数理解析研究所講究録 1325 巻 2003 年 227-232

結び目の非自明性判定問題の計算量について

東海大学・理学部　原 正雄* (Masao Hara)
Deparmtment Mathematical Science
School of Science, Tokai University
日本大学・文理学部　谷 聖一†‡ (Sei'ichi Tani)
Department of Computer Science and System Analysis
College of Humanties and Science, Nihon University
中央大学・理工学部　山本 慎§¶ (Makoto Yamamoto)
Department of Mathematics,
Facullty of Science and Enginering, Chuo University

概 要

Hass-Lagarias-Pippenger は結び目理論，絡み目理論における様々な決定問題の計算量を解析し，3 次元球面内の結び目の自明性判定問題が **NP** に含まれることを証明した．彼らはこの問題が **NP** ∩ co-**NP** に含まれるだろうと予想している．その後 Hass は Algo, Thurston と共同で結び目の自明性判定問題を含む一般の 3 次元多様体における種数判定問題が **NP**–完全であることを証明している．我々は自明性判定問題の補問題である非自明性判定問題に対する対話型証明系を構成し，この問題が **IP**(2) に含まれること，言い換えると自明性判定問題が **AM** ∩ co-**AM** に含まれることを示す．このことから，自明性判定問題が **NP**–完全ならば $\Sigma_2^p = \Pi_2^p$ であることになり，自明性判定問題は **NP**–完全ではないと予想される．

*masao@ss.u-tokai.ac.jp
†sei-ichi@tani.cs.chs.nihon-u.ac.jp
‡本研究の一部は 2001 年度中央大学特定課題研究費および日本学術振興会科学技術研究費補助金 基盤研究 (C) (2) 14580391 による
§makotoy@math.chuo-u.ac.jp
¶本研究の一部は 2001 年度中央大学特定課題研究費および日本学術振興会科学技術研究費補助金 基盤研究 (C) 14540136 による

1 序

結び目理論とは多様体の部分多様体の位置を研究する幾何学である. 広い意味では向き付け可能な3次元多様体 M の円周と同相な部分多様体 K を**結び目**という. 最も簡単な結び目は M 内の円盤の境界になっている結び目であり, これを**自明な**結び目という.

M 内の結び目 K, K' について M の向きを保つ自己同相写像 $f : M \longrightarrow M$ が存在して $f(K) = K'$ が成り立つとき K と K' は**同じ型** であるまたは**同値**であるという. とくに自明な結び目はすべて同じ型である.

本稿ではいわゆる PL カテゴリーで議論する. つまり, 多様体には単体分割が与えられているものとし, 部分多様体もその単体分割の適当な細分における部分複体になっているものと仮定する. また, 多様体間の連続写像とはそれぞれの適当な細分のもとで単体的写像になっているものとする. PL 多様体, とくに3次元多様体の諸性質については [9] を参考すると良い.

ここでは同相な多様体は同じものとみなすので, 単体分割において単体同士が共有する辺や面などの情報だけが必要であり, 各単体の座標や形はほとんど意味がない. したがって, 多様体の符号化は 0–単体（頂点）から $1, 2, 3$–単体を順に頂点のリストで表現すればよい. さらに結び目もサイクルをなす頂点のリストを与えれば十分である.

一般には M は3次元球面 $\mathbb{S}^3$ のときに結び目ということが多いので本稿でもとくに断らない限り M は $\mathbb{S}^3$ であるとする. $\mathbb{S}^3$ 内の結び目 K に対して向き付け可能な $\mathbb{S}^3$ 内の曲面 F が存在し $\partial F = K$ となることが知られている. このような曲面を K の *Seifert* **曲面**といい, K の Seifert 曲面の中で種数が最小の曲面の種数を K の種数といい, genus(K) と記す. 一般の多様体内の結び目についても同様に種数を定義できるが, この場合には Seifert 曲面が存在してない場合もある. そのときは, 種数が無限大であるとみなす.

球面 $\mathbb{S}^3$ から任意の1点を取り除いた空間は3次元ユークリッド空間 $\mathbb{R}^3$ と同相だから結び目に含まれない点を取り除くことにより球面内の結び目は $\mathbb{R}^3$ 内の結び目と思うことができる. 逆に $\mathbb{R}^3$ 内の結び目は1点コンパクト化[1]することにより $\mathbb{S}^3$ 内の結び目と思うことができる. したがって, この2つを適宜使い分ける.

$\mathbb{R}^3$ 内の結び目は多辺形（折れ線）になっているので頂点の座標のリストで与えられる. さらに結び目の同値な範囲で変形することにより $\mathbb{R}^3$ から xy 平面への直行射影による結び目の像が平面上の自己交差のある折れ線になり, しかも各頂点の像は異なる頂点に対応し, 自己交差は辺の内部にあるようにできることが知られている. この射影に交差における上下の情報（z 座標の大小）を付加したものを結び目の**ダイアグラム**という. 結び目のダイアグラムは結び目に対して一意的に決まるわけではないが結び目を視覚的に表現する方法として重要である. 結び目を同値な範囲で変形してさらにダイアグラムの頂点の座標が整数値にすることができることは明らかである. したがって, $\mathbb{R}^3$ $(\mathbb{S}^3)$ 内の結び目の符号化はそのダイアグラムの頂点のリストと交点をなす辺を上の辺, 下の辺の順でリスト化すればよい. この符号化を結び目の標準の符号化とするが, [8] にもあるようにこの符号化は多項式時間で先に述べた $\mathbb{S}^3$ の単体分割を利用した符号化に変換することが可能である. このとき, ダイアグラムがのっている xy 平面が部分複体となるようにできる.

結び目理論の中心的問題はこの同値関係で結び目を分類することである. その意味では与えられた2つの結び目が同じ型になるかどうかを判定することは結び目理論で最も重要な

[1]無限遠点を加えると思えばよい.

問題の1つである．結び目が自明かどうかを判定する問題はその中でも基本的な問題であり，そのアルゴリズムに関する研究は計算位相幾何学の重要な問題である．

1961年, Haken [7] は結び目の自明性判定問題（以下 *Unknotting* と記す）が計算可能であることを証明した．同じ年に, Schubert [11] はそのアルゴリズムが結び目の種数判定問題にも適応できることを示した．ただし, 種数判定問題とは結び目 K と非負の整数 g の組を入力し $\mathrm{genus}(K) \leq g$ かどうかを判定する問題である．その時点ではこれらの問題の計算量を議論するには至らなかったが, 1999年に Hass-Lagarias-Pippenger [8] は Haken らのアルゴリズムをはじめとする様々な結び目理論の判定問題の計算量をそれまでの低次元多様体論の進展を踏まえて考察し, *Unknotting* が **NP** に含まれることや種数判定問題が **PSPACE** に含まれることを証明した．彼らは [8] のなかで *Unknotting* が $\mathbf{NP} \cap \text{co-}\mathbf{NP}$ に含まれることを予想している．さらに, Hass は Algo, Thurston [1] と共に一般の多様体内の種数判定問題が **NP**–完全であることを証明した．

本稿では *Unknotting* の補問題である結び目の非自明性判定問題（以下 *Knotting* と記す） に対する対話型証明系を構成し, *Knotting* が $\mathbf{IP}(2)$ に含まれることを証明する．任意の定数 $k > 2$ に対して $\mathbf{IP}(k) = \mathbf{IP}(2) = \mathbf{AM}$ であることが知られている ([2, 3, 6]) ので *Unknotting* $\in \mathbf{AM} \cap \text{co-}\mathbf{AM}$ であることが判る．もし, *Unknotting* が **NP**–完全ならば $\Sigma_2^P = \Pi_2^P$ が成り立つことになり, 多項式時間階層が第2層まで崩壊することになる．よって, *Unknotting* は **NP**–完全ではないだろうと予想される．

2 *Knotting* に対する対話型証明系の構成

この節では対話型証明系の定義と既知の性質をまとめた後に我々のプロトコルを述べるのに必要な範囲で結び目理論に関する用語をまとめプロトコルを述べる．結び目理論に関する詳細については [12] や [13] 等を参考にすると良い．

対話型証明系 [5] とは，証明者と検証者からなり，両者は入力へのアクセスを持ち，また，両者間には通信チャネルが存在し，交互にメッセージを計算した後通信チャネルに書き込み，最終的に検証者が受理か拒否をするようなシステムである．ここで，もう少し形式的な定義を与える．x を入力文字列，r をランダム文字列，C を通信チャネル上に書かれた履歴（文字列のリスト），k を計算が終わるまでの総ラウンド数とする．**検証者** V とは，(x, r, C) を入力すると文字列 S か特別な文字列 *accept*, *reject* のいずれかを出力する関数で，次を満たすものとする：

- $C = \epsilon$ のとき，出力は $S = V_1$
- $C = (V_1, P_1, \ldots, V_i, P_i)$ かつ $i < k$ のとき，出力は $S = V_{i+1}$
- $C = (V_1, P_1, \ldots, V_k, P_k)$ のとき，出力は *accept* か *reject* のいずれか．

同様に，**証明者** P とは，(x, C) を入力すると文字列 S を出力する関数で次を満たすものとする：

- $C = (V_1, P_1, \ldots, V_i)$ のとき，出力は $S = P_i$.

$(V(x, r), P(x))$ で，検証者 V と証明者 P による入力 x に対するランダム列 r を用いた対話型証明系を表わすものする．$(V(x, r), P(x))$ が k ラウンドの計算を行うよう設計されい

るとき，$V(x,r,(V_1,P_1,\ldots,V_k,P_k))$ が *accept* を出力するならば $(V(x,r),P(x))$ は受理するといい，*reject* を出力するならば $(V(x,r),P(x))$ は拒否するということにする．

言語 L が $\mathbf{IP}(k)$ に属するとは，k ラウンド後に *accept* か *reject* を出力する多項式時間計算可能な検証者 V が存在して次を満たすときをいう：

- $x \in L \Longrightarrow \exists P$ s.t. $\mathrm{Prob}_r[(V(x,r),P(x))$ が受理$] \geq 2/3$
- $x \notin L \Longrightarrow \forall P$ s.t. $\mathrm{Prob}_r[(V(x,r),P(x))$ が受理$] \leq 1/3$

任意の定数 $k>2$ に対して，$\mathbf{IP}(k)=\mathbf{IP}(2)=\mathbf{AM}$ となること，および，$\mathbf{IP}(2)\subseteq\Sigma_2^p$ が知られている ([2, 3, 6])．これに関連して，グラフ同型性判定問題は $\mathbf{AM}\cap\text{co-}\mathbf{AM}$ に属すことが知られており [4, 10]，グラフ同型性判定問題は **NP**–完全問題ならば多項式時間階層が $\Sigma_2^p=\Pi_2^p=\mathbf{AM}$ まで潰れることになる．

結び目 K に対して K の管状近傍 V の内部 $\mathring{V}$ を取り除いた空間 $\mathbb{S}^3\backslash\mathring{V}$ を K の**補空間**といい $E(K)$ と記す．補空間は管状近傍の取り方によらず同相である．$\partial E(K)$ と K の Seifert 曲面が交わってできる単純閉曲線を**ロンジチュード** という．ロンジチュードは Seifert 曲面の取り方によらず $\partial E(K)$ の isotopy を法として一意的に定まる．また，V がソリッドトーラスであることに注意すると V 内の $\partial V\cap D=\partial D$ を満たす 2 次元円盤 D で，$\partial V=\partial E(K)$ 内では 2 次元円盤の境界とはならないものが isotopy を法として一意的に存在する．これを**メリディアン**という．前節で述べたように入力されたダイアグラムのデータから $\mathbb{S}^3$ の単体分割を多項式時間で構成することができるが，得られた単体分割を細分することにより補空間が部分複体で得られる．さらに，必要ならダイアグラムに無駄な交差を付け加えることにより補空間の単体分割において結び目のロンジチュードとメリディアンが部分複体で得られるように分解することもできる．このような $\mathbb{S}^3$ の分割を**良い分割**と呼ぶ．単体分割や無駄な交差を付け加える作業は多項式時間で行えるので与えられたダイアグラムから良い分割を多項式時間で構成することができる．

プロトコル (*Knotting* に対する対話型証明系)
検証者は，証明者が与えられた単体分割が球面であれば 1 そうでなければ 2 を回答することを期待している．

入力: 結び目ダイアグラム

ラウンド 1

検証者

Step 1: 入力から球面 $\mathbb{S}^3$ の良い単体分割 S を作る．S において，結び目の管状近傍，補空間，ロンジチュード，メリディアンをそれぞれ V, E, ℓ, m とする．

Step 2: i_1 をランダムに 1 または 2 とする．

Step 3: $i_1=1$ のとき $M=S$, $i_1=2$ のとき $M=E\cup_{\ell=m,m=\ell}E$ とおく．

Step 4: M を S と $M=E\cup_{\ell=m,m=\ell}E$ の 2 回重心細分よりも単体の個数が多くなるようにランダムに細分し，頂点のラベルと単体のリストの順番をランダムに並べ替える．

Step 5: M を通信チャネルに書き込む

証明者 $j_1\in\{1,2\}$ を計算し，通信チャネルに書き込む

ラウンド 1 終了

ラウンド 2

検証者 Step 2 から Step 5 の i_1 を i_2 にして，もう一度繰り返す．

証明者 $j_2 \in \{1,2\}$ を計算し，通信チャネルに書き込む

ラウンド 2 終了

検証者 $i_1 = j_1$ かつ $i_2 = j_2$ ならば *accept* を出力し，そうでなければ *reject* を出力

終了

定理 上のプロトコルは *Knotting* に対する対話型証明系であり，*Knotting* は $\mathbf{IP}(2)$ に含まれる．

略証 まず検証者が多項式時間で動作することを確認しよう．これまでに述べたようにステップ 1 は多項式時間で終了する．細分も多項式時間で終了することは明らかだから M の構成に関して述べれば十分であろう．まず E のコピー E_0, E_1 を頂点のラベルが重ならないように構成し，E_ε $(\varepsilon = 0,1)$ のロンジチュードとメリディアンを $\ell_\varepsilon, m_\varepsilon$ とする．次に多様体 $\mathbb{S}^1 \times \mathbb{S}^1 \times [0,1]$ を考える．ただし，$\mathbb{S}^1$ は 1 次元球面（円周）である．$\mathbb{S}^1$ の 1 点 $*$ を固定する．$\mathbb{S}^1 \times \mathbb{S}^1 \times 0$ を $\mathbb{S}^1 \times * \times 0$ と $* \times \mathbb{S}^1 \times 0$ がそれぞれ ℓ_0, m_0 になるように ∂E_0 と同じように単体分割する．$\mathbb{S}^1 \times \mathbb{S}^1 \times 1$ を $\mathbb{S}^1 \times * \times 1$ と $* \times \mathbb{S}^1 \times 1$ がそれぞれ m_1, ℓ_1 になるように ∂E_0 と同じように単体分割する．これで $\mathbb{S}^1 \times \mathbb{S}^1 \times [0,1]$ の境界が単体分割が与えられるが，この分割を多様体の内部にまで拡張することは容易であり，多項式時間で終了する．E_0, E_1 と $\mathbb{S}^1 \times \mathbb{S}^1 \times [0,1]$ を単体分割が拡張できるように境界で張り合わせると M の単体分割になるのでステップ 3 は多項式時間で終了する．

次に，プロトコルの完全性を示す．証明者が直前に通信チャネルに書き込んだ単体分割が，球面であれば 1 を，そうでなければ 2 を通信チャネルに書き込む検証者を考える．非自明な結び目が入力されたとする．このとき M は決して球面と同相にはならない，なぜなら包含写像 $\iota : \partial E \subset E$ が誘導する基本群の順同型 $\iota_* : \pi_1(\partial E) \longrightarrow E$ は単射であり，van Kampen の定理から $\iota_* : \pi_1(\partial E) \longrightarrow M$ も単射であり，M は球面ではない．つまり，ステップ 3 の単体分割 M は $i_1 = 1$ のときは明らかに球面の単体分割であるが，$i_1 = 2$ のときは決して球面にはならない．したがって，証明者が通信チャンネルから受け取った単体分割が球面のものなら 1 をそうでないなら 2 を j_1 として通信チャンネルに回答すると，回答 j_1 と i_1 は必ず一致する．同様に，2 ラウンド目においても必ず $i_2 = j_2$ となり，受理される．つまり，非自明な結び目が入力されたときに受理される確率は 1 である．

最後に，プロトコルの健全性を示す．自明な結び目が入力されたとする．このとき，ステップ 3 の単体分割 M は $i_1 = 2$ のときも球面の単体分割になる．したがって，どのような証明者でも入力と通信チャンネル上のデータからだけで i_1 を推定することはできない．よって，$i_1 = j_1$ となる確率は高々 $1/2$ である．2 ラウンド目においても同様である．よって，受理される確率は高々 $1/4$ である．

以上により，プロトコルは *Knotting* に対する 2 ラウンド対話型証明系となっている．よって，*Knotting* $\in \mathbf{IP}(2)$ である． □

関連する問題が定数ラウンド対話型証明系を持つことを指摘いただいた東京工業大学の渡辺治氏に感謝する．渡辺氏の指摘が今回の研究の契機となった．

参考文献

[1] I. Agol, J. Hass, and W. Thurston. 3-manifold knot genus is NP-complete. In *Proceedings of the thiry-fourth annual ACM symposium on Theory of computing*, pp. 761–766, New York, USA, 2002. ACM Press.

[2] L. Babai. Trading group theory for randomness. In *Proceedings of the 17th ACM Symposium on Theory of Computing*, pp. 421–429, 1985.

[3] L. Babai and S. Moran. Arthur-merlin games: a randomized proof system. *Journal of Computer and System Sciences*, 36:254–276, 1988.

[4] R. B. Boppana, J. Hastad, and S. Zachos. Does co-NP have short interactive proofs? *Information Processing Letters*, 25:27–32, 1987.

[5] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18:196–208, 1989.

[6] S. Goldwasser and M. Sipser. Private coins versus public coins in interactive proof systems. In *Proceedings of the 18th ACM Symposium on Theory of Computing*, pp. 59–68, 1986.

[7] W. Haken. Theorie der Normalflachen, ein Isotopiekriterium für den Kreisknoten. *Acta Math.*, 105:245–375, 1961.

[8] J. Hass, J. C. Lagarias, and N. Pippenger. The computational complexity of knot and link problems. *Journal of the ACM*, 46(2):185–211, March 1999.

[9] J. Hempel. *3-Manifolds*. No. 86 in Annals of mathematics Studies. Princeton University press, Princetion, New Jersey, 1976.

[10] U. Schöning. Graph isomorphism is in the low hierarchy. *Journal of Computer and System Sciences*, 37:312–323, 1988.

[11] H. Schubert. Bestimmung der Primfactor zerlegung von Verkettungen. *Math Z.*, 76:116–148, 1961.

[12] 河内明夫（編）. 結び目理論. シュプリンガー・フェアラーク東京, 1990.

[13] 鈴木晋一. 結び目理論入門. No. 1 in Library of Mathematical Sciences. サイエンス社, 1991.