# 結び目と量子コンピュータの数学

河東泰之

東京大学
THE UNIVERSITY OF TOKYO
KAVLI IPMU INSTITUTE FOR THE PHYSICS AND MATHEMATICS OF THE UNIVERSE
RIKEN

IPMU, 2021 年 11 月 21 日

## 数学におけるダイバーシティ

これまで指導した大学院生約 70 人中，女性は 7 人，留学生は 13 人．これは東大数理平均の約 2 倍．このうち数学者になった人は世界 7 か国で 24 人，女性は日米で 3 人．またこれまで受け入れたポスドク研究員 17 人中，女性は 2 人，外国人は 7 人．家族の女性の大学の専攻は，母が化学，妻が電気工学，娘 2 人は医学と数学．

私自身は東大数学科を卒業してその年の夏にアメリカに留学．カリフォルニア大学ロサンゼルス校 (UCLA) に 4 年在学して Ph.D.(博士号) を取得．うち 1 年間はフランス・パリ郊外の数学，理論物理学の研究所 IHES に滞在．その後日本で助手 (現在の助教) になったあと，カリフォルニア大学バークレー校でポスドク研究員を 1 年間務める．

# 私のバックグラウンド

・大学院数理科学研究科: 理学部数学科に対応する大学院組織.
・世の中には実用と関係した数学を研究している人たちもたくさんいる.（たとえば AI，特にディープラーニングはかなり数学的な理論を用いる.）
・私はそうではなく，同僚からも応用と関係ない純粋数学者とみなされているはず.
・ずっと数学科に所属していて，自分と話が通じるのは純粋数学者だけだと思っていた.
・しかし最近の物理学の研究では多くの最先端の数学が使われていることに気づき，最近理論物理の人たちとの交流が深まっている．まずは素粒子理論（超弦理論），最近は物性物理学である.

## なぜ量子コンピュータが題名に入っているのか

私の研究テーマ： フォン・ノイマンの創始した作用素環論である．理論物理学とは関係するが，普通の分類では純粋数学に入る．

量子コンピュータは，Google の量子超越性など多くの IT 企業が莫大な人手と研究費をかけて研究している．

その中でマイクロソフトだけが他社と違う数学的アプローチを取っており，多くの数学者を雇用して研究を進めている．その内容が私の研究と関連しており，多くの数学の問題と関係する．

私のコンピュータ関連のバックグラウンド：大学生時代にパソコンの解説書，ゲーム集を書いて印税で生活していた．

# 数の代わりに行列を

$\mathbf{3}$ 次の行列は数が $\mathbf{3 \times 3}$ に並んでおり，$\mathbf{3}$ 次元の縦ベクトルにかかる．$\mathbf{4, 5, 6 \ldots}$ 次の行列も同様である．$\mathbf{4}$ 次元以上のベクトルの意味が分からないかもしれないが，数学的にはただ数が縦に並んでいるだけである．

また，行列は数と似ている．同じサイズの行列は足したり掛けたりできるし，大小関係も，$\boldsymbol{A \geq B}$, $\boldsymbol{A \leq B}$ のほかに「どちらでもない」というものを許容すればかなりうまくいく．

今まで数だと思っていた，位置，エネルギー，運動量などは実は行列であるというのが量子力学の教えである．時空の物理学や究極の粒子を求めていくと，必然的に数の代わりに行列を考える必要が生じる．ただしサイズが無限大の行列を考えることが重要である．

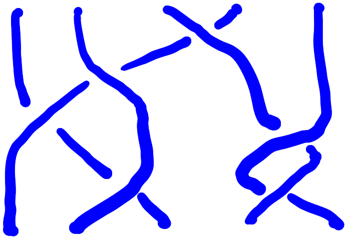
# 作用素環

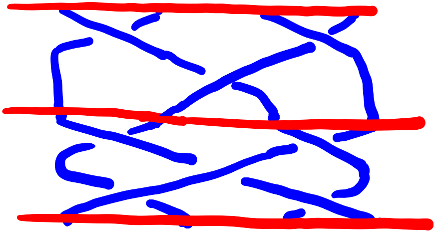
この種の無限次元版の行列のようなものを作用素または演算子という．どちらも operator の和訳である．これらは行列のように足したり掛けたりすることができる．足し算や掛け算が数のようにできる集合を環というので，作用素のなす環のことを作用素環という．これは1930年代にフォン・ノイマンが考え出した．

フォン・ノイマンは，計算機開発(「フォン・ノイマン型アーキテクチャ」),『量子力学の数学的基礎』の出版，ゲーム理論(数理経済学)の元祖，原爆開発への関与などでよく知られ，20世紀最高の科学者の一人．純粋数学においても多数の偉大な業績がある．作用素環は量子力学に関連する数学的構造として導入されたもので，彼の数学における最大の業績の一つである．

## 組み紐

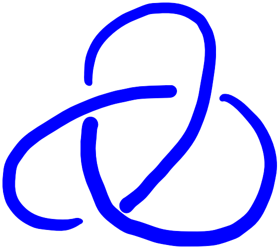
$\boldsymbol{n}$ 本の紐が横に並んで上から下に垂れていて途中でこれらが絡まっている，という状況を考える．こういうものを組み紐という．紐は太さがなく，自由に伸び縮みさせられるが切ることはできない，紐は必ず上から下に垂れており，上に上がることはない，とする．また同じ本数の組み紐が二つあるとき，上下にくっつけると新しい組み紐となる．これを組み紐の積という．

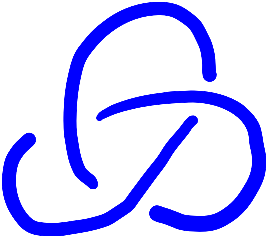




# 結び目

これと似たものとして，結び目というものがある．$n$ 本の紐があり，各紐の両端はつながって閉じている．紐の太さはないものとし，紐は自由に伸び縮みさせられるが切ってはいけないものとする．この設定で互いに移り合える結び目は同じものと思う．二つの結び目が同じかどうか判定することが根本問題である．

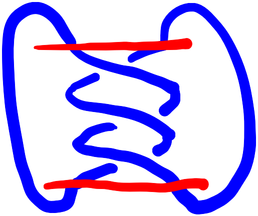


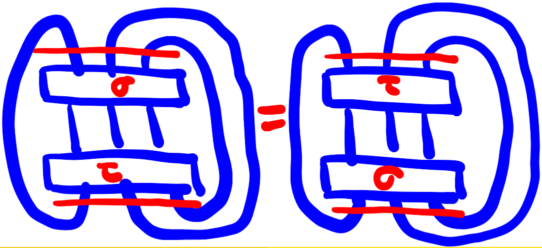


たとえば上の二つの結び目は互いに移り合えない．

## 組み紐から結び目へ

組み紐と結び目は似たものだが，もっと正確な関係が分かっている．組み紐が一つあったとすると，$n$ 本の紐のそれぞれの上端と下端を図のようにつなぐ．これによって結び目ができる．
実はどのような結び目もこのようにして組み紐から作れることが分かっている．さらに次の図のように，違う組み紐から同じ結び目ができることもあるのだが，これについてもいつそうなるかが正確にわかっている．

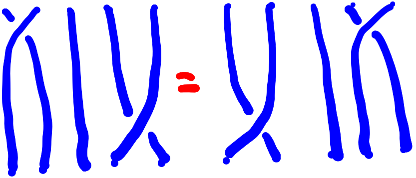


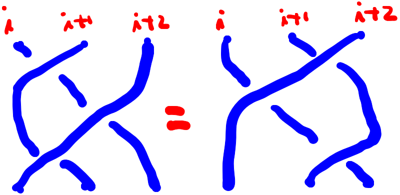


# 行列と組み紐

行列と組み紐には何も関係がないように見えるが，ジョーンズは1984年に無限次元空間の研究を通じて驚くべき関係を発見した．

まず組み紐の間にある関係を調べる．$\boldsymbol{i}$本目の紐と$\boldsymbol{i+1}$本目の紐を入れ替える操作を$\boldsymbol{\sigma_i}$と書く．すると左図のように，$|\boldsymbol{i}-\boldsymbol{j}|>\mathbf{1}$の時$\boldsymbol{\sigma_i\sigma_j=\sigma_j\sigma_i}$であり，また右図のように$\boldsymbol{\sigma_i\sigma_{i+1}\sigma_i=\sigma_{i+1}\sigma_i\sigma_{i+1}}$である．





# 行列による表現とトレース

各 $\boldsymbol{\sigma}_i$ に同じサイズの行列を対応させ，$\boldsymbol{\sigma}_i\boldsymbol{\sigma}_j = \boldsymbol{\sigma}_j\boldsymbol{\sigma}_i$, $\boldsymbol{\sigma}_i\boldsymbol{\sigma}_{i+1}\boldsymbol{\sigma}_i = \boldsymbol{\sigma}_{i+1}\boldsymbol{\sigma}_i\boldsymbol{\sigma}_{i+1}$ の関係式が行列側でも保たれるようにする．これを組み紐群の表現と言う．(このときこの行列の表示にパラメータ $\boldsymbol{t}$ が入っている．)

行列 $\boldsymbol{A} = (\boldsymbol{a}_{jk})$ に対し，対角成分 $\boldsymbol{a}_{jj}$ を足したものを行列 $\boldsymbol{A}$ のトレースと言い，$\mathbf{Tr}(\boldsymbol{A})$ と書く．行列 $\boldsymbol{A}, \boldsymbol{B}$ に対し，一般に $\boldsymbol{AB} \neq \boldsymbol{BA}$ であるが，常に $\mathbf{Tr}(\boldsymbol{AB}) = \mathbf{Tr}(\boldsymbol{BA})$ という重要な性質が成り立つ．

そこで，組み紐 $\boldsymbol{\sigma}, \boldsymbol{\tau}$ に対し，対応する行列を $\boldsymbol{A}, \boldsymbol{B}$ とすれば，$\boldsymbol{\sigma\tau}$ と $\boldsymbol{\tau\sigma}$ は一般に違う組み紐であるが，組み紐の上下をつなぐ操作で同じ結び目を与え，また $\mathbf{Tr}(\boldsymbol{AB})$ と $\mathbf{Tr}(\boldsymbol{BA})$ は等しくなっていることがわかる．

# 結び目のジョーンズ多項式

結び目が与えられたとき，これを作り出す組み紐を一つ取り，対応する行列を考え，そのトレースを取る．組み紐が，$\sigma\tau$ でも $\tau\sigma$ でもできるトレースは同じである．違う組み紐が出てくるパターンはもう一つあるが，少し細工すれば，そちらの場合でも，生じるトレースが同じであるようにできる．

これで一つの結び目から生じるトレースは一つであるようにでき，結び目に数を対応させる規則ができた．最後に出てくる数にもパラメータ $t$ が入っているので，$t$ の式(より正確には $\sqrt{t}^{\pm 1}$ の多項式)が出てくる．結び目にこの式を対応させる規則をジョーンズ多項式という．たとえば前のページの結び目に対応する式は $t + t^3 - t^4$, $t^{-1} + t^{-3} - t^{-4}$ であることがわかる．

## マイクロソフトの取り組み

カリフォルニア大学サンタバーバラ校内にマイクロソフト・ステーションQが2005年に設立された.

初代所長は，4次元ポアンカレ予想の解決により1986年にフィールズ賞を受賞したフリードマンである．彼がゲイツに働きかけてこの研究所ができた．現在のトップはフリードマンの弟子のチェンハン・ワンで，彼ももともとの専門は4次元トポロジーである．現在も多くの数学者を雇用して，量子コンピュータに関連する話題を研究している.

私は3回行ったことがあり，ジョーンズ多項式に関係する研究をしている人たちがいる．ジョーンズの弟子も何人も採用されていた.

# 普通のコンピュータの数学的原理

現行のコンピュータの原理

ビット：0 または 1

ビットの有限列に対し操作を行う．基本演算はたとえば，2 ビットの NAND：$(\boldsymbol{a}$ かつ $\boldsymbol{b})$ の否定であり，四則演算は NAND の組み合わせで実現できる．

計算の複雑さを測るには，基本演算が何回必要かを数える．

$\boldsymbol{n}$ ビットの入力の処理に必要な基本演算の回数が $\boldsymbol{n}$ の多項式で抑えられるならば，実用的な速いアルゴリズムであると考えられる．

たとえば素数判定はそのようなアルゴリズムが知られているが，素因数分解については知られていない．

## 量子コンピュータの数学的原理 (1)

量子ビット: 複素2次元ベクトル空間の単位ベクトル $\boldsymbol{\alpha}|\mathbf{0}\rangle + \boldsymbol{\beta}|\mathbf{1}\rangle$, $(|\boldsymbol{\alpha}|^2 + |\boldsymbol{\beta}|^2 = \mathbf{1})$.
$\boldsymbol{n}$ 量子ビットの入る空間：複素 $\mathbf{2}^{\boldsymbol{n}}$ 次元ベクトル空間
正規直交基底ベクトルとして $|\boldsymbol{a}_1\boldsymbol{a}_2\cdots\boldsymbol{a}_n\rangle$ が取れる (各 $\boldsymbol{a}_j$ は $\mathbf{0}$ または $\mathbf{1}$).

基本演算として例えば $\dfrac{\mathbf{1}}{\sqrt{\mathbf{2}}}\begin{pmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{1} & -\mathbf{1} \end{pmatrix}$,

$\begin{pmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \boldsymbol{e}^{\pm\pi i/4} \end{pmatrix}$, $\begin{pmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} \end{pmatrix}$ を取る.

これらを2次元分，あるいは4次元分の空間に作用させる.

# 量子コンピュータの数学的原理 (2)

複素 $2^n$ 次元ベクトル空間内で単位ベクトルを初期化する． $\longrightarrow$ 上記の基本演算を有限回行う． $\longrightarrow$ 結果を観測する．

結果の単位ベクトルを $\sum \alpha_{a_1a_2\cdots a_n}|a_1a_2\cdots a_n\rangle$ とすると，確率 $|\alpha_{a_1a_2\cdots a_n}|^2$ で状態 $|a_1a_2\cdots a_n\rangle$ が観測される．

Yes か No かの問題なら確率 $p$ $(p > 1/2)$ で正しい答えを返せばよい (何度もやって多数決を取ればよい).

原理的には普通のコンピュータでも量子コンピュータでも解ける問題は同じである．しかし量子コンピュータの方がはるかに速く解ける問題がある (と思われる).

## トポロジカル量子計算

かつてマイクロソフトに所属していたキタエフが1997年に提唱した．エニオンと呼ばれる2次元平面内の準粒子を使う．(エニオンは多くの準粒子の総称だが，その存在は未確認である．)

エニオンを平面内で操作し，その時間的経路を組み紐とみなす．二つのエニオンが互いに位置を変えることが紐の絡まりに対応する．よいエニオンを使うと，紐を絡まらせる操作が量子ビットに対する基本演算の代わりとして使える．

組み紐や結び目は，紐を伸ばしたりひっぱったりしても同じものとみなされる．これはエニオンの経路が少々変動しても結果に影響を与えないということで，トポロジカルに安定でエラーに対して強い．

## エニオンのふるまい

有限種類のエニオンが一つのセットになっている．各エニオンには反エニオンがこのセットの中にある．(エニオンと反エニオンは同じこともあれば違うこともある．) 二つのエニオンがぶつかると，このセットの中のいくつかのエニオンに分解する．

何もない状態も「真空」と呼んでエニオンの一種とみなす．何もない状態からエニオンとその反エニオンの対が生じる．(対生成)．エニオンとその反エニオンがぶつかってできるエニオンの中には真空が含まれる．(対消滅)．

例 (イジング模型)：エニオンは $\mathbf{1}, \boldsymbol{\sigma}, \boldsymbol{\psi}$ の 3 種．各エニオンはその反エニオンは同じ．$\boldsymbol{\sigma}^2 = \mathbf{1} + \boldsymbol{\psi}$, $\boldsymbol{\sigma\psi} = \boldsymbol{\psi\sigma} = \boldsymbol{\sigma}$, $\boldsymbol{\psi}^2 = \mathbf{1}$ という積の規則がある．

## 組み紐とトポロジカル量子コンピュータ

一つの組み紐が，量子コンピュータの一つのプログラムに対応している．対応するジョーンズ多項式の $t$ がある複素数における値が，そのプログラムを量子コンピュータで実行した答えと対応している．

現在作られている量子コンピュータではエラーコントロールがうまくできておらず，実用レベルの計算を実行する妨げになっている．このような原理で計算ができれば，エラーコントロールが比較的容易にできるはず．これをトポロジカル量子コンピュータという．

このように，ある種のタイプの量子コンピュータを実現するための理論的枠組みは，実用と無関係に考えられた現代数学の抽象理論に支えられている．