

Fix a base chunk B in Γ. We construct an epimorphism $\pi_B : \mathrm{Aut}(A_\Gamma) \to \mathrm{Iso}(\Gamma)$ using Chuck Invariance Lemma. This construction is essentially due to John Crisp who worked on a groupoid setting. In fact we will show that for an automorphism $\varphi \in \mathrm{Aut}(A_\Gamma)$, there are $\gamma \in \mathrm{PT}(\Gamma)$ and $\iota \in \mathrm{Inv}(A_\Gamma)$ such that $\gamma \circ \iota \circ \varphi$ gives a graph isomorphism that represents a class in $\mathrm{Iso}(\Gamma)$. Given an inversion-free automorphism $\varphi \in \mathrm{Aut}(A_\Gamma)$, there is an innerautomorphism $\gamma_0 \in \mathrm{PC}(\Gamma)$ such that $\gamma_0 \circ \varphi$ gives a graph isomorphism on B by Chunk Invariant Lemma. That is, $\gamma_0 \circ \varphi$ sends each vertex of B to a vertex of a chunk B' in Γ and gives a graph isomorphism $: B \to B'$.

For an inductive step, we are given an inversion-free isomorphism $\varphi : A_\Gamma \to A_\Delta$ for a graph Δ twist-equivalent to Γ such that φ is a graph isomorphism on some connected subgraph Γ' of Γ that is a union of chunks including B. Let C be a chunk of Γ that is not in Γ' but which intersects Γ'. We are done if there is $\gamma \in \mathrm{PT}(\Gamma)$ such that $\gamma \circ \varphi$ is an isomorphism $: A_\Gamma \to A_{\Delta_1}$ that is a graph isomorphism on $\Gamma' \cup C$. Chunk Invariance Lemma gives $a \in A_\Delta$ such that $a^\# \circ \varphi$ gives a graph isomorphism on C. If $\Gamma' \cap C$ is an edge $\{s, t\}$ of label m. Then φ and $a^\# \circ \varphi$ must have the same image $\{s_1, t_1\}$ of the intersection $\{s, t\}$ as an unoriented edge. Let $\gamma \in \mathrm{PT}(\Gamma)$ be the partial conjugation by a on vertices in the connected component of $\Delta - \{s_1, t_1\}$ containing the image of C under $a^\# \circ \varphi$. Then $\gamma \circ \varphi$ gives a graph isomorphism on $\Gamma' \cup C$. If $\Gamma' \cap C$ is a vertex s. Let s_1 and s_2 be the image of s under φ and $a^\# \circ \varphi$, respectively. It is possible that $s_1 \neq s_2$ but there must be an edge path of odd labelled edges from s_1 to s_2 in Δ since Γ and Δ are twist-equivalent. Let $\gamma \in \mathrm{PT}(\Gamma)$ be the partial conjugation by a on vertices in the connected component of $\Delta - \{s_2\}$ containing the image of C under $a^\# \circ \varphi$. Then $\gamma \circ \varphi$ gives a graph isomorphism on $\Gamma' \cup C$.

THEOREM 2.2. *We have a short exact sequence:*

$$1 \to \ker(\pi_B) \to \mathrm{Aut}(A_\Gamma) \xrightarrow{\pi_B} \mathrm{Iso}(\Gamma) \to 1.$$

We remark that the epimorphisms π_B and $\pi_{B'}$ differ by an innerautomorphism of A_Γ for distinct base chunks B and B'.

THEOREM 2.3. $\ker(\pi_B) = \mathrm{Inv}(A_\Gamma) \times \mathrm{PC}(A_\Gamma)$.

3. The group $\mathrm{Iso}(\Gamma)$ of graph isomorphisms

We define a special family of graph isomorphisms called *partial reflections* that are sources for graph isomorphisms that are not graph automorphisms. Consider a subgraph Γ' bounded by separating slides $\{e_i\}$ and separating vertices of slides $\{\ell_j\}$ in Γ so that slides $\{\ell_j\}$ lie outside of Γ'. Let E_i or L_j be subgraphs outside of Γ' bounded by slide e_i or ℓ_j, respectively. A *partial reflection* on Γ' is a graph isomorphism $\tau : \Gamma \to \Delta$ that fixes subgraphs E_i and is a graph automorphism on L_j that switches two end vertices of ℓ_j so that the set of bad or neutral slides for τ is exactly $\{e_i, \ell_j\}$. In fact, for each $e_i = \{s, t\}$ and an edge $\{s, v\}$ with $v \neq t$ in Γ', $\{\tau(s), \tau(v)\}$ is not an edge of Γ but $\{\tau(t), \tau(v)\}$ is. The similar thing holds when the roles of s and t are exchanged. For each $\ell_j = \{s_1, s_2, \cdots, s_k\}$ with the separating vertex s_1 and an even

positive integer k and an edge $\{s_1, v\}$ with $v \neq s_2$ in Γ', $\{\tau(s_1), \tau(v)\}$ is not an edge of Γ but $\{\tau(s_k), \tau(v)\}$ is.

For any partial reflection τ, τ^2 is obviously a graph automorphism. If Γ' is bounded only by separating edges, then it may contains *rotors*. For example, Figure 1 depicts a partial reflection on a subgraph containing a rotor of order 4. This partial reflection switches $v_1 \leftrightarrow v_2$ and $v_3 \leftrightarrow v_4$ and rotates $v_5 \to v_6 \to v_7 \to v_8 \to v_5$. If Γ' contains rotors of orders $2r_i$ in general, partial reflections on Γ' form a subgroup of $\mathrm{Iso}(\Gamma)$ that is isomorphic to the cyclic group of order m where m is the least common multiple of $2r_i$. This subgroup intersects $\mathrm{Aut}(\Gamma)$ at a subgroup isomorphic to the cyclic group of order $m/2$. Partial reflections on distinct subgraphs obviously commute. Let $\mathrm{PR}(\Gamma)$ denote the subgroup of $\mathrm{Iso}(\Gamma)$ generated by partial reflections. Then $\mathrm{PR}(\Gamma) \cap \mathrm{Aut}(\Gamma)$ is generated by graph automorphisms that rotate rotors.

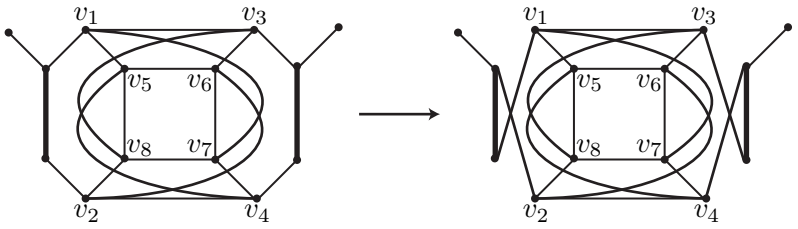


FIGURE 1. Rotor of order 4

THEOREM 3.1. *We have a short exact sequence:*

$$1 \to \mathrm{PR}(\Gamma) \to \mathrm{Iso}(\Gamma) \to \frac{\mathrm{Aut}(\Gamma)}{\mathrm{PR}(\Gamma) \cap \mathrm{Aut}(\Gamma)} \to 1.$$

If every partial reflection has no rotors, that is, every partial reflection has order 2, then $\mathrm{PR}(\Gamma) \cap \mathrm{Aut}(\Gamma) = \{1\}$ and we have a splitting short exact sequence:

$$1 \to \mathrm{PR}(\Gamma) \to \mathrm{Iso}(\Gamma) \to \mathrm{Aut}(\Gamma) \to 1.$$

A graph automorphism in $\mathrm{Aut}(\Gamma)$ gives an automorphism in $\mathrm{Aut}(A_\Gamma)$ that permutes generators. The subgroup $\mathrm{PR}(\Gamma)$ of $\mathrm{Iso}(\Gamma)$ is lifted into $\mathrm{Aut}(A_\Gamma)$ via the lifting function $\sigma : \mathrm{Iso}(\Gamma) \to \mathrm{Aut}(A_\Gamma)$ discussed in Thereom 2.2. Recall the partial reflection τ given in its definition earlier in this section. Since τ is a graph isomorphism : $\Gamma \to \Delta$, it induces an isomorphism $\varphi_\tau : A_\Gamma \to A_\Delta$ that permutes vertices on the interior of Γ' by τ. If the subgraph Γ' contains no other slides inside, we call τ a *small partial reflection*. Small partial reflections obviously generates $\mathrm{PR}(\Gamma)$. Assume that τ is a small partial reflection. Our choice $\sigma(\tau)$ of lifts of τ is an automorphism of A_Γ that is a composition of φ_τ and partial conjugations on vertices of E_i or L_j by their quasi-centers if E_i or L_j do not contain the base chunk B, and partial conjugations on vertices of $\Gamma - E_i$ or $\Gamma - L_j$ if E_i or L_j contain B. Since each ℓ_i stays in L_i, partial conjugations on E_i or L_j commute each other and a partial conjugation on $\Gamma - E_i$ or $\Gamma - L_j$ is a composition of a conjugation on E_i or L_j and a cancelling innerautomorphism. We note that only one among E_i and L_j may contain B if any. Up to innerautomorphisms, $\sigma(\tau)$ is well-defined regardless of the composing order of partial conjugations. We will make a canonical choice for the composing order so that the partial conjugation on E_i or L_j that contain the base chunk performed last together with the cancelling innerautomorphism.

Given α, β that are partial reflections or graph automorphisms, let $\delta(\alpha, \beta) \in \mathrm{PC}(\Gamma)$ be such that $\delta(\alpha, \beta)\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$. We obtain relations among lifts via $\delta(\alpha, \beta)$. If α or β is a graph automorphism, then $\delta(\alpha, \beta) = 1$. For a partial reflection τ, $\delta(\tau, \tau)$ is the composition of the same partial conjugations as in $\sigma(\tau)$ but by their centers instead of their quasi-centers. Let τ_1 and τ_2 be small partial reflections on subgraphs Γ_1 and Γ_2, respectively. If no slide for τ_1 invades Γ_2 and vice versa, there is a lift $\sigma(\tau_1\tau_2)$ such that $\delta(\tau_1, \tau_2) = 1$.

4. Conclusion and an example

The automorphism group $\mathrm{Aut}(A_\Gamma)$ of a CLTTF Artin group A_Γ is generated by inversions, partial conjugations, graph automorphisms, and small partial reflections. Graph automorphisms and small partial reflections generate a finite group $\mathrm{Iso}(\Gamma)$. In particular, if all small partial reflections are of order 2, we have

$$\mathrm{Iso}(\Gamma) \cong \mathrm{PR}(\Gamma) \rtimes \mathrm{Aut}(\Gamma)$$

where $\alpha\tau\alpha^{-1}$ is the partial reflection on $\alpha(\Gamma')$ for a partial reflection τ on a subgraph Γ' and a graph automorphism α.

We had $\ker(\pi_B) \cong \mathrm{Inv}(A_\Gamma) \times (\mathrm{Inn}(A_\Gamma) \rtimes \mathrm{PC}_B(A_\Gamma))$ for the epimorphism $\pi_B : \mathrm{Aut}(A_\Gamma) \to \mathrm{Iso}(\Gamma)$. Partial reflections or graph automorphisms act on $\ker(\pi_B)$ via conjugations by their lifts. In this section, we abuse notations so that α denotes our choice $\sigma(\alpha)$ of its lifts. Let α be a graph automorphism. For an inversion ι at a terminal vertex v, $\alpha\iota\alpha^{-1}$ is the inversion at $\alpha(v)$. The global inversion is in the center of $\mathrm{Aut}(A_\Gamma)$. For a partial conjugation f, $\alpha f\alpha^{-1} = f'$ where $C(f') = \alpha(C(f))$, $\lambda_{f'} = \alpha(\lambda_f)$. In particular, $\alpha a^{\#}\alpha^{-1} = (\alpha(a))^{\#}$ for $a \in A_\Gamma$.

Our lift of a small partial reflection τ is given by $a^{\#}g_n \cdots g_1\varphi_t au$ for an innerautormorphism $a^{\#}$, partial conjugation isomorphisms g_i and an isomorphism φ_τ. For an inversion ι at a terminal vertex v, $\tau\iota\tau^{-1}$ is the inversion at $\varphi_\tau(v)$. For a partial conjugation $f \in \mathrm{PC}(A_\Gamma)$, one can derive that

$$\tau f\tau^{-1} = (a^{\#}g_n \cdots g_1\varphi_\tau)f(a^{\#}g_n \cdots g_1\varphi_\tau)^{-1} = b^{\#}f'g'_n \cdots g'_1$$

where $f', g'_1, \ldots, g'_n$ are partial conjugations in $\mathrm{PC}_B(A_\Gamma)$ such that $C(f') = \varphi_\tau(C(f))$, $C(g'_i) = C(g_i)$. We omit the formulas for b, $\lambda_{f'}$, and $\lambda_{g'_i}$ since they become rather complicated if f is, for example, a partial conjugation via a complicated central loop.

Finally we consider an example given in the left of Figure 2. Thick edges are labelled 3 and all others are labelled 4. Let the middle square be the base chunk. The global inversion and a leaf inversion at v_{12} generates $\mathrm{Inv}(A_\Gamma) \cong (\mathbb{Z}/2\mathbb{Z})^2$. Partial conjugation along two separating odd-labelled edges generate $\mathbb{Z}^2$. The separating vertex v_3 has 11 independent central loops and so its centralizer is isomorphic to $\mathbb{Z} \times F_{11}$. Thus $\mathrm{PC}_B(A_\Gamma) \cong \mathbb{Z} \times (F_{11} \rtimes \mathbb{Z}^2)$. We have relations in $\mathrm{PC}(A_\Gamma)$.

There is one graph automorphism switching v_9 and v_{10}. There are partial reflections on the left square and on the right square. There are two independent partial reflections on the top square. Thus $\mathrm{Iso}(\Gamma)$ is generated by five graph isomorphisms. In fact, $\mathrm{Iso}(\Gamma) \cong ((\mathbb{Z}/2\mathbb{Z})^2 \rtimes (\mathbb{Z}/2\mathbb{Z})^2) \rtimes \mathbb{Z}/2\mathbb{Z}$. Conjugate actions of $\mathrm{Iso}(\Gamma)$ on other generators explained above complete a set of relations.

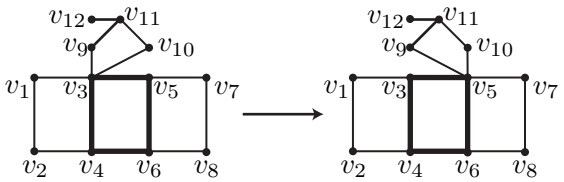


FIGURE 2. Partial reflection on the top chunk

Bibliography

[1] N. Brady, J. McCammond, B. Mühlherr, and W. Neumann, *Rigidity of Coxeter groups and Artin groups*, Geometriae Dedicata **94** (2002) 91–109.

[2] J. Crisp, *Automorphisms and abstract commensurators of 2-dimensional Artin groups*, Geom. Topol. **9** (2005) 1381–1441.

[3] M. B. Day, *Peak reduction and finite presentations for automorphism groups of right- angled Artin groups*, Geom. Topol. **13** (2009) 817–855.

[4] M. B. Day, *Full-featured peak reduction in right-angled Artin groups*, Algebr. Geom. Topol. **14** (2014) 1677–1743.

[5] C. Droms, *Isomorphisms of graph groups*, P. Am. Math. Soc. **100** (1987) 407–408.

[6] E. Godelle, *Parabolic subgroups of Artin groups of type FC*, Pac. J. Math. **208** (2003) 243–254.

[7] E. Godelle, *Artin-Tits groups with CAT(0) Deligne complex*, J. Pure Appl. Algebra **208** (2007) 39–52.

BIPARTITE INTRINSICALLY KNOTTED GRAPHS WITH 23 EDGES

HYUNGJUN KIM*, THOMAS MATTMAN AND SEUNGSANG OH

Abstract. Every bipartite intrinsically knotted graph with 23 edges and $\delta(G) \geq 3$ contains C_{14} or Cousin 110 of $E_9 + e$ family.

1. Introduction

Throughout the paper, an embedded graph will mean one embedded in $\mathbb{R}^3$. A graph is *intrinsically knotted* if every embedding of the graph in $\mathbb{R}^3$ contains a non-trivially knotted cycle. Conway and Gordon [**2**] showed that the complete graph K_7 is intrinsically knotted. Foisy [**4**] showed that $K_{3,3,1,1}$ is also intrinsically knotted. A graph H is called a *minor* of the graph G if H can be obtained from G by deleting or contracting edges. A graph G is said to be *minor minimal intrinsically knotted* if G is intrinsically knotted and its every proper minor is not intrinsically knotted. Robertson and Seymour [**14**] proved that for any property of graphs, there is a finite set of graphs minor minimal with respect to that property. In particular, there are only finitely many minor minimal intrinsically knotted graphs, but finding the complete set is still an open problem.

A ∇Y *move* is an exchange operation on a graph that removes all edges of a 3-cycle abc and then add a new vertex v and connect it to each vertex of the 3-cycle, as shown in Figure 3. We say two graphs G and G' are cousins if G' is obtained from G by a finite sequence of ∇Y and $Y\nabla$ moves. The set of all cousins of G is called the G family.

Since ∇Y or $Y\nabla$ moves do not change the number of edges of the graph, all graphs in the family have same number of edges. Note that ∇Y move preserves intrinsic knottedness [**13**], and $Y\nabla$ move does not preserve intrinsic knottedness [**3**]. It is known [**2, 4, 10**] that K_7 and the 13 graphs obtained from K_7 by ∇Y moves, and $K_{3,3,1,1}$ and the 25 graphs obtained from $K_{3,3,1,1}$ by ∇Y moves are minor minimal intrinsically knotted.

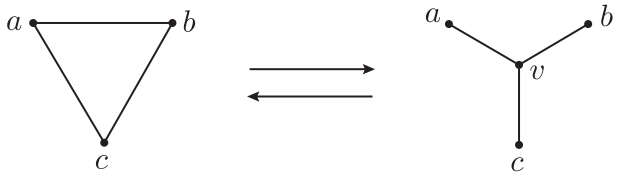


Figure 3. ∇Y and $Y\nabla$ moves

Johnson, Kidwell and Michael [**7**], and, independently, Mattman [**12**], showed that intrinsically knotted graphs have at least 21 edges. Lee, Kim, Lee and Oh [**11**], and, independently, Barsotti and Mattman [**1**] showed that K_7 and the 13 graphs obtained from K_7 by ∇Y moves are the only minor minimal intrinsically knotted graphs with 21 edges. The $K_{3,3,1,1}$ family consists of 58 graphs, and Goldberg, Mattman and Naimi [**5**] showed that all of them are minor minimal intrinsically knotted They also studied the $E_9 + e$ family which consists of 110 graphs, and showed that all graphs of them are intrinsically knotted, and exactly 33 graphs among them are minor minimal intrinsically knotted.

A *bipartite* graph is a graph whose vertices can be divided into two disjoint sets A and B such that every edge connects a vertex in A to one in B. We say that a graph G is *minor minimal bipartite intrinsically knotted*, if G is an intrinsically knotted bipartite graph, but no proper minor of G is intrinsically knotted and bipartite. Since contracting edges can lead to a bipartite minor for a graph that was not bipartite to begin with, it is easy to construct examples of graphs that are not themselves bipartite intrinsically knotted even though they have a minor that is minor minimal bipartite intrinsically knotted. Nonetheless, Robertson and Seymour's [**14**] Graph Minor Theorem guarantees that there are a finite number of minor minimal bipartite intrinsically knotted graphs and every bipartite intrinsically knotted graph must have one as a minor. It is known that there are exactly two minor minimal bipartite intrinsically knotted graphs, which are *the Heawood graph*(C_{14}) and the Cousin 110 of the $E_9 + e$ family [**8**].

Our goal in this paper is to show there does not exist any minor minimal intrinsically knotted graph with 23 edges which is bipartite. We first classify bipartite intrinsically knotted graphs which consists 23 edges and vertices with degree 3 or more.

THEOREM 1.1. *There are exactly five graphs with 23 edges and every vertex has degree 3 or more that are bipartite intrinsically knotted: 2 graphs are obtained from Cousin 110 of the $E_9 + e$ family by adding an edge, and 4 graphs are obtained from C_{14} by adding 2 edges.*

Since minor minimal intrinsically knotted graphs do not have vertices with degree 1 or 2, we also have the following corollary.

COROLLARY 1.2. *There is no minor minimal intrinsically knotted graphs with 23 edges that are bipartite.*

2. Terminology and strategy

The notation and terminology used in this paper follow those employed in the previous paper [**8**]. Let $G = (A, B, E)$ denote a bipartite graph with 23 edges whose partition has the parts A and B with E denoting the edges of the graph. For distinct vertices a and b, let $G \setminus \{a, b\}$ denote the graph obtained from G by deleting two vertices a and b. Deleting a vertex means removing the vertex, interiors of all edges adjacent to the vertex and remaining isolated vertices. Let $G_{a,b}$ denote the graph obtained from $G \setminus \{a, b\}$ by deleting all degree 1 vertices, and $\widehat{G}_{a,b} = (\widehat{V}_{a,b}, \widehat{E}_{a,b})$ denote the graph obtained from $G_{a,b}$ by contracting edges adjacent to degree 2 vertices, one by one repeatedly, until no degree 2 vertex remains. The degree of a, denoted by $\deg(a)$, is the number of edges adjacent to a. We say that a is adjacent to b, denoted by $a \sim b$, if there is an edge connecting them. If they are not adjacent, we denote $a \nsim b$. If a is adjacent to more than a vertex, say $b, \ldots, b'$, then we write $a \sim \{b, \ldots, b'\}$. Note that $\sum_{a \in A} \deg(a) = \sum_{b \in B} \deg(b) = 23$ by the definition of bipartition. We need some notations to count the number of edges of $\widehat{G}_{a,b}$.

- $E(a)$ is the set of edges that are adjacent to a vertex a.
- $V(a) = \{c \in A \cup B \mid \mathrm{dist}(a, c) = 1\}$
- $V_n(a) = \{c \in A \cup B \mid \mathrm{dist}(a, c) = 1,\ \deg(c) = n\}$
- $V_n(a, b) = V_n(a) \cap V_n(b)$
- $V_Y(a, b) = \{c \in A \cup B \mid \exists\ d \in V_3(a, b)$ such that $c \in V_3(d) \setminus \{a, b\}\}$

Obviously in $G \setminus \{a, b\}$ for some distinct vertices a and b, each vertex of $V_3(a, b)$ has degree 1. Also each vertex of $V_3(a), V_3(b)$ (but not of $V_3(a, b)$) and $V_4(a, b)$ has degree 2. Therefore to derive $\widehat{G}_{a,b}$ all edges adjacent to a, b and $V_3(a, b)$ are deleted from G, followed by contracting one of the remaining two edges adjacent to each vertex of $V_3(a)$, $V_3(b)$, $V_4(a, b)$ and $V_Y(a, b)$ as in Figure 4 (a). Thus we have the following equation counting the number of edges of $\widehat{G}_{a,b}$

which is called the *count equation*;

$$|\widehat{E}_{a,b}| \leq 23 - |E(a) \cup E(b)| - (|V_3(a)| + |V_3(b)| - |V_3(a,b)| + |V_4(a,b)| + |V_Y(a,b)|).$$

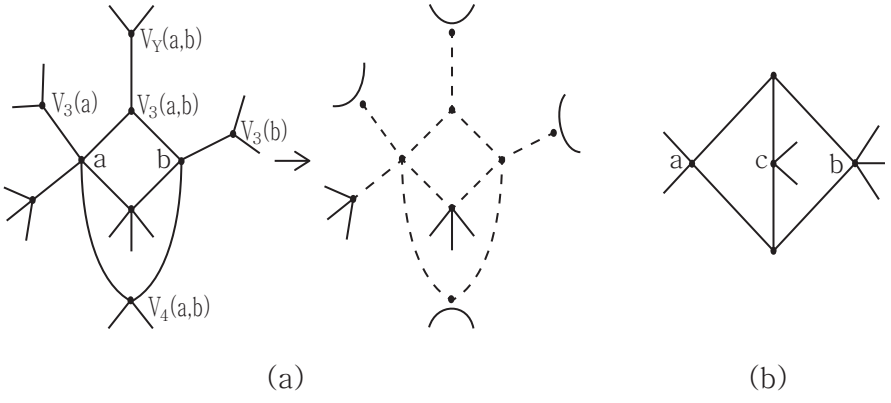


FIGURE 4. Deriving $\widehat{G}_{a,b}$

For short, write $NE(a,b) = |E(a) \cup E(b)|$ and $NV_3(a,b) = |V_3(a)| + |V_3(b)| - |V_3(a,b)|$. If a and b are adjacent (i.e. $\mathrm{dist}(a,b) = 1$), then $V_3(a,b), V_4(a,b)$ and $V_Y(a,b)$ are all empty sets because G is triangle-free. Note that the derivation of $\widehat{G}_{a,b}$ must be handled slightly differently when there is a vertex c in V such that more than one vertex of $V(c)$ is contained in $V_3(a,b)$ as in Figure 4 (b). In this case we usually delete or contract more edges even though c is not in $V_Y(a,b)$.

The following proposition, which was mentioned in [**11**], gives three important conditions that ensure a graph fails to be intrinsically knotted.

PROPOSITION 2.1. *If $\widehat{G}_{a,b}$ is planar, then G is not intrinsically knotted. Especially, if $\widehat{G}_{a,b}$ satisfies one of the following two conditions, then $\widehat{G}_{a,b}$ is planar, so G is not intrinsically knotted.*

(1) $|\widehat{E}_{a,b}| \leq 8$, *or*
(2) $|\widehat{E}_{a,b}| = 9$ *and $\widehat{G}_{a,b}$ is not isomorphic to $K_{3,3}$.*
(3) $|\widehat{E}_{a,b}| = 10$ *and $\widehat{G}_{a,b}$ is not isomorphic to K_5, or does not have $K_{3,3}$ as minor.*

3. Restoring method and G contains a vertex with degree 5 or more

In this section we introduce the *restoring method*, which is introduced in [**9**] and will be used frequently in this paper.

The purpose of this work is to find all candidates of bipartite intrinsically knotted graphs with 23 edges. To prove the main theorem, we distinguish into several cases according to combination of degrees of all vertices and further sub-cases according to connections of some edges among 23 edges in each combination. Let G be a bipartite graph with 23 edges with some distinct vertices a and b, in which we assume that information about degree of every vertex and some edges including all edges incident to a and b is known as shown in Figure 5(a) for example.

First, we examine the number of the edges of the graph $\widehat{G}_{a,b}$. If it has at most eight edges, then it is planar and so G can not be intrinsically knotted by Proposition 2.1. For otherwise, G can rarely be intrinsically knotted. Especially if it has nine edges, $\widehat{G}_{a,b}$ must be isomorphic to $K_{3,3}$ in order to G being intrinsically knotted. In this case, $G_{a,b}$ being a subdivision of $K_{3,3}$ has exactly six vertices with degree 3 and extra vertices with degree 2. The restoring method

is a way to find candidates of such $G_{a,b}$ as shown in Figure 5(b) and (c). Finally we recover G from $G_{a,b}$ by restoring the deleted vertices and edges.

$$\begin{array}{ccccc} \widehat{G}_{a,b} & \to & G_{a,b} & \to & G \\ \| & & & & \\ K_{3,3} & & & & \end{array}$$

By using the count equation and the restoring method, we can find every bipartite intrinsically knotted graph with 23 edges which has a degree 5 or more vertex. We give an example of this case that A consists of one degree 6 vertex, two degree 4 vertices and three degree 3 vertices, and B consists of five degree 4 vertices and one degree 3 vertex with edge information as drawn in Figure 5(a). In the figure, the vertices are labeled by $a_1, \ldots, a_6, b_1, \ldots, b_6$ and the numbers near vertices indicate their degrees.

In this case, G_{a_1,a_2} has six degree 3 vertices $a_3, a_4, a_5, a_6, b_4, b_5$ and three degree 2 vertices b_1, b_2, b_3. Now we examine the number of the edges $|\widehat{E}_{a_1,a_2}|$ of the graph $\widehat{G}_{a_1,a_2}$. Since $NE(a_1, a_2) = 10$, $|V_4(a_1, a_2)| = 3$ and $NV_3(a_1, a_2) = 1$, the count equation gives $|\widehat{E}_{a_1,a_2}| = 9$.

We now assume that $\widehat{G}_{a_1,a_2}$ is isomorphic to $K_{3,3}$. As the bipartition of $K_{3,3}$, we assign the bipartition A' (white vertices) and B' (black vertices) for six degree 3 vertices of G_{a_1,a_2}. Since all four vertices a_3, a_4, a_5, a_6 have degree 3, b_4 is not adjacent to b_5 ($b_4 \not\sim b_5$) in $\widehat{G}_{a_1,a_2}$. This implies that b_4 and b_5 should be in the same partition, say B'. The remaining vertex of B' is a_3 or a_4 without loss of generality. Compare two figures in Figure 5(b) and (c).

In the former case, A' has three vertices a_4, a_5, a_6. The three edges of $\widehat{G}_{a_1,a_2}$ connecting a_3 and A' inevitably passes through three degree 2 vertices b_1, b_2, b_3. The three edges of $\widehat{G}_{a_1,a_2}$ incident to b_4 (or b_5) are directly connected to A'. This G_{a_1,a_2} is drawn by the solid edges in the figure. By restoring the deleted vertices and dotted edges, we recover G. In the latter case, A' has three vertices a_3, a_5, a_6. Then the three edges of $\widehat{G}_{a_1,a_2}$ connecting a_4 and A' passes through three degree 2 vertices b_1, b_2, b_3. The remaining arguments are similar to the former case.

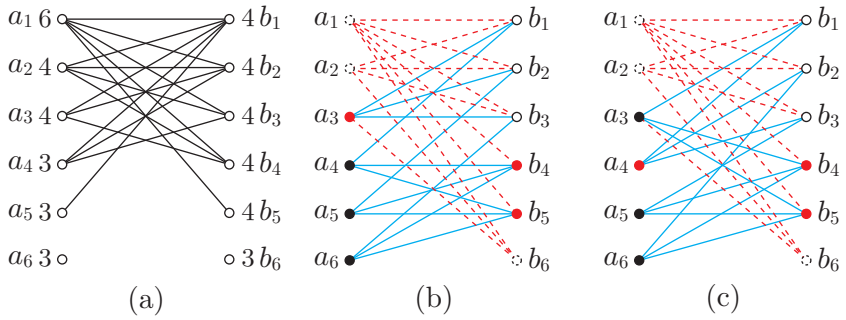


FIGURE 5. Restoring method

4. Twin restoring method and G consists of degree 3 or 4 vertices

In this section we introduce the *twin restoring method*. Sometimes the restoring method applied to $G_{a,b}$ for only one pair of vertices $\{a, b\}$ does not give sufficient information to construct the graph G. In this case, we apply the restoring method to two graphs $G_{a,b}$ and $G_{a',b'}$ simultaneously for different pairs of vertices. This method is called the twin restoring method.

By using the count equation and the twin restoring method, we can find every bipartite intrinsically knotted graph with 23 edges which consists of degree 3 or 4 vertices. We give an example of this case that both A and B consist of two degree 4 vertices and five degree 3 vertices with vertex labelling and partial edge information as drawn in Figure 6(a). In this case, we apply the restoring method to two graphs G_{b_1,b_2} and $G_{b_1',b_2'}$ simultaneously. These two graphs

have the bipartitions assigned as in Figure 6(b) and (c). Since there is exactly one degree 2 vertex in G_{b_1,b_2}, c'_4 and c'_5 are connected by passing through c_4. Similarly $c_5 \sim c'_4$. We use the same argument for the remaining edges of c_5 and c'_5. By recovering the removed vertices and its related edges, we obtain G which contains C_{14} as subgraph.

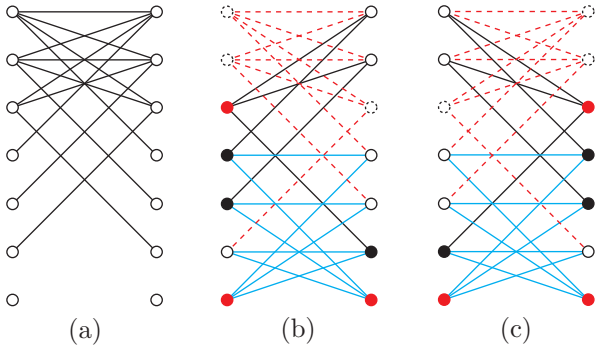


FIGURE 6. Twin restoring method

Bibliography

[1] J. Barsotti and T. Mattman, *Graphs on 21 edges that are not* 2*–apex*, Involve **9** (2016) 591–621.

[2] J. Conway and C. Gordon, *Knots and links in spatial graphs*, J. Graph Theory **7** (1985) 445–453.

[3] E. Flapan and R. Naimi, *The $Y\nabla$ moves does not preserve intrinsic knottedness*, Osaka J. Math. **45** (2008) 107–111.

[4] J. Foisy, *Intrinsically knotted graphs*, J. Graph Theory **39** (2002) 178–187.

[5] N. Goldberg, T. Mattman, and R. Naimi, *Many, many more intrinsically knotted graphs*, Algebr. Geom. Top. **14** (2014) 1801–1823.

[6] R. Hanaki, R. Nikkuni, K. Taniyama, and A. Yamazaki, *On intrinsically knotted or completely* 3*-linked graphs*, Pacific J. Math. **252** (2011) 407–425.

[7] B. Johnson, M. Kidwell, and T. Michael, *Intrinsically knotted graphs have at least* 21 *edges*, J. Knot Theory Ramifications **19** (2010) 1423–1429.

[8] H. Kim, T. Mattman, and S. Oh, *Bipartite intrinsically knotted graphs with 22 edges*, J. Graph Theory **85** (2017) 568–584

[9] H. Kim, T. Mattman, and S. Oh, *More intrinsically knotted graph with 22 edges and the restoring method*, J. Knot Theory Ramifications **27** (2018) 1850059.

[10] T. Kohara and S. Suzuki, *Some remarks on knots and links in spaital graphs*, Knots 90 (Osaka, 1990) (1992) 435–445.

[11] M. Lee, H. Kim, H. J. Lee, and S. Oh, *Exactly fourteen intrinsically knotted graphs have 21 edges*, Algebr. Geom. Topol. **15** (2015) 3305–3322.

[12] T. Mattman, *Graphs of 20 edges are 2-apex, hence unknotted*, Algebr. Geom. Top. **11** (2011) 691–718.

[13] R. Motwani, A. Raghunathan, and H. Saran, *Constructive results from graph minors; linkless embeddings*, Proc. 29th Annual Symposium on Foundations of Computer Science, IEEE (1988) 398–409.

[14] N. Robertson and P. Seymour, *Graph minors XX, Wagner's conjecture*, J. Combin. Theory Ser. B **92** (2004) 325–357.

PRIMITIVE DISKS AND INTERSECTION PATTERN

SANGBUM CHO, YUYA KORA AND JUNG HOON LEE*

Abstract. It is known that the primitive disk complex for a genus-2 Heegaard splitting of the 3-sphere is closed under disk surgery operation. We show that, for a genus-g Heegaard splitting of the 3-sphere with $g \geq 3$, the primitive disk complex for the splitting is not weakly closed under disk surgery operation. That is, there exist two primitive disks in one of the handlebodies of the splitting such that any disk surgery on one along the other one yields no primitive disks. Moreover, we give an example of primitive disks D, E_1, E_2 for a genus-g ($g \geq 4$) Heegaard splitting of the 3-sphere satisfying the following conditions:

- E_1 and E_2 are isotopic.
- Every surgery on E_1 along D yields primitive disks.
- Every surgery on E_2 along D yields non-primitive disks.

1. Introduction

It is well known that any closed orientable 3-manifold can be decomposed into two handlebodies V and W of the same genus g, which we call a *genus-g Heegaard splitting* of the manifold. We denote the splitting by the triple $(V, W; \Sigma)$ where $\Sigma = \partial V = \partial W$ is a closed orientable surface, called a *Heegaard surface*, of genus g. In particular, the 3-sphere admits a Heegaard splitting of each genus $g \geq 0$, and it was shown in [**11**] that the splitting is unique up to isotopy for each genus. A Heegaard splitting $(V, W; \Sigma)$ of a 3-manifold M is said to be *stabilized* if there exists essential disks D and $\overline{D}$ in V and W respectively such that ∂D intersects $\partial \overline{D}$ transversely in a single point. A 3-manifold M admits a stabilized Heegaard splitting of genus-2 if and only if M is one of the 3-sphere, $S^2 \times S^1$ or a lens space $L(p, q)$.

For a handlebody V of genus $g \geq 2$, the *disk complex* $\mathcal{K}(V)$ of V is the simplicial complex defined as follows. The vertices are the isotopy classes of compressing disks in V, and a collection of distinct $k+1$ vertices spans a k-simplex if the vertices are represented by pairwise disjoint disks. The disk complex $\mathcal{K}(V)$ is $(3g-4)$-dimensional and is not locally finite. When the handlebody V is one of the handlebodies of a stabilized genus-g Heegaard splitting $(V, W; \Sigma)$, with $g \geq 2$, the disk complex $\mathcal{K}(V)$ has a special kind of subcomplex, called the *primitive disk complex*. The primitive disk complex, denoted by $\mathcal{P}(V)$, is the full subcomplex of $\mathcal{K}(V)$ spanned by the vertices of *primitive disks*. A compressing disk D in V is called *primitive* if there exists a compressing disk $\overline{D}$ in W such that ∂D intersects $\partial \overline{D}$ transversely in a single point. We call such a disk $\overline{D}$ a *dual disk* of D.

For the genus-2 Heegaard splitting $(V, W; \Sigma)$ of each of the 3-sphere, $S^2 \times S^1$ and lens spaces $L(p, q)$, the structure of the primitive disk complex $\mathcal{P}(V)$ is fully studied in [**1**], [**2**], [**3**], [**4**] and [**5**]. Understanding the structure of the primitive disk complexes enables us to obtain finite presentations of the mapping class groups of the splittings by investigating the simplicial action of the group on the primitive disk complex. Actually, it was shown that the primitive disk complex $\mathcal{P}(V)$ is contractible for the genus-2 Heegaard splitting of each of the 3-sphere, $S^2 \times S^1$ and some lens spaces. Furthermore, the quotient of $\mathcal{P}(V)$ by the action of the mapping class group of the splitting is a simple finite complex for each case, and the group is presented easily in terms of the isotropy subgroups of the simplices of the quotient.

The contractibility of $\mathcal{P}(V)$ in the case of the genus-2 splittings is based on the fact that $\mathcal{P}(V)$ is *closed under the disk surgery operation*. In other words, given any two primitive disks in V intersecting each other, any surgery on one disk along the other one always yields a primitive disk, whose meaning explained in detail in the next section. In particular, it was shown in [**1**] that the primitive disk complex for the genus-2 Heegaard splitting of the 3-sphere is closed under disk surgery operation, and so it has been conjectured that it is also true for the higher genus splittings of the 3-sphere. The main result of this work is to show that it is not true. In fact, we show further that, in the case of genus $g \geq 3$, there exist two primitive disks such that *no* surgery on one along the other one yields a primitive disk.

THEOREM 1.1. *Let $(V, W; \Sigma)$ be a genus-g Heegaard splitting of the 3-sphere with $g \geq 3$. Then the primitive disk complex $\mathcal{P}(V)$ is not closed under the disk surgery operation. In fact, $\mathcal{P}(V)$ is not even weakly closed under the disk surgery operation.*

Moreover, we give an interesting example of primitive disks with distinct intersection patterns in Section 4. Throughout the paper, any disks (except subdisks of a disk) in an irreducible 3-manifold are always assumed to be properly embedded, and their intersection is transverse and minimal up to isotopy. In particular, if a disk D intersects a disk E, then $D \cap E$ is a collection of pairwise disjoint arcs that are properly embedded in both D and E. For convenience, we will not distinguish disks from their isotopy classes in their notation.

2. Disk surgery operation

Let M be a compact, orientable, irreducible 3-manifold with compressible boundary. The *disk complex* $\mathcal{K}(M)$ for M is a simplicial complex defined as follows. The vertices are the isotopy classes of compressing disks in M, and a collection of distinct $k+1$ vertices spans a k-simplex if and only if the vertices are represented by pairwise disjoint disks.

Let D and E be compressing disks in M with $D \cap E \neq \varnothing$. We warn the reader that the intersection pattern of D and E may not be unique, by isotopy of D and E. See [**8**, Example 2.4] for an example. Throughout the discussions on disk surgery that follow, we assume that the intersection pattern $D \cap E$ is predetermined. Let Δ be a disk cut off from E by an outermost arc δ of $D \cap E$ in E such that $\Delta \cap D = \delta$. We call such a subdisk Δ an *outermost subdisk* of E cut off by $D \cap E$. The arc δ cuts D into two subdisks, say C_1 and C_2. Let $D_1 = C_1 \cup \Delta$ and $D_2 = C_2 \cup \Delta$. By a slight isotopy, the two disks D_1 and D_2 can be moved to be disjoint from D. We say that D_1 and D_2 are the disks obtained by *surgery* on D along E (with the outermost subdisk Δ). Of course there are many choices of the outermost subdisk of E cut off by $D \cap E$, and the resulting two disks from surgery depend on the choice of the outermost subdisks. We note that each of D_1 and D_2 has fewer arcs of intersection with E than D had since at least the arc δ no longer counts. Further, if D is non-separating, at least one of D_1 and D_2 is non-separating.

DEFINITION 2.1. Let $\mathcal{X}$ be a full subcomplex of $\mathcal{K}(M)$.

(1) We say that $\mathcal{X}$ is *closed under disk surgery operation* if for any disks D and E with $D \cap E \neq \varnothing$ representing vertices of $\mathcal{X}$, there exists an intersection pattern $D \cap E$ such that every surgery on D along E always yields a disk representing a vertex of $\mathcal{X}$.
(2) We say that $\mathcal{X}$ is *weakly closed under disk surgery operation* if for any disks D and E with $D \cap E \neq \varnothing$ representing vertices of $\mathcal{X}$, there exists an intersection pattern $D \cap E$ with a surgery on D along E yielding a disk representing a vertex of $\mathcal{X}$.

It is clear that the "closedness" implies the "weak closedness". For the weak closedness, it is enough to find only an outermost subdisk Δ of E such that at least one of the two disks obtained from surgery on D along E with Δ yields a disk representing a vertex of $\mathcal{X}$, while for

the closedness, we need to show that the surgery with "any" outermost subdisk always yields a disk representing a vertex of $\mathcal{X}$.

It is easy to see that the disk complex $\mathcal{K}(M)$ itself is closed under disk surgery operation, and so is the *non-separating disk complex*, denoted by $\mathcal{D}(M)$, the full subcomplex of $\mathcal{K}(M)$ spanned by all vertices of non-separating disks. The weak closedness with the closedness have served as a useful tool to understand the structure of various subcomplexes of the disk complex, for example we have the following.

THEOREM 2.2. *Let $\mathcal{X}$ be a full subcomplex of $\mathcal{K}(M)$.*

(1) *If $\mathcal{X}$ is weakly closed under disk surgery operation, then $\mathcal{X}$ is connected.*
(2) *If $\mathcal{X}$ is closed under disk surgery operation, then $\mathcal{X}$ is contractible.*

The first statement of the theorem is easy to verify. Whenever we have two vertices D and E of $\mathcal{X}$ far from each other, that is, $D \cap E \neq \varnothing$, then we have an outermost subdisk Δ of E cut off by $D \cap E$ such that the surgery on D along E with Δ yields a disk, say D_1, representing a vertex of $\mathcal{X}$. The vertex of D_1 is joined by an edge to D. If $D_1 \cap E \neq \varnothing$, we do surgery on D_1 along E to have a vertex of $\mathcal{X}$ and so on. Then eventually we have a path in $\mathcal{X}$ from D to E. The second statement was essentially proved in [**9**] and updated in [**1**]. In [**1**], the contractibility is proved in the case where M is a handlebody, but the proof is still valid for an arbitrary irreducible manifold with compressible boundary.

From Theorem 2.2, we see that the disk complex $\mathcal{K}(M)$ and the non-separating disk complex $\mathcal{D}(M)$ are all contractible. Recall that when a handlebody V is one of the handlebodies of the genus-g Heegaard splitting $(V, W; \Sigma)$, with $g \geq 2$, of the 3-sphere, $S^2 \times S^1$ or a lens space $L(p, q)$, the primitive disk complex $\mathcal{P}(V)$ is the full subcomplex of $\mathcal{K}(V)$ spanned by the vertices of primitive disks in V. The following are known results on the primitive disk complexes $\mathcal{P}(V)$ for the genus-2 splittings (see [**1, 2, 3, 4**]).

(1) For the genus-2 splittings of 3-sphere and $S^2 \times S^1$, the complex $\mathcal{P}(V)$ is closed under disk surgery operation, and hence they are all contractible.
(2) For the genus-2 splittings of lens spaces $L(p, q)$ with $1 \leq q \leq p/2$, if $p \equiv \pm 1 \pmod{q}$, then $\mathcal{P}(V)$ is closed under disk surgery operation and hence it is contractible. If $p \not\equiv \pm 1 \pmod{q}$, then $\mathcal{P}(V)$ is not weakly closed under disk surgery operation, and in fact, it is not connected.

We remark that the weak closedness and closedness under disk surgery operation are just sufficient conditions for connectivity and contractibility respectively. It is still an open question whether the primitive disk complex $\mathcal{P}(V)$ in the case of $g > 3$ for the 3-sphere is connected, contractible or not, and whether $\mathcal{P}(V)$ in the case of $g = 3$ is contractible or not. Concerning the connectivity in the case of $g = 3$, recently Freedman and Scharlemann [**6**] showed that the genus-3 Goeritz group for the 3-sphere is finitely generated (the Powell conjecture for $g = 3$) and Zupan [**12**] showed the equivalence of the Powell conjecture and the connectivity of the reducing sphere complex. From the fact that the reducing sphere complex for $g = 3$ is connected, it can be shown that $\mathcal{P}(V)$ is connected in the case of $g = 3$.

3. Primitive curves on the boundary of a handlebody

In this section, we fix a handlebody W of genus $g \geq 2$, and a *complete meridian system* $\{\overline{D}_1, \overline{D}_2, \ldots, \overline{D}_g\}$ for W. That is $\overline{D}_1, \overline{D}_2, \ldots, \overline{D}_g$ are mutually disjoint essential disks in W whose union cuts W into a 3-ball. A simple closed curve l on ∂W is said to be *primitive* if there exists a disk $\overline{D}$ properly embedded in W such that the two simple closed curves l and $\partial\overline{D}$ intersect transversely in a single point. We call such a disk $\overline{D}$ a *dual disk* of l.

Suppose that the curve l on ∂W meets the union of $\partial\overline{D}_1 \cup \partial\overline{D}_2 \cup \cdots \cup \partial\overline{D}_g$ of the oriented circles transversely and minimally. Fixing an orientation of l, and assigning the symbol x_i to

$\partial\overline{D}_i$ for each $i \in \{1, 2, \ldots, g\}$, the curve l represents the conjugacy class $c(l)$ of an element of the free group $\pi_1(W)$ of rank g. That is, l determines a word w in $\{x_1^{\pm 1}, x_2^{\pm 1}, \ldots, x_g^{\pm 1}\}$ (up to cyclic permutation) that can be read off from the intersections of l with each of $\partial\overline{D}_i$'s. Hence l represents an element $[w]$ of the free group $\pi_1(W) = \langle x_1, x_2, \ldots, x_g\rangle$ (up to conjugation). Recall that an element of a free group is said to be *primitive* if it is a member of some of its free basis. If an element of a free group is primitive, then any element of its conjugacy class is also primitive. Thus we simply say that a simple closed curve l represents a primitive element of $\pi_1(W)$ if a member (thus every member) of $c(l)$ is primitive. The following lemma provides a geometric interpretation of the primitive elements.

LEMMA 3.1 (Gordon [**7**]). *An oriented simple closed curve l on ∂W is primitive if and only if l represents a primitive element of $\pi_1(W)$.*

Consider the free group $F_g = \langle x_1, x_2, \ldots, x_g\rangle$ of rank g. Given $1 \leq g' < g$, let w be a word in $\{x_1^{\pm 1}, x_2^{\pm 1}, \ldots, x_{g'}^{\pm 1}\}$. It is clear that if the element represented by w is primitive in the free group $F_{g'} = \langle x_1, x_2, \ldots, x_{g'}\rangle$, then so it is in $F_g = \langle x_1, x_2, \ldots, x_g\rangle$.

LEMMA 3.2. *Suppose that a word w in $\{x_1^{\pm 1}, x_2^{\pm 1}, \ldots, x_{g'}^{\pm 1}\}$, where $1 \leq g' < g$, represents a primitive element of F_g. If there exists an oriented simple closed curve l on ∂W such that $[w] \in c(l)$ and $l \cap \overline{D}_i = \varnothing$ for each $i \in \{g'+1, \ldots, g\}$, then w also represents a primitive element of $F_{g'}$.*

PROOF. Suppose that l represents a primitive element of F_g. By Lemma 3.1, there exists a dual disk $\overline{D}$ of l in W. Let W' be the genus-g' handlebody obtained by cutting W along $\overline{D}_{g'+1} \cup \cdots \cup \overline{D}_g$. If the disk $\overline{D}$ is disjoint from $\overline{D}_j$ for each $j \in \{g'+1, \ldots, g\}$, then $\overline{D}$ is again a dual disk of l in W'. Thus l is a primitive curve on $\partial W'$, and so by Lemma 3.1 again, w represents a primitive element of $\pi_1(W') = \langle x_1, x_2, \ldots, x_{g'}\rangle$.

If $\overline{D}$ intersects $\overline{D}_j$ for some $j \in \{g'+1, \ldots, g\}$, then we choose an outermost subdisk of $\overline{D}_j$ cut off by $\overline{D} \cap \overline{D}_j$. Then exactly one of the two disks, say $\overline{D}'$, obtained by surgery on $\overline{D}$ along $\overline{D}_j$ with this outermost subdisk is again a dual disk of l in W. Note that $\overline{D}'$ has fewer arcs of intersection with $\overline{D}_j$ than $\overline{D}$ had. If $\overline{D}'$ still intersects $\overline{D}_{g'+1} \cup \cdots \cup \overline{D}_g$, we repeat this process finitely many times to obtain a dual disk $\overline{D}''$ of l disjoint from $\overline{D}_j$ for each $j \in \{g'+1, \ldots, g\}$. □

4. Proof of Theorem 1.1 and intersection pattern example

We first consider the genus-3 Heegaard splitting $(V, W; \Sigma)$ of the 3-sphere. Fix a complete meridian system $\{\overline{D}_1, \overline{D}_2, \overline{D}_3\}$ for W, and assign the symbol x_i to the oriented circle $\partial\overline{D}_i$ for each $i \in \{1, 2, 3\}$. Then any oriented simple closed curve l on ∂W determines a word w of the free group $\pi_1(W) = \langle x_1, x_2, x_3\rangle$ up to cyclic permutation.

Figure 7 depicts two disks D and E in V. The disk E is the band sum of two parallel copies of the disk in Figure 15(a) with the "half-twisted" band wrapping around $\partial\overline{D}_3$ as described. It is obvious that D is a primitive disk with the dual disk $\overline{D}_2$. The disk E is also primitive by Lemma 3.1 since we read off a word determined by ∂E from Figure 7 (with a suitable choice of orientations) as

$$(x_1x_2^{-1}x_1x_2^{-1}x_1x_2x_1^{-1}x_2x_2x_1^{-1})(x_1x_2^{-1}x_2^{-1}x_1x_2^{-1}x_1^{-1}x_2x_1^{-1}x_2x_1^{-1})x_2,$$

and this word is reduced to x_2, representing a primitive element.

It is easy to see that the intersection pattern $D \cap E$ is unique as well as it consists of two arcs. For each of D and E, there are two outermost disks. Any disk obtained by any surgery on D along E (and on E along D) is one of the two disks in Figure 15. The disk in Figure 15(a) determines a word w_1 of the form $x_1x_2^{-1}x_1x_2x_1^{-1}x_2$, while the disk in Figure 15(b) determines a word w_2 of the form $x_1x_2^{-1}x_1x_2^{-1}x_1x_2x_1^{-1}x_2x_2x_1^{-1}x_2$. Both disks are disjoint from $\partial\overline{D}_3$ and hence

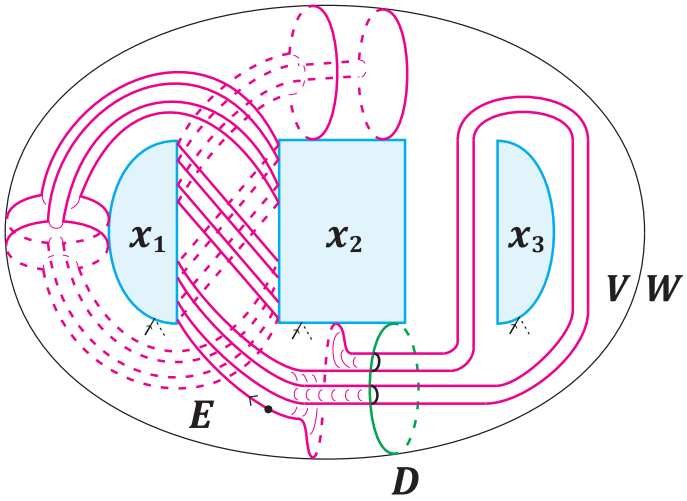


FIGURE 7. Primitive disks D and E in V.

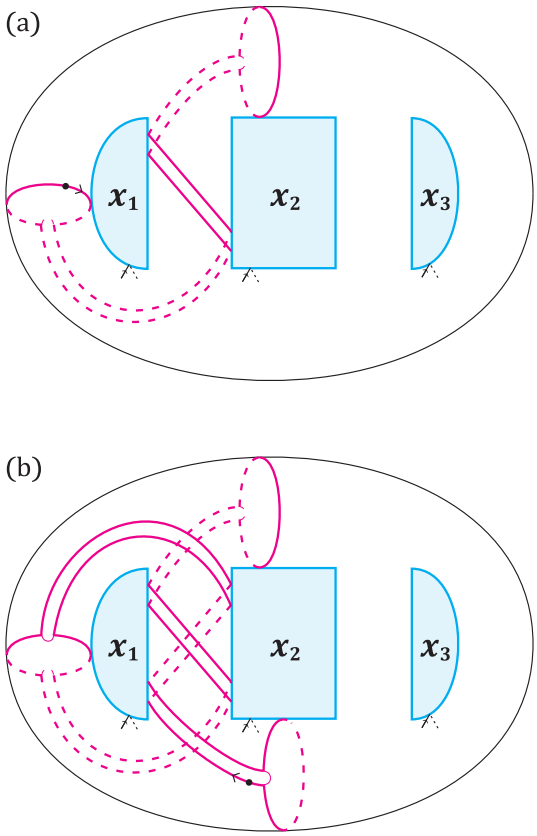


FIGURE 8. The disks obtained by surgery.

the generator x_3 does not appear in both w_1 and w_2. So w_1 and w_2 represent elements of the free group $\langle x_1, x_2 \rangle$. We observe that each of w_1 and w_2 is cyclically reduced and contains x_1 and x_1^{-1} simultaneously (also x_2 and x_2^{-1} simultaneously). Thus, by Osborne-Zieschang [**10**], the elements represented by w_1 and w_2 are not primitive in the free group $\langle x_1, x_2 \rangle$, and hence are not primitive in the free group $\langle x_1, x_2, x_3 \rangle$ by Lemma 3.2. Thus the two disks in Figure 15 are not primitive in V by Lemma 3.1.

So far we gave an example for the genus-3 Heegaard splitting of the 3-sphere, but the same argument applies for any genus g with $g \geq 3$. See Figure 16. We remark that even though the

pair (D, E) demonstrates that $\mathcal{P}(V)$ is not weakly closed under disk surgery operation, they are still connected by a path of length two in $\mathcal{P}(V)$.

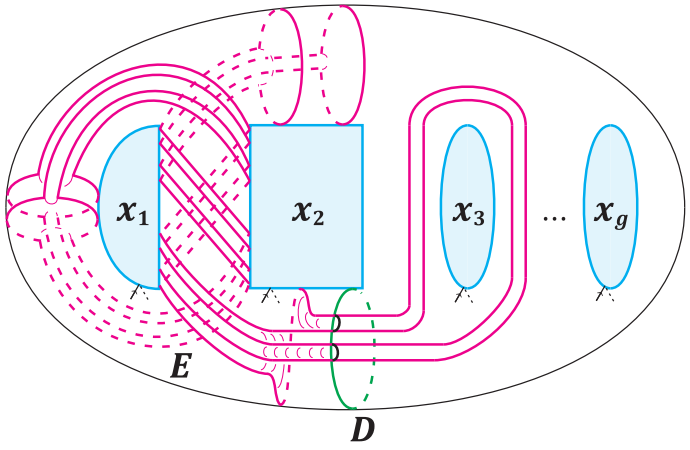


FIGURE 9. Primitive disks D and E for the case of genus $g \geq 3$.

Figure 17 depicts primitive disks D, E_1, E_2 for a genus-4 Heegaard splitting of S^3 satisfying the following conditioins:

- E_1 and E_2 are isotopic.
- Every surgery on E_1 along D yields primitive disks.
- Every surgery on E_2 along D yields non-primitive disks.

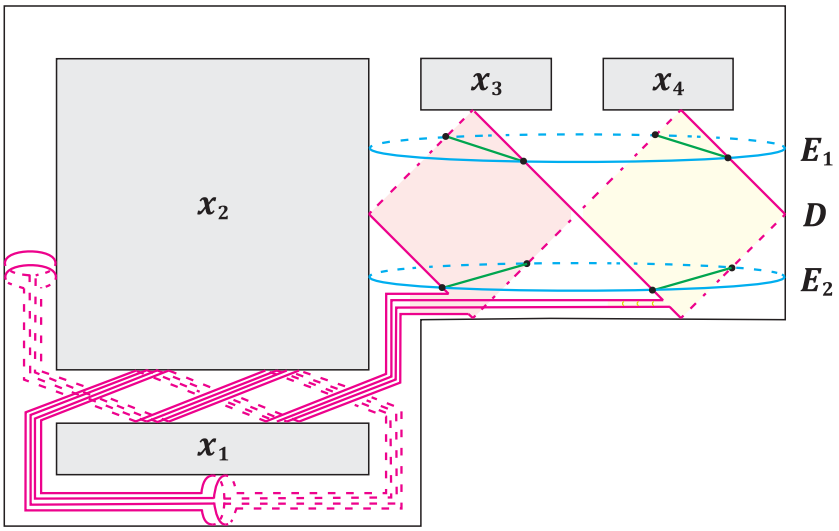


FIGURE 10. Primitive disks with distinct intersection patterns.

Bibliography

[1] **S. Cho**, Homeomorphisms of the 3-sphere that preserve a Heegaard splitting of genus two, Proc. Amer. Math. Soc. **136** (2008), 1113–1123.

[2] **S. Cho**, Genus-two Goeritz groups of lens spaces, Pacific J. Math. **265** (2013), no. 1, 1–16.

[3] **S. Cho, Y. Koda**, The genus two Goeritz group of $S^2 \times S^1$, Math. Res. Lett. **21** (2014), no. 3, 449–460.

[4] **S. Cho, Y. Koda**, Connected primitive disk complexes and genus two Goeritz groups of lens spaces, Int. Math. Res. Not. **IMRN 2016**, no. 23, 7302–7340.

[5] **S. Cho, Y. Koda**, The mapping class groups of reducible Heegaard splittings of genus two, Trans. Amer. Math. Soc. **371**, no. 4, 2473–2502.

[6] **M. Freedman and M. Scharlemann**, Powell moves and the Goeritz group, arXiv:1804.05909.

[7] **C. McA. Gordon**, On primitive sets of loops in the boundary of a handlebody, Topology Appl. **27** (3) (1987), 285–299.

[8] **S. Hensel**, A primer on handlebody groups, https://www.mathematik.uni-muenchen.de/ hensel/papers/hno4.pdf

[9] **D. McCullough**, Virtually geometrically finite mapping class groups of 3-manifolds, J. Differential Geom. **33** (1991), no. 1, 1–65.

[10] **R. P. Osborne, H. Zieschang**, Primitives in the free group on two generators, Invent. Math. **63** (1981), no. 1, 17–24.

[11] **F. Waldhausen**, Heegaard-Zerlegungen der 3-Sphäre, Topology **7** (1968), 195–203.

[12] **A. Zupan**, The Powell conjecture and reducing sphere complexes, arXiv:1906.07664.

STICK NUMBERS OF MONTESINOS KNOTS

HWA JEONG LEE, SUNGJONG NO* AND SEUNGSANG OH

Abstract. Negami found an upper bound on the stick number $s(K)$ of a nontrivial knot K in terms of the minimal crossing number $c(K)$: $s(K) \leq 2c(K)$. Huh and Oh found an improved upper bound: $s(K) \leq \frac{3}{2}(c(K)+1)$. Huh, No and Oh proved that $s(K) \leq c(K)+2$ for a 2-bridge knot or link K with at least six crossings. As a sequel to this study, we present an upper bound on the stick number of Montesinos knots and links. Let K be a knot or link which admits a reduced Montesinos diagram with $c(K)$ crossings. If each rational tangle in the diagram has five or more index of the related Conway notation, then $s(K) \leq c(K) + 3$. Furthermore, if K is alternating, then we can additionally reduce the upper bound by 2.

1. Introduction

A *stick knot* is a knot which consists of finite line segments, called *sticks*. The *stick number* $s(K)$ of a knot K is the smallest number of sticks needed to construct K. The stick presentation of knot is chemically useful because it can provide a model of the molecular structure. The stick number of the model indicates how complex the molecular structure is.

In 1991, Negami [**6**] found lower and upper bounds for the stick number of any nontrivial knot or link K other than the Hopf link in terms of the minimal crossing number $c(K)$. That is given by Negami's inequality:

$$\frac{5+\sqrt{8c(K)+9}}{2} \leq s(K) \leq 2c(K).$$

Calvo [**2**] improved the lower bound to $\frac{7+\sqrt{8c(K)+1}}{2}$. Huh and Oh [**4**] utilized the arc index $a(K)$ to determine a more precise upper bound, showing that $s(K) \leq \frac{3}{2}(c(K)+1)$ for any nontrivial knot K. They mainly used the fact that $a(K) \leq c(K)+2$ for any nontrivial knot K in [**1**] and converted any minimal arc presentation of K into a stick knot by using $\frac{3}{2}(a(K)-1)$ sticks.

There are several results about upper bounds on the stick number for 2-bridge knots. McCabe [**5**] proved that $s(K) \leq c(K)+3$ for any 2-bridge knot K other than the unlink and the Hopf link. Huh, No and Oh [**3**] reduced this upper bound by 1 for 2-bridge knots with at least six crossings. They described the standard projection of a 2-bridge knot in terms of rational tangles using the Conway notation and then constructed each integer $\pm n$-tangle by using $n+1$ sticks.

In this paper we apply this construction to find an upper bound on the stick number of Montesinos knots. A Montesinos knot is defined as a knot admitting a diagram obtained by putting rational tangles together in a circle.

Theorem 1.1. *Let K be a Montesinos knot or link which admits a reduced Montesinos diagram with $c(K)$ crossings. If each rational tangle in the diagram has five or more index of the related Conway notation, then*

$$s(K) \leq \begin{cases} c(K)+1 & \text{if } K \text{ is alternating,} \\ c(K)+3 & \text{if } K \text{ is non-alternating.} \end{cases}$$

2. Proof of Theorem 3.2

2.1. Stick rational tangle.

We first construct stick representations of rational tangles, which are basic building blocks of a Montesinos knot.

We construct a rational tangle of Conway notation $[t_1, t_2, \ldots, t_m]$ for all positive integers t_i and odd m by using $t_1 + t_2 + \cdots + t_m + 1$ sticks. See Figure 11. When all t_i's are greater than 1, Figure 11(a) describes how to connect integer tangles together to build a rational tangle with $t_1 + t_2 + \cdots + t_m + 1$ sticks. When some t_i's are 1, Figure 11(b) and Figure 11(c) show the number of sticks to make the rational tangle does not exceed this number.

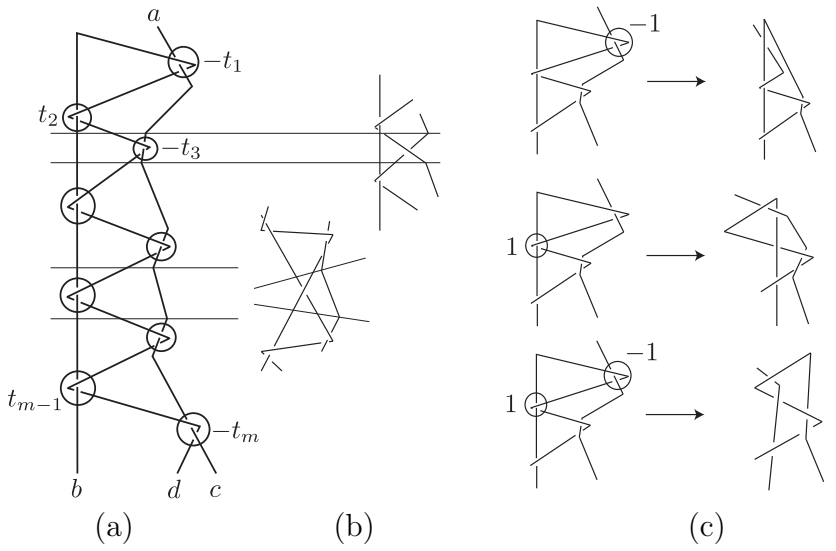


FIGURE 11. How to construct a stick rational tangle

To compose rational tangles, we denote the four end points of stick rational tangle R by a, b, c, and d and the related end sticks by l_a, l_b, l_c and l_d, respectively as illustrated in Figure 11(a).

From now on, we consider a rational tangle as a stick representation of the rational tangle together with the virtual box.

2.2. Stick Montesinos knot.

By Figure 12 and Figure 13, we can construct the stick presentation of alternating knot and non-alternating knot respectively. Let K be an alternating Montesinos knot.

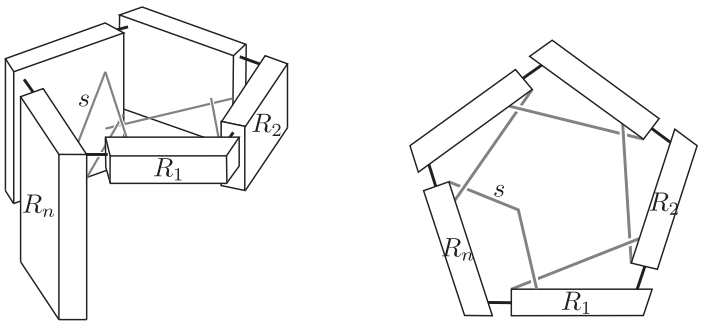


FIGURE 12. Alternating Montesinos knot

For alternating case, the total number of the sticks used to construct K becomes $c(K)+1$. For non-alternating case, two more sticks are needed to construct K. This says that $s(K) \leq c(K)+3$ if K is non-alternating. We complete the proof.

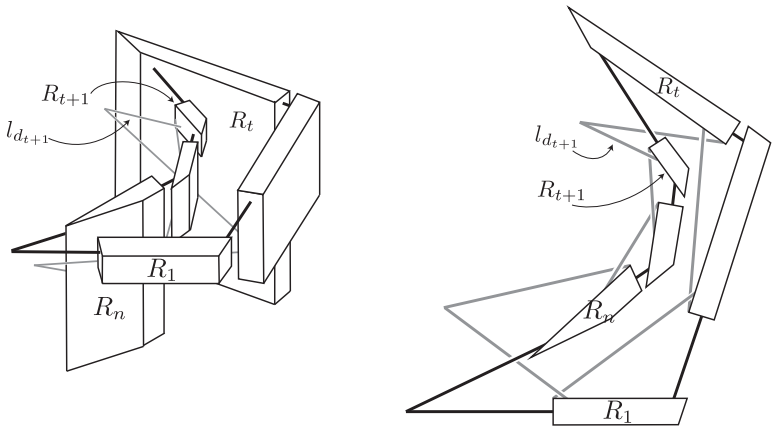


FIGURE 13. Non-alternating Montesinos knot

Bibliography

[1] Y. Bae and C. Park, *An upper bound of arc index of links*, Math. Proc. Camb. Phil. Soc. **129** (2000) 491–500.

[2] J. Calvo, *Characterizing polygons in* $\mathbb{R}^3$, in Physical knots, Contemporary Mathematics **304** (2002) 37–53.

[3] Y. Huh, S. No and S. Oh, *Stick numbers of 2-bridge knots and links*, Proc. Amer. Math. Soc. **139** (2011) 4143–4152.

[4] Y. Huh and S. Oh, *An upper bound on stick number of knots*, J. Knot Theory Ramifications **20** (2011) 741–747.

[5] C. McCabe, *An upper bound on edge numbers of 2-bridge knots and links*, J. Knot Theory Ramifications **7** (1998) 797–805.

[6] S. Negami, *Ramsey theorems for knots, links, and spatial graphs*, Trans. Amer. Math. Soc. **324** (1991) 527–541.

LOWER CENTRAL SERIES AND HOMOLOGY CYLINDERS

MINKYOUNG SONG

Abstract. All of Johnson homomorphisms of a mapping class group of a surface, Milnor invariants and Orr invariants of links are related to lower central series of a free group. Moreover, it is known that they are closely connected. In this talk, we consider extension of those invariants to homology cylinders and a filtration via their kernels. A homology cylinder is a kind of 3-manifold, which is a generalization of both a string link and a mapping class group. We determine the images of the filtration under the invariants and get relations of quotients of the filtration to automorphism groups of free nilpotent groups, and free Lie algebras. We also obtain the numbers of linearly independent invariants.

The 5th Mini Workshop on Knot theory *in Jeju*

Lower central series & Homology cylinders

Minkyoung Song
in IBS-CGP
2020.7.23.

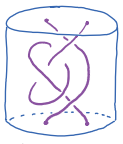
Start of (the homology cobordism group of) homology cylinders

[Goussarov, 99] [Habiro, 00]

: finite type invariants of { links ⇝ string link; 3-manifolds ⇝ homology cylinder }
(using clasper surgery)

$\amalg S^1 \hookrightarrow S^3$, HS^3

$\amalg I \hookrightarrow D^2 \times I$ $(\simeq B^3)$

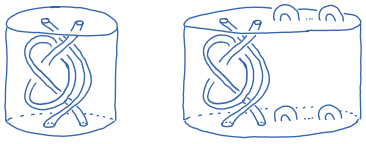


$H(D^2 \times I)$ $(\simeq HB^3)$

$H(\Sigma_{g,1} \times I)$

[Levine, 01] [Garoufalidis-Levine, 05]

: mapping class group of $\Sigma_{g,1}$



homology cobordism group of homology cylinders over $\Sigma_{g,1}$

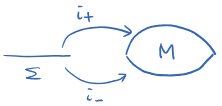
$H(\Sigma_{g,n} \times I)$

Definitions & Examples of $\mathcal{H}_{g,n}$

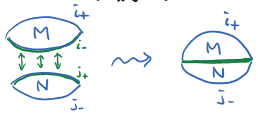
Def A homology cylinder over $\Sigma = (M^3, i_+, i_- : \Sigma \hookrightarrow M)$

s.t. (1) $i_+ \cup (-i_-) : \Sigma \underset{\partial}{\cup} (-\Sigma) \xrightarrow{\simeq} \partial M$

(2) $i_+, i_- : \Sigma \to M$ induce $\cong$ on $H_*(-)$



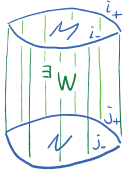
- $(M, i_+, i_-) \cdot (N, j_+, j_-) = (M \underset{i_-=j_+}{\cup} N, i_+, j_-)$



$\Rightarrow$ monoid

Def For homology cylinders $(M, i_+, i_-), (N, j_+, j_-)$ over Σ, M and N are homology cobordant

if $\exists\ W^4$ s.t. (1) $\partial W = M \underset{\substack{i_+=j_+ \\ i_-=j_-}}{\cup} (-N)$



(2) $M \hookrightarrow W \hookleftarrow N$ induce $\cong$ on $H_*(-)$.

- $\mathcal{H}_{g,n} := \{\text{homology cylinders over } \Sigma_{g,n}\} / \text{homology cobordism}$ $\Rightarrow$ group

Ex
- $\mathcal{H}_{0,0} \cong \mathcal{H}_{0,1} \cong$ homology cobordism group of HS^3
- $\mathcal{H}_{0,2} \cong$ concordance group of framed knots in HS^3
- $\mathcal{H}_{0,n} \cong$ concordance group of $(n-1)$-component framed string links in HB^3

} abelian

- mapping class group $\mathcal{M}_{g,n} \hookrightarrow \mathcal{H}_{g,n}$

Johnson homomorphism

$\eta_k : \mathcal{M}_{g,n} \to \mathrm{Aut}(F/F_k)$

$\varphi \mapsto \eta_k(\varphi)$

$$\begin{array}{ccc} \pi_1\Sigma & \xrightarrow{\varphi}_{\simeq} & \pi_1\Sigma \\ \downarrow & & \downarrow \\ F/F_k & \underset{\eta_k(\varphi)}{\overset{\simeq}{\uparrow}} & F/F_k \end{array}$$

$\mathcal{M}_{g,n}[k] := \ker \eta_k$

$\mathrm{Im}\,\eta_k$: unknown

[Morita, 93]

$\dfrac{\mathcal{M}_{g,1}[k]}{\mathcal{M}_{g,1}[k+1]} \hookrightarrow D_k(H)$

$\tilde{\eta}_k : \mathcal{H}_{g,n} \to \mathrm{Aut}(F/F_k)$

$M \mapsto \tilde{\eta}_k(M)$

$$\begin{array}{ccccc} \pi_1\Sigma & \xrightarrow{i_-} & \pi_1 M & \xleftarrow{i_+} & \pi_1\Sigma \\ \downarrow & & \downarrow & & \downarrow \\ F/F_k & \twoheadrightarrow & \pi_1 M/(\pi_1 M)_k & \xleftarrow{\simeq} & F/F_k \end{array}$$

$\tilde{\eta}_k(M)$

$\mathcal{H}_{g,n}[k] := \ker \tilde{\eta}_k$

[Garoufalidis - Levine, 05] $\tilde{\eta}_k(\mathcal{H}_{g,1}) = \{\phi \mid \phi(\partial) = \partial\}$

$\dfrac{\mathcal{H}_{g,1}[k]}{\mathcal{H}_{g,1}[k+1]} \cong D_k(H)$

[S.] $\tilde{\eta}_k(\mathcal{H}_{g,n}) = \{\phi \mid \phi(x_i) = \alpha_i^{-1} x_i \alpha_i,\ i \le n-1,\ \phi(\partial_n) = \partial_n\}$

$\dfrac{\mathcal{H}_{g,n}[k]}{\mathcal{H}_{g,n}[k+1]} \cong \ker\{\mathrm{Aut}_2(F/F_{k+1}) \to \mathrm{Aut}_2(F/F_k)\}$

Stallings' Thm ('65)

$f : G \to G'$ homom.

$H_1(f) : \cong$, $H_2(f) :$ surj.

$\Rightarrow f_* : G/G_k \simeq G'/G'_k\ \ \forall k$

Milnor invariant

$\bar{\mu}_k : \left\{ \text{based links with } \bar{\mu}_{\le k-1} = 0 \right\} \to (F/F_k)^m$

$\cup$

$(L,\tau) \longmapsto (\bar{\mu}_k(L)_i)_{i\le m}$

$\tau : VS^1 \to E_L$

$F \xrightarrow{\tau} \pi_1 E_L \quad \ni i\text{th longitude}$

$\downarrow \qquad \downarrow$

$F/F_k \xrightarrow{\simeq} \pi_1 E_L / (\pi_1 E_L)_k$

$\cup$

$\bar{\mu}_k(L)_i$

$\bar{\mu}_k : SL_m \to (F/F_k)^m$

$\cup$

$\sigma \longmapsto (\bar{\mu}_k(\sigma)_i)_{i\le m}$

$F \to \pi_1 E_\sigma$

$\downarrow \qquad \downarrow$

$F/F_k \xrightarrow{\simeq} \pi_1 E_\sigma / (\pi_1 E_\sigma)_k$

$SL_m(k) := \ker \bar{\mu}_k$

$\tilde{\mu}_k : \mathcal{H}_{g,n} \to (F/F_k)^{2g+n-1}$

$\cup$

M

$F \xrightarrow{i_+} \pi_1 M$

$\downarrow \qquad \downarrow$

$F/F_k \xrightarrow{\simeq} \pi_1 M / (\pi_1 M)_k$

$\mathcal{H}_{g,n}(k) := \ker \tilde{\mu}_k$

[Orr, 89]

$\exists\, r_k$ linearly indep. $\bar{\mu}_{k+1}$ distinguishing links with trivial $\bar{\mu}_{\le k}$.

$(r_k := \operatorname{rank} D_k(H))$

$\dfrac{SL_m(k)}{SL_m(k+1)} \cong D_k(H)$

[S.]

$\dfrac{\mathcal{H}_{g,n}(k)}{\mathcal{H}_{g,n}(k+1)} \cong D_k(H)$

Relation between Milnor inv. & Johnson homom.

Recall

$$\frac{SL_m^*(k)}{SL_m^*(k+1)} \cong D_k(H(m)), \qquad \frac{\mathcal{H}_{g,1}[k]}{\mathcal{H}_{g,1}[k+1]} \cong D_k(H(2g))$$

[Habegger, 00] "Milnor-Johnson corresp."

$\exists$ 1-1 corresp. $SL_{2g}^{HB^3}(2) \longleftrightarrow \mathcal{H}_{g,1}[2]$ (not homom.)

which induces $\dfrac{SL_{2g}^{HB^3}(k)}{SL_{2g}^{HB^3}(k+1)} \xleftarrow{\sim} \dfrac{\mathcal{H}_{g,1}[k]}{\mathcal{H}_{g,1}[k+1]}$

$\bar{\mu}_k \longleftrightarrow \tilde{\eta}_k$

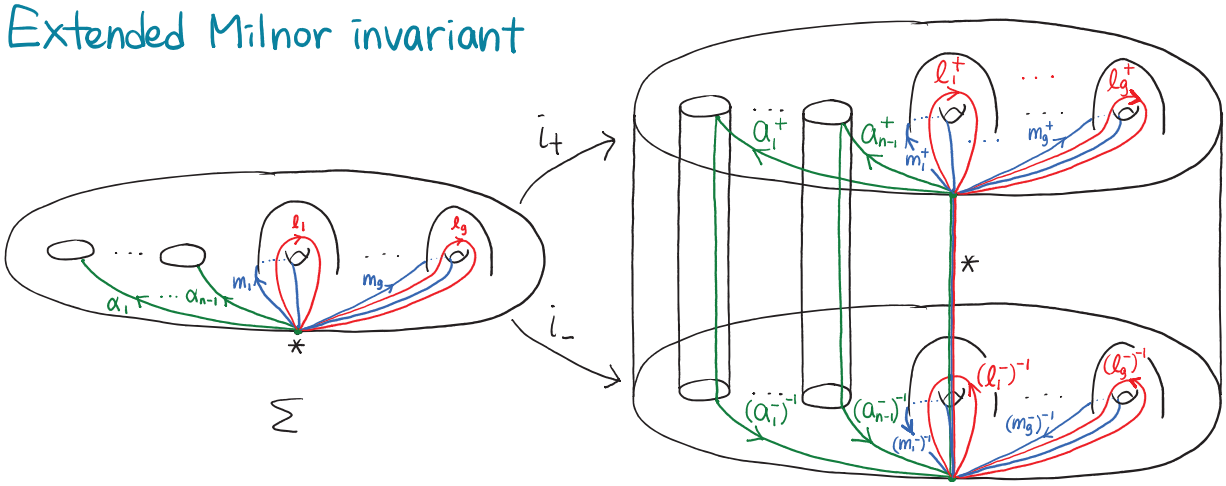
[Levine, 01]

$\Sigma_{0,g} \hookrightarrow \Sigma_{2g,1}$ induces $SL_g^{HB^3} \hookrightarrow \mathcal{H}_{g,1}$

$\dfrac{SL_g^{HB^3}(k)}{SL_g^{HB^3}(k+1)} \hookrightarrow \dfrac{\mathcal{H}_{g,1}[k]}{\mathcal{H}_{g,1}[k+1]}$

$\bar{\mu}_k \longmapsto \tilde{\eta}_k$

Extended Milnor invariant



$\alpha_i^\pm := i_\pm \circ \alpha_i$, $m_j^\pm := i_\pm \circ m_j$, $l_j^\pm := i_\pm \circ l_j$

extended Milnor invariant = Milnor invariant + Johnson homomorphism (extended)

$\widetilde{\mu}_k : H_{g,n} \to (F/F_k)^{2g+n-1}$ $\quad \overline{\mu}_k : SL^{HB^3}_{n-1} \to (F/F_k)^{n-1}$ $\quad \widetilde{\eta}_k : H_{g,1} \to \mathrm{Aut}(F/F_k)$

$H_{g,n}(k) := \ker \widetilde{\mu}_k$ $\quad SL^{HB^3}_1 = H_{0,n}$

$SL^{HB^3}_m(k) = H_{0,m+1}(k)$ $\quad H_{g,1}[k] = H_{g,1}(k)$

Milnor inv. + Johnson homom. $\rightsquigarrow$ Extended Milnor invariant

Recall $\dfrac{SL^*_m(k)}{SL^*_m(k+1)} \cong \dfrac{H_{0,m+1}(k)}{H_{0,m+1}(k+1)} \cong D_k(H(m))$, $\dfrac{H_{g,1}[k]}{H_{g,1}[k+1]} \cong \dfrac{H_{g,1}(k)}{H_{g,1}(k+1)} \cong D_k(H(2g))$

Thm[S.] $\dfrac{H_{g,n}(k)}{H_{g,n}(k+1)} = D_k(H(2g+n-1))$

cf. $\dfrac{H_{g,n}[k]}{H_{g,n}[k+1]} \cong \ker\{\mathrm{Aut}_2(F/F_{k+1}) \to \mathrm{Aut}_2(F/F_k)\}$

[Habegger, 00] "Milnor-Johnson corresp."

$\exists$ 1-1 corresp. $SL^{HB^3}_{2g}(2) \longleftrightarrow H_{g,1}[2]$ (not homom.)

which induces $\dfrac{SL^{HB^3}_{2g}(k)}{SL^{HB^3}_{2g}(k+1)} \xleftrightarrow{\sim} \dfrac{H_{g,1}[k]}{H_{g,1}[k+1]}$

$\overline{\mu}_k \longleftrightarrow \widetilde{\eta}_k$

$SL^{HB^3}_m \cong H_{0,m+1}$
$SL^{HB^3}_m(k) \cong H_{0,m+1}(k)$
$H_{g,1}[k] = H_{g,1}(k)$

[Levine, 01]

$\Sigma_{0,g} \hookrightarrow \Sigma_{2g,1}$ induces $SL^{HB^3}_g \hookrightarrow H_{g,1}$

$\dfrac{SL^{HB^3}_g(k)}{SL^{HB^3}_g(k+1)} \hookrightarrow \dfrac{H_{g,1}[k]}{H_{g,1}[k+1]}$

$\overline{\mu}_k \longmapsto \widetilde{\eta}_k$

[S., 16] $\Sigma_{g,n} \hookrightarrow \Sigma_{g',n'}$ induces $H_{g,n} \hookrightarrow H_{g',n'}$ if $g \le g'$, $n \le n'$

(Igusa-)Orr invariant

$\overline{\theta}_k : \left\{ \begin{array}{l} \text{based links} \\ \text{with } \overline{\mu}_{\le k}(L) = 0 \end{array} \right\} \to H_3(F/F_k)$

$(L, \tau) \longmapsto f_*([M_L])$

$f : M_L \to K(\pi_1 M_L, 1) \to K(F/F_k, 1)$

along $\pi_1 M_L \twoheadrightarrow \pi_1 M_L / (\pi_1 M_L)_k \simeq F/F_k$

[Igusa-Orr, 01]

L : k-slice $\Leftrightarrow \overline{\mu}_{\le 2k}(L) = 0$

$\overline{\theta}_k(L) = 0 \Leftrightarrow \overline{\mu}_{\le 2k-1}(L) = 0$

$\widetilde{\theta}_k : \mathcal{H}_{g,n}(k) \to H_3(F/F_k)$

$M \longmapsto f_*([\widehat{M}])$

where $\widehat{M}$: closure of M

$f : \widehat{M} \to K(\pi_1 \widehat{M}, 1) \to K(F/F_k, 1)$

along $\pi_1 \widehat{M} \twoheadrightarrow \pi_1 \widehat{M} / (\pi_1 \widehat{M})_k \xrightarrow{\simeq} F/F_k$

[S.] $\widetilde{\theta}_k$: surjective $(\mathrm{Ker} = \mathcal{H}(2k-1))$

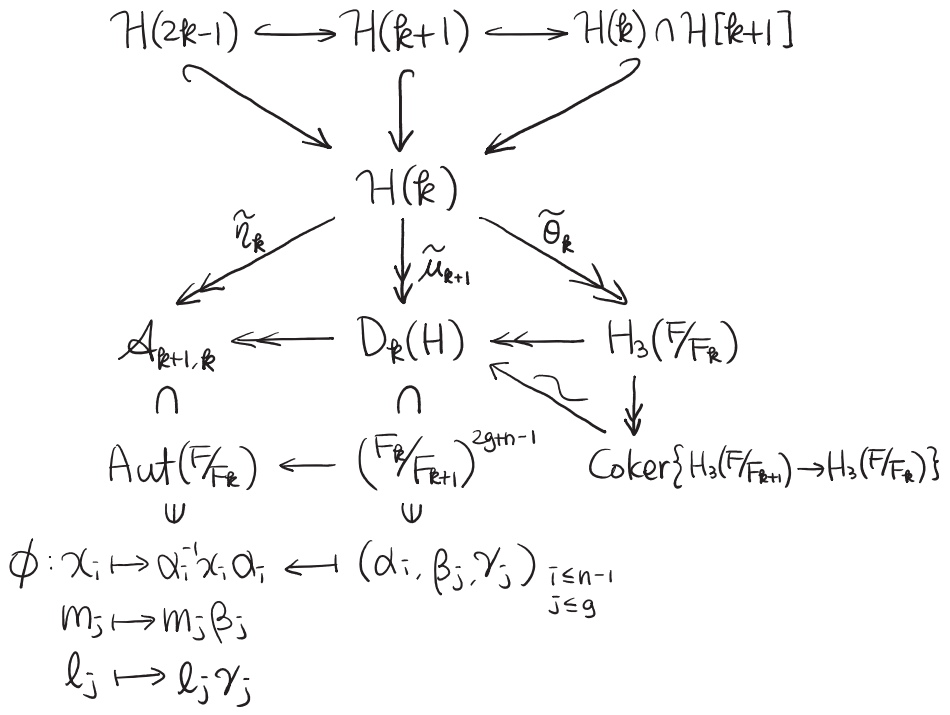
$$\frac{\mathcal{H}(k)}{\mathcal{H}(2k-1)} \cong H_3(F/F_k)$$

$$\frac{\mathcal{H}(k)}{\mathcal{H}(k+1)} \cong \mathrm{Coker}\{H_3(F/F_{k+1}) \to H_3(F/F_k)\}$$

SI known

$D_k(H)$

Relations among the three invariants



MINIMALLY KNOTTED SPATIAL CUBIC GRAPHS WITH TWO VERTICES

HYUNGKEE YOO

Abstract. A spatial graph is called minimally knotted if it is nontrivial, but every proper subgraph is trivial. Clearly, the minimum degree of any minimally knotted spatial graph is at least two. If every degree of vertex is two, then it becomes a Brunnian link. Therefore, we consider the simplest case, the minimally knotted spatial cubic graph with two vertices. In this paper, we observe the properties of a minimally knotted spatial cubic graph with two vertices. Using these properties, we find exact values of lattice stick numbers for several spatial graphs.

1. Introduction

All definitions and statements throughout this paper will concern the piecewise linear category.

A *graph* Γ is a finite one-dimensional CW-complex, and a *spatial graph* G is an embedded graph in S^3. Two spatial graph are *equivalent* if there is an ambient isotopy between them. A spatial graph is called *unknotted* or *trivial* if it is equivalent to a plane graph. Otherwise, it is *knotted* or *nontrivial*.

Definition 1.1. A spatial graph is called *minimally knotted* if it is nontrivial, but every proper subgraph is trivial.

Clearly, if spatial graph has a degree 0 or 1 vertex, then it cannot be minimally knotted. In 1993, Wu showed the following theorem.

Theorem 1.2 (Wu, 1993). *If Γ is a planar graph with no degree 0 or 1 vertices, then it admits a minimally knotted embedding into S^3.*

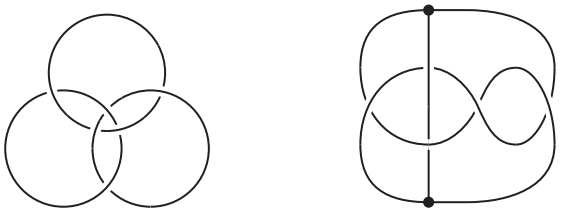


Figure 14. Borromean link and Kinoshita theta-curve

If every degree of vertices is two, then Minimally knotted graphs are Brunnian links. Thus we consider the cubic (or trivalent) graphs.

A *theta-curve* is a graph in $\mathbb{R}^3$ (or in S^3) which consists of two vertices and three edges between them. Two theta-curves are considered to be *equivalent* if there exists an ambient isotopy taking one to the other. Especially, since theta-curves are trivalent graphs (or cubic graphs), we can consider a theta-curve in the cubic lattice $\mathbb{Z}^3 = (\mathbb{R} \times \mathbb{Z} \times \mathbb{Z}) \cup (\mathbb{Z} \times \mathbb{R} \times \mathbb{Z}) \cup (\mathbb{Z} \times \mathbb{Z} \times \mathbb{R})$. That is, the vertices are located at lattice points, and the edges consist of sticks parallel to the x, y, or z-axes. This theta-curve is called a *lattice theta-curve*. The *lattice stick*

number $s_L(\Theta)$ of a theta-curve Θ is the minimal number of sticks necessary to construct lattice theta-curve which is equivalent to Θ.

A graph in $\mathbb{R}^3$ is said to be *trivial* if it is equivalent to a graph on a plane, otherwise *nontrivial*. Let e be an edge of given theta-curve Θ. The cycle consisting of two edges of Θ, except for e, is called a *constituent knot* of Θ corresponding to e. If Θ is nontrivial and every constituent knot of Θ is trivial, then this theta-curve is called a *Brunnian theta-curve*.

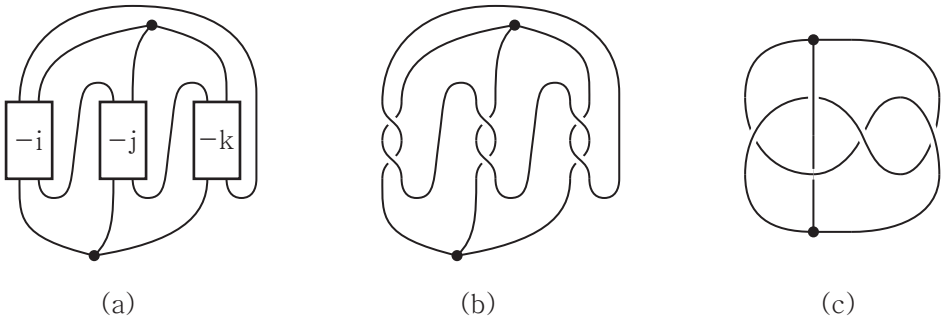


FIGURE 15. Examples of Brunnian theta-curves

The most famous example of a Brunnian theta-curve is the *Kinoshita theta-curve* [**8**]. In [**15**], Wolcott generalizes the Kinoshita theta-curve to the theta-curve Figure 15 (a) where the integers i, j and k mean that the number of full twists in each box. This theta-curve is called *Kinoshita-Wolcott theta-curve*. If $i = j = k = 1$, then the Kinoshita-Wolcott theta-curve becomes the Kinoshita theta-curve as in Figure 15 (b). In addition, the Kinoshita theta-curve is 5_1 theta-curve in moriuchi's table [**11**]. as in Figure 15 (c). In Example 3.3.12 of [**14**], Thurston proved that the Kinoshita theta-curve is hyperbolic. Jang et al. [**7**] introduce more Brunnian theta-curves. They suggested the question that their examples are hyperbolic.

A theta-curve Θ is *rational* if it is nontrivial and there is a 2-sphere which bounds two 3-balls B_1 and B_2 in S^3 as shown in Figure 16.

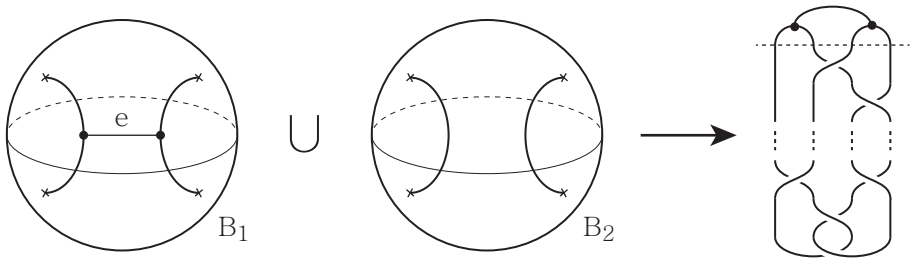


FIGURE 16. rational theta-curve

In [**2**], Harikae shows that above Θ is trivial if and only if the constituent knot corresponding to edge e in B_1. That is, every Brunnian theta-curve is not rational.

2. Order-3 vertex connected sum and tight disk

Like a connected sum of two knots, there is an operation of two theta-curves which constructs new theta-curve. Suppose that Θ_1 and Θ_2 are theta-curves in S^3. Take vertices v_1 of Θ_1 and v_2 of Θ_2. We can construct a new theta-curve by removing regular open neighborhoods of v_1 and v_2 and gluing the resulting 3-balls together along their boundaries so that a point from Θ_1 is matching to a point from Θ_2 as in Figure 17. Then we call this operation the *order-3 vertex connected sum* and denote the result theta-curve as $\Theta_1 \#_3 \Theta_2$. Note that an order-3 vertex connected sum $\Theta_1 \#_3 \Theta_2$ is not unique. Let Θ be a theta curve in S^3. A 2-sphere S is said to be

decomposing sphere if S meets each edge of Θ transversally at exactly one interior point of the edge.

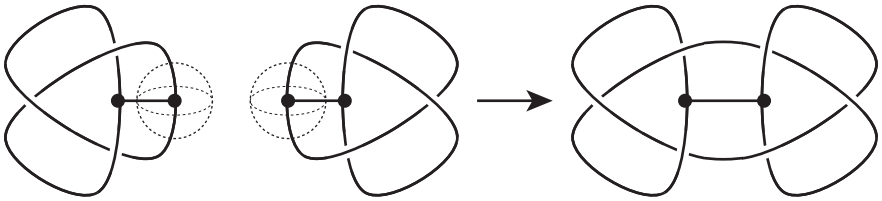


FIGURE 17. the order-3 vertex connected sum $\Theta_1 \#_3 \Theta_2$

A theta-curve Θ is said to be *prime* if it satisfies the following three conditions:

- it is nontrivial;
- it is not the connected sum of nontrivial knot and (possibly trivial) theta-curve;
- it is not the order-3 vertex connected sum of two nontrivial theta-curves.

In [**9**], Litherland announced a table of prime theta-curves with up to seven crossings. However, he did not prove that the table is complete. In [**11**], Moriuchi proved that Litherland's table is complete by using Yamada polynomial. If Θ is Brunnian, then we just consider the third condition to check that Θ is prime by definition of a Brunnian theta-curve. By the definition, a constituent knot of $\Theta_1 \#_3 \Theta_2$ is the connected sum of a constituent knot of Θ_1 and a constituent knot of Θ_2. Since the connected sum of two trivial knots is trivial, the order-3 vertex connected sum of two Brunnian theta-curves is also Brunnian [**15**].

Let Θ be a Brunnian theta-curve. Since every constituent knot K of Θ is trivial, there is an embedded disk D_K which is bounded by K. This disk D_K is called a *tight disk* for Θ if the intersection number $|\mathring{D}_K \cap \{\Theta \backslash K\}|$ is minimal among all possible cases of a constituent knot K and a bounded disk D_K. This minimum intersection number is denoted by $\tau(\Theta)$.

We recall that the order-3 vertex connected sum of two Brunnian theta-curves is also a Brunnian theta-curve.

THEOREM 2.1. *Let Θ_1 and Θ_2 be any Brunnian theta-curves. Then*

$$\tau(\Theta_1 \#_3 \Theta_2) \geq \tau(\Theta_1) + \tau(\Theta_2).$$

PROOF. Let $\Theta = \Theta_1 \#_3 \Theta_2$ be the order-3 vertex connected sum of Θ_1 and Θ_2, and let S be it's decomposing sphere. Let D_K be a tight disk of Θ with a constituent knot K and let e be the remaining edge of Θ.

We assume that D_K and S intersect transversely, and so $D_K \cap S$ consists of several loops and a simple arc α whose endpoints lie on K. By using the standard innermost disk argument we will remove these loops of the intersection. Let γ be an innermost loop of the intersection of $D_K \cap S$ in S, bounding a disk E in S and a disk F in D_K as in Figure 18. Note that $D_K \cap \mathring{E}$ is empty.

We consider the case that the remaining edge e meets S in $\mathring{E}$. If e does not pass through $\mathring{F}$, then the two vertices of Θ are located on each side of the sphere $E \cup F$. Then the two edges of Θ constructing K must pass through $\mathring{E}$, contradicting $D_K \cap \mathring{E} = \varnothing$. In this case, e must meet F.

Now a 2-surgery of D_K along the disk E converts D_K into a sphere and a disk D'. Whether e passes through $\mathring{E}$ or not, $|D' \cap e|$ is less than or equal to $|D_K \cap e|$. So D' is also a tight disk for Θ. Since $D' \cap S$ has less loops than $D_K \cap S$, by repeating this argument, we can assume the intersection $D_K \cap S$ consists of only an arc α.

Split the tight disk D_K along the arc α into two disks D_1 and D_2, which can be also considered as disks bounding some constituent knots of Brunnian theta-curves Θ_1 and Θ_2,

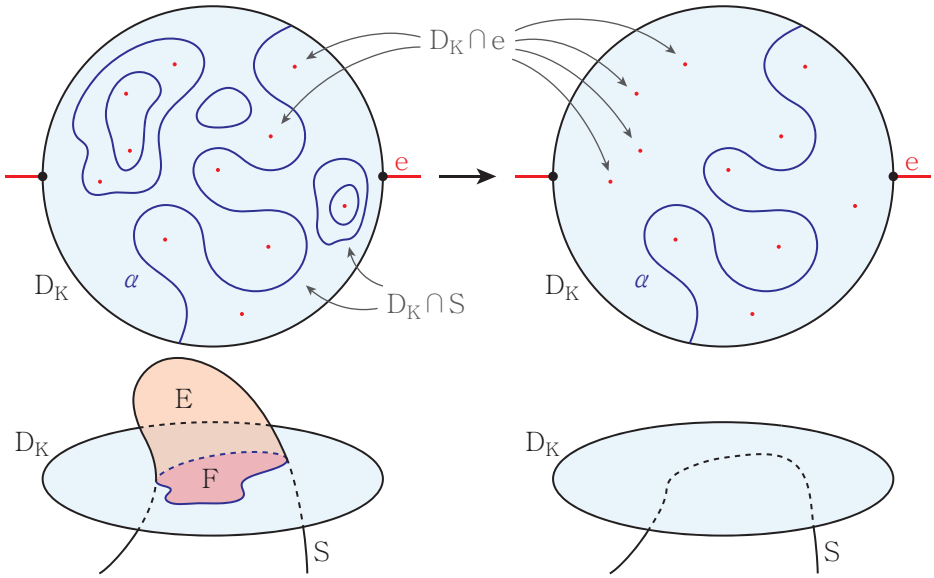


FIGURE 18. A schematic diagram of D_K

respectively. This implies that

$$\tau(\Theta) \geq \tau(\Theta_1) + \tau(\Theta_2).$$

We complete the proof of superadditivity of τ under the order-3 vertex connected sum. □

We introduce Scharlemann and Thompson's result [**13**] regarding maximal Euler characteristics of oriented links. A Seifert surface for an oriented link L is a compact oriented surface none of whose components are closed and whose boundary is the link. Define $\chi(L)$ to be the maximal Euler characteristic of all Seifert surfaces for L.

THEOREM 2.2. [**13**, Theorem 1.4] *Suppose L_+, L_- and L_0 are three links under a skein relation. Then two of $\chi(L_+)$, $\chi(L_-)$ and $\chi(L_0) - 1$ are equal and are no larger than the third.*

Let v_1 and v_2 be two vertices of given Θ, and let e be a edge of Θ. We choose an orientation of Θ so that v_2 is a terminal point of e and v_1 is a terminal point of the other edges. Notes that this orientation does not allow source and sink points. Following the definition in [**10**], we call this the *Y-orientation* corresponding to e.

THEOREM 2.3. *Let Θ be a Brunnian theta-curve. Then $\tau(\Theta) \geq 2$.*

PROOF. Suppose a Brunnian theta-curve Θ has $\tau(\Theta) \leq 1$. Let D_K be a tight disk of Θ with a constituent knot K and let e be the remaining edge of Θ.

First we assume that $\tau(\Theta) = 0$. Choose an embedded disk D' bounded by another constituent knot of Θ which contains e. By using the standard innermost disk and outermost arc arguments, we may assume that the interiors $\mathring{D}_K$ and $\mathring{D}'$ do not intersect. This implies that Θ is contained in a disk $D_K \cup D'$, and hence Θ is trivial.

Now we assume that $\tau(\Theta) = 1$. Then Θ is prime by above result and Theorem 2.1. Take the Y-orientation corresponding to e. Consider a regular projection of Θ into $\mathbb{R}^2$. Then we modify Θ by shrinking D_K so that projection image of D_K is a small disk and the edge e crosses the boundary of D_K twice as drawn in the left side of Figure 19. After that, we give the Y-orientation corresponding to e on Θ. Let e_+ denote the edge of Θ that has a positive crossing with e, and let e_- denote the edge that has a negative crossing with e. Consider the constituent knots $K_+ = e \cup e_+$ and $K_- = e \cup e_-$. Then K_+ and K_- differ only at the crossing in the projection image of disk E. Take a link K_0 so that K_+, K_- and K_0 satisfy a skein relationship.

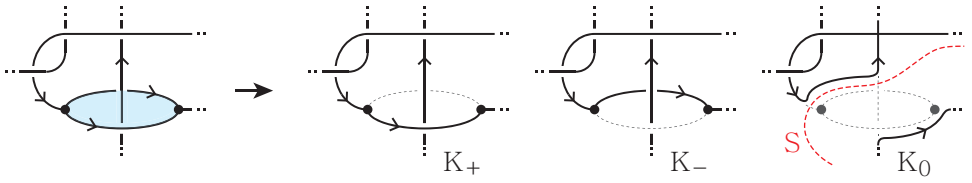


FIGURE 19. Skein triple

Since Θ is Brunnian, $\chi(K_+) = \chi(K_-) = 1$. Thus $\chi(K_0) - 1 \geq 1$ by Theorem 2.2. This implies that K_0 is the trivial link with two components, and hence it is a split link.

Let S be a splitting sphere of K_0 with the minimum number of intersections with Θ. Then S meets transversally Θ at two points inside the edge e. Press S along the part of the edge e that does not pass through the disk D_K. Then we obtain the splitting sphere S of K_0 such that S meets once with each edge of Θ. That is S is the decomposing sphere of order-3 vertex connected sum. But since Θ is prime, one part of order-3 vertex connected sum is trivial. Thus after Reidemeister moves for spatial graph, we reduce the number of intersection of the disk D_K and the edge e. This is a contradiction, and hence the result follows. □

Note that, Figure 15 (c) shows that the minimum intersection number of the Kinoshita theta-curve is at most two. Thus the lower bound in the above theorem is optimal.

3. Application

Only this section deals with not only theta-curves but whole spatial graphs. For a lattice spatial graph G, let $|G|$ denote the number of sticks of G. A stick of G which is parallel to the x-axis is called an *x-stick*. The number of x-sticks of G is denoted by $|G|_x$. In the same manner, we define y- and z-sticks. Two lattice spatial graphs are said to be equivalent if they are ambient isotopic in $\mathbb{R}^3$. A lattice spatial graph G is called *reducible* if there is another equivalent lattice spatial graph which has fewer sticks. Otherwise, it is called *irreducible*.

An xy-plane (so perpendicular to the z-axis) is called a *z-level* of G if it contains some x-sticks or y-sticks of G. For some integer i, the z-level with height i is denoted by Z_i. If G has n z-levels, then, without loss of generality, these z-levels are considered as $1, 2, \ldots, n$ like height numbers. Note that a z-stick whose endpoints lie on the z-levels Z_i and Z_j has length $|i-j|$, simply denoted by z_{ij}. Similarly, we denote i-th x- and y-level to X_i and Y_i respectively. Also x-stick between X_i and X_j is denoted by x_{ij}, y-stick between Y_i and Y_j is denoted by y_{ij}.

A lattice spatial graph G is said to be *properly leveled* with respect to the z-coordinate if each Z_i contains exactly one connected component of $G \cap Z_i$ which consists of x-sticks or y-sticks, and some singletons coming from z-sticks passing through Z_i. If G is properly leveled with respect to every coordinate, then it is simply said to be properly leveled. This definition is in the same context as that of proper levelness for knots [**4, 5**] and links [**3**].

LEMMA 3.1. *Every lattice spatial graph can be deformed to be properly leveled with the number of sticks preserved.*

PROOF. The proof follows that Lemma 2.1 of [**4**]. Suppose that some Z_i contains the portion H of G, which has more than or equal to two components consisting of x-sticks or y-sticks. Here we ignore the singletons on this level. We re-arrange z-levels so that Z_j for $j > i$ moves one step-up to Z_{j+1}. Now pick one connected component H_1 in H, move it one step-up to Z_{i+1}, and make the related z-sticks longer or shorter so that they are still adjoined to H_1. Repeat this operation for every component of H except the last one and at every z-level. Then we obtain the properly leveled lattice spatial graph with respect to the z-coordinate. Repeat the same arguments with respect to the x- and y-coordinates. One notices that this operation is an ambient isotopy and the number of x, y and z-stick have remained unchanged. □

Using properties of tight disk, we can provev the following theorem.

THEOREM 3.2. *Let Θ be a Brunnian theta-curve. Then $s_L(\Theta) \geq 17$.*

We observed the properties of Brunnian theta curves and used these properties to prove the lower bound of lattice stick number of Brunnian theta-curves. We found examples for a lattice Kinoshita theta-curve with 18 sticks. One of examples is drawn in Figure 20. Therefore, we suggest the following question.

QUESTION. Should a lattice Brunnian theta curve consists of at least 18 sticks?

If this question is true, then the lower bound in the question is optimal. Furthermore the lattice stick number of the Kinoshita theta-curve is exactly 18.

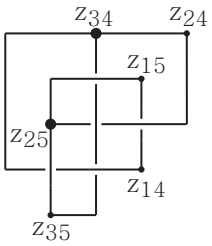


FIGURE 20. A lattice Kinoshita theta-curve with 18 sticks.

Bibliography

[1] H. Goda, *Bridge index for theta curves in the 3-sphere*, Topol. Appl. **79** (1997) 177–196.

[2] T. Harikae, *On rational and psuedo-rational theta curves in the 3-sphere*, Kobe J. Math. **7** (1997) 125–138.

[3] K. Hong, S. No and S. Oh, *Links with small lattice stick numbers*, J. Phys. A: Math. Theor. **47** (2014) 155202 (9pp).

[4] Y. Huh and S. Oh, *The lattice stick numbers of small knots*, J. Knot Theory Ramif. **14** (2005) 859–868.

[5] Y. Huh and S. Oh, *Knots with small lattice stick numbers*, J. Phys. A: Math. Theor. **43** (2010) 265002 (8pp).

[6] Y. Huh and S. Oh, *An upper bound on stick number of knots*, J. Knot Theory Ramif. **20** (2011) 741–747.

[7] B. Jang, A. Kronaeur, P. Luitel, D Medici, S. Taylor and A. Zupan *New examples of Brunnian theta graphs*, Involve. **9**(5) (2016) 857–875.

[8] S. Kinoshita, *Alexander polynomials as isotopy invariants. I*, Osaka Math. J. **10** (1958) 263–273.

[9] R. A. Litherland, *A table of all prime theta-curves in S^3 up to 7 crossings*, a letter, 1989.

[10] T. Murau, *The tunnel number and the cutting number with constituent handlebody-knots*, preprint(arXiv:1802.03295 [math.GT]).

[11] H. Moriuchi, *An enumeration of theta-curves up to seven crossings*, J. Knot Theory Ramif. **18** (2009) 167–197.

[12] T. Motohashi, *2-bridge θ-curves in S^3*, Topol. Appl. **108** (2000) 267–276.

[13] M. Scharlemann and A. Thompson, *Link genus and the Conway moves*, Comment. Math. Heluetici **64** (1989) 527–535.

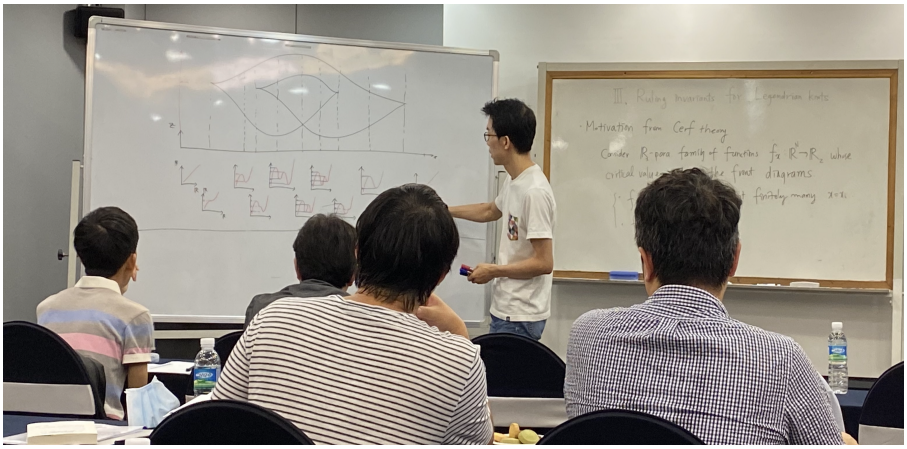
[14] W. Thurston, *Three-dimensional geometry and topology. Vol. 1*, Princeton Mathematical Series, vol. 35, Princeton University Press, Princeton, NJ, 1997. Edited by Silvio Levy.

[15] K. Wolcott, *The knotting of theta curves and other graphs in S^3*, Lecture Notes in Pure and Appl. Math. **105** (1987) 325–346.

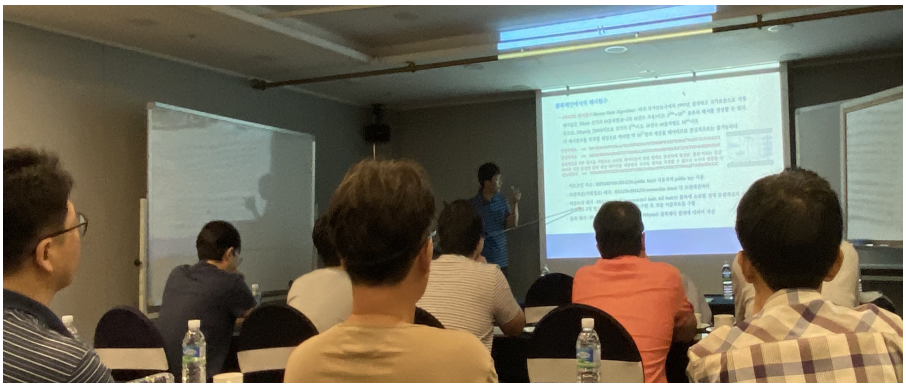
[16] Y. Q. Wu, *Minimally knotted embeddings of planar graphs*, Math. Z. **214** (1993), 653–658.

Commemorative Photographs

Youngjin's Lectures

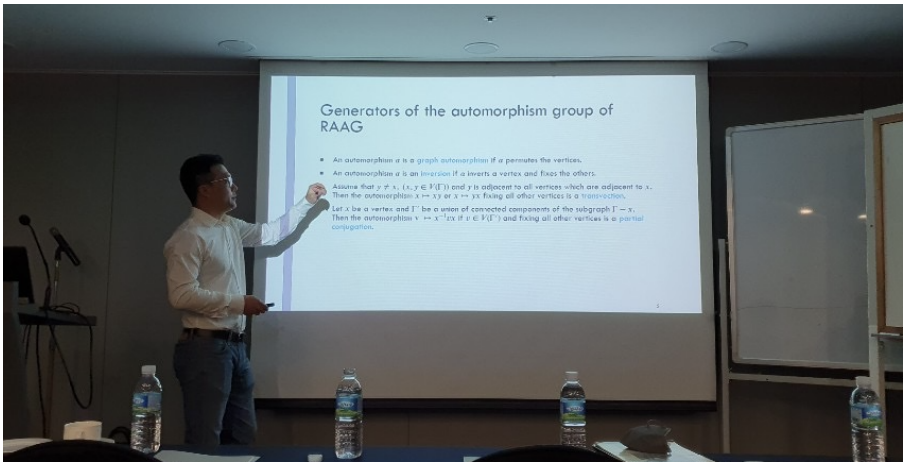


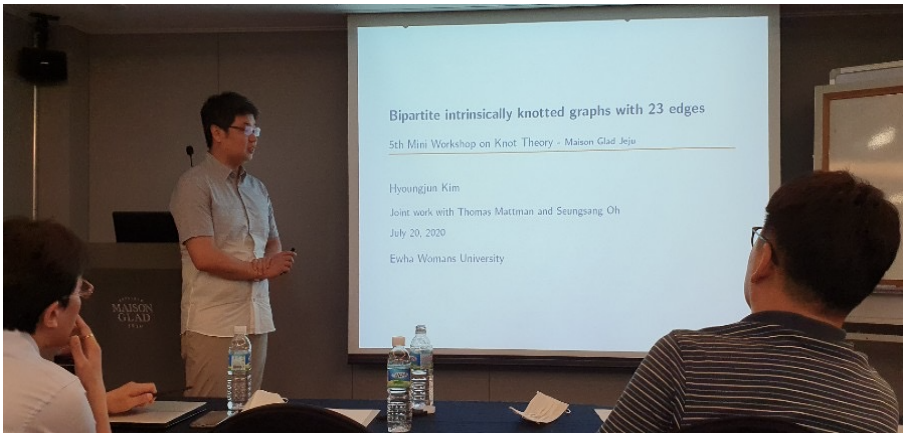

Blockchain overview
Seungsang Oh
Department of Mathematics, Korea University

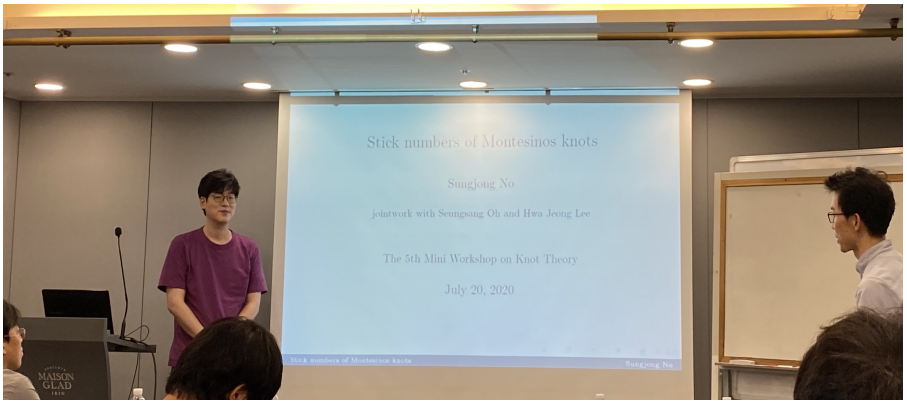


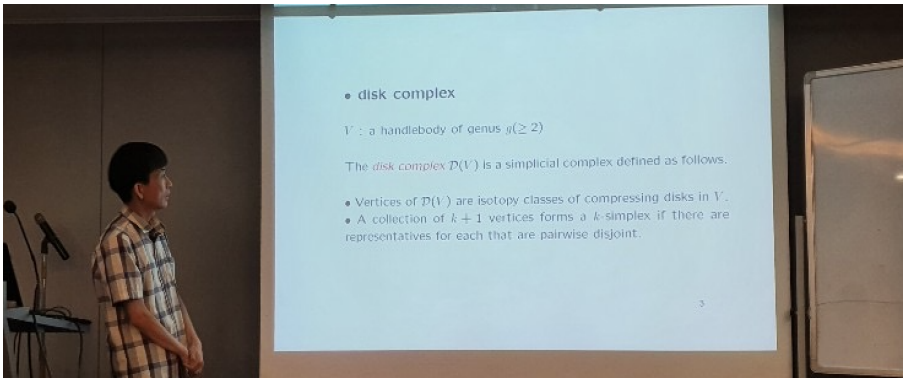

전자서명(Digital sign)

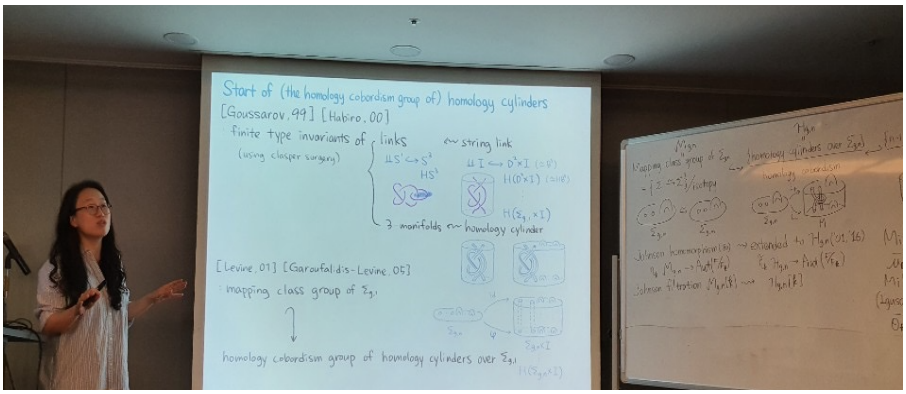
Other lecturers








• disk complex
V : a handlebody of genus $g(\geq 2)$
The *disk complex* $\mathcal{D}(V)$ is a simplicial complex defined as follows.
• Vertices of $\mathcal{D}(V)$ are isotopy classes of compressing disks in V.
• A collection of $k+1$ vertices forms a k-simplex if there are representatives for each that are pairwise disjoint.
3


Start of (the homology cobordism group of) homology cylinders
[Goussarov, 99] [Habiro, 00]
finite type invariants of
(using clasper surgery)
links
string link
3-manifolds
homology cylinder
[Levine, 01] [Garoufalidis-Levine, 05]
mapping class group of $\Sigma_{g,1}$
homology cobordism group of homology cylinders over $\Sigma_{g,1}$


Minimally knotted spatial cubic graphs with two vertices
Hyungkee Yoo
Minimally knotted spatial cubic graphs with two vertices
Hyungkee Yoo
Department of Mathematics
Korea University
The 5th Mini Workshop on Knot Theory
July 19, 2020