2.7.5 計算理論

（1）研究開発領域の定義

計算理論とは、チューリングマシンのように抽象化された計算を使って、計算のモデルやアルゴリズムを理論的に扱う研究開発領域である。それは計算複雑性理論や計算可能性理論を含んでいる。電子計算機が実現し、現実的なリソースでの計算可能性を明らかにする目的で、アルゴリズムの効率と実効的計算可能性を問う計算量理論が発達し、公開鍵暗号の安全性に貢献し、P対NP問題が注目を集めた。近年は、量子計算機の実現や利活用を目的とした量子計算モデルや量子計算量の研究が進められ、量子超越性、耐量子計算機暗号、量子誤り訂正符号などが研究されている。

（2）キーワード

計算可能性、チャーチ・チューリングの提唱、計算量理論、多項式時間計算可能性、多項式階層、量子計算機、量子計算量理論、量子超越性、耐量子計算機暗号、量子誤り訂正符号

（3）研究開発領域の概要

［本領域の意義］

計算理論が数学の一分野になったのは、数学の長い歴史の中では驚くほど新しい。計算理論は、20世紀前半に数学の基礎に関する数理論理学の研究から生まれた。それは計算可能な関数を一般帰納的関数によって定義するというチャーチ・チューリングの提唱が起源である。計算の可能性や効率、優位性を取り扱うことができ、それと結びついた暗号や符号を進化させることができることが本領域の意義である。以下で歴史を元により詳しく見ていく。

まずは18世紀までさかのぼろう。18世紀にカントは、論理学はアリストテレスの時代に完成され、それ以後、後退もなければ、進歩もなかったと書いた。しかし、17世紀にライプニッツは形式言語による科学の普遍記述という構想を明らかにし、19世紀にはブールの記号論理学の体系が生まれた。これは、命題論理と呼ばれ、アリストテレスの論理学を大いに一般化したが、数学を基礎付けるには不十分であった。19世紀末にフレーゲは述語論理を発見し、数学を述語論理によって基礎付けるために「全ての述語の外延が集合をなす」という内包公理を仮定したが、ラッセルはそこから矛盾が導かれることを発見し、19世紀末の数学の危機と呼ばれる状況が生まれた。この危機を救うために、ヒルベルトは、数学を述語論理で形式化し、公理系の無矛盾性を数学的に証明するという形式主義のプログラムを提唱した（ヒルベルトの23問題の2番目）。

ところが、1931年にゲーデルは、不完全性定理を発見して、算術を含む無矛盾な公理系には、肯定も否定も証明できない命題が存在し、特にその理論の無矛盾性を意味する命題がそれにあたることを証明して、形式主義のプログラムの本質的困難を明らかにした。この証明の中で、ゲーデルは原始帰納的関数という数論的関数が、無矛盾な自然数論で表現可能、つまり、計算の過程が定理の証明として書き下せることを示した[1)]。1936年に、チャーチは、自然数論で表現可能な関数の全体が、原始帰納的関数をより一般化した一般帰納的関数のクラスに一致することを一つの根拠として計算可能関数とは一般帰納的関数のことであると提唱し[2)]、さらに、チューリングはチューリング機械と呼ばれる計算機の数学モデルを定義して、チューリング機械で計算可能な関数の全体も一般帰納的関数に一致することを示した[3)]。ここから、計算可能な関数を一般帰納的関数によって定義するというチャーチ・チューリングの提唱が生まれた。これが、数学の一分野としての計算理論の始まりであり、計算可能性という新しい概念が数学の中に生まれた。

プログラミング可能な機械式計算機は、19世紀にバベッジによって最初に設計されたとされるが、チューリング機械が生まれて10年ほどでプログラム内蔵型電子計算機が完成した。ところが、計算可能な関数といえども、現実的な時間内には解けない事例（例えば、シラミつぶしに解を探索するアルゴリズムなど）が明らかになると、計算の効率を研究する計算量理論が生まれた。計算量に計算量理論では、実効的な計算可能性

として、入力の桁数の多項式時間でチューリング機械による計算が完了することを求める。この多項式時間計算可能性の概念は、階層（多項式階層）として理解されており、また現代社会で必須の公開鍵暗号の理論と深く結びついている。1976年にDiffieとHellmanは、暗号化関数の計算量と復号化関数の計算量の間にギャップを与える「落とし戸付き一方向性関数」の概念で公開鍵暗号の原理を提唱したが[4]、これは1978年にRSA暗号として実用化された。

20世紀も終わりに近づくと、新しい計算モデルである量子計算機の理論が生まれ、従来のチューリング機械に基づく計算量理論に従って、暗号の安全性を論ずることに疑問を投げかけることになった。チューリング機械の動作や状態記述は古典物理学と共通のものであったが、Deutschが1985年に量子力学の原理に従う計算モデルである量子チューリング機械の定式化を与えると[5]、1994年にはShorが素因数分解を量子チューリング機械によって多項式時間で解決する量子アルゴリズムを発見し、量子計算機が実現すると素因数分解の計算量を根拠とするRSA暗号などの公開鍵暗号の安全性が崩壊することを示した[6]。

現在では、量子チューリング機械に基づく量子計算量理論が生まれ、量子計算機が実際に古典計算機を凌駕することを示す量子超越性や、量子計算機でも安全性が崩壊しない公開鍵暗号とされる耐量子計算機暗号などの研究が進められている。一方で、量子計算機の動作に必須な量子コヒーレンスは、環境の影響で破壊されやすく、不可避の量子誤りを生むことが知られたが、それを訂正する量子誤り訂正符号が生まれ、それを組み込んだ誤り耐性型量子計算機・アーキテクチャーにより、いくらでも大規模な万能量子計算機が理論的に実現可能だとされている。

［研究開発の動向］

❶ 計算可能性

計算可能性理論において近年目覚ましい発展を遂げているのは、計算論的ランダム性の理論[7]と計算可能解析学[8]が挙げられる。

計算理論において、理論的にも実用的にも幅広く用いられている概念として、乱数（ランダム性）がある。ところが、現代確率論は、確率概念を公理的に取り扱う代償として、「確率」や「ランダム」が何であるかという問いに答えを与えない。公理的確率論では切り捨てられた観点を補完するために、晩年のコルモゴロフらは、計算可能性に基づくランダム性と情報の理論を構築した。この計算論的ランダム性の理論では、データ圧縮可能性に基づく情報量（コルモゴロフ複雑性）によって、個々の数学的対象がどれだけの規則性を持つかを定量化し、ランダムか否かをふるい分けることができる。

近年の計算論的ランダム性の理論は、計算可能解析学の知見を取り込むことによって飛躍的な発展を遂げている。古典計算論は離散的な問題を対象とするが、一般に実世界の問題は、何らかの形で実数を含む連続的な構造によってモデル化される。このため、実数などの連続量の計算可能性に関する理論が、理論的にも実用的にも重要である。このために誕生したものが、計算可能解析学と呼ばれる分野である。

計算可能解析学によって、連続量構造の下で計算論的ランダム性を分析することが可能になり、例えばデータ圧縮の概念の解析学・幾何学的理解が大きく進んだ。近年は、データ圧縮率とフラクタル次元の関連性に関わる新たな技術が開発され、その応用として、フラクタル幾何学の問題が解決されている[9]。その他にも、計算論的ランダム性の理論の技術は超越数論などへも応用され、数学の他分野への応用技術としての重要性が増している。

これらの枠組みの理論的整備は重要な課題である。計算可能解析学では、「連続的なデータ構造をどうコンピューターで（近似的に）取り扱うか」という点が問題になる。どのような数学的対象ならば（数学的構造を崩さずに）デジタルの世界にコード可能かを整備するための強力な枠組みとして、圏論のような抽象数学の理論が、近年、幅広く用いられるようになった[10]。

この下地となるものが直観主義論理に基づく数学（構成的数学）である。クリーネは直観主義算術の計算論的解釈（実現可能性解釈）を与え、直観主義論理は計算機科学の論理として扱われるようになった。

グロタンディークらの導入したトポスの概念は、一種の数学的宇宙の役割を担い、その内部論理は直観主義論理に従う。 Hylandはクリーネの実現可能性解釈に基づくトポスを発見し、それを計算可能数学の世界と呼んだ。計算可能解析学は、このような計算可能数学のトポス内部における解析学として整備できる[11)]。

❷ 多項式階層

CookやKarpにより、NP完全問題[12)] の存在が明らかにされた後、Meyer–Stockmeyer[13)] は、自然な問題の中で、NPよりさらに難しいと思われる問題が存在することに着目した。この着想を一般化し、NP完全問題を解くオラクル（サブルーチン）を再帰的に呼ぶことができる非決定性チューリングマシンで認識できる言語クラスを多項式階層（PH: Polynomial Hierarchy）として定義した。すなわち、再帰の深さにk対応する言語クラスを Σ_k^p で表すことにすると、 $\Sigma_{k+1}^p = \mathrm{NP}^{\Sigma_k^p}$ であり、PHは全てのにk対する Σ_k^p の合併集合として定義される。「階層」と呼ばれる理由は、定義から $\Sigma_k^p \subseteq \Sigma_{k+1}^p$ であるため、 Σ_k^p が入れ子構造になっているためである。また、定義から、 $\Sigma_1^p = \mathrm{NP}$ である。

PHに関して、「 Σ_k^p は、 Σ_{k+1}^p の真部分集合である」と言う命題（予想）の真偽は、P対 NP問題にも深く関連する重要な未解決問題である[14)]。この予想は、「PHが無限の階層を持つ」と言うこととも同値であることが知られている。 PHに関する研究は、計算量理論の発展に、さまざまな角度から影響を与えてきた。

例えば、 Σ_k^p が Σ_{k+1}^p の真部分集合であることの状況証拠を与える標準的な手法として、オラクル分離という手法がある。この証明のためには、ある論理関数を計算する定数深さ論理回路のサイズの下界を与えれば良いことから、論理回路サイズの下界に関する研究の強い動機付けとなった。

また、「PHが無限の階層を持つ」という予想が正しいという仮定のもとで、「充足可能性問題（SAT）は、多項式サイズの回路では解けない」、「グラフ同型問題は、NP困難ではない」など、多くの重要な命題が真であることが示されている。

さらに、戸田[15)] は、「#P関数を計算するサブルーチンが与えられれば、多項式時間でPHを計算可能である」という驚くべき定理を証明し、PHと数え上げに関するクラス# Pの間の橋渡しを実現した。ここで言う# Pとは、NP に属する決定問題に対応した数え上げ問題のクラスである。この事実は、量子超越性の理論において本質的な役割を果たしている（❸量子超越性の項目参照）。

最近では、量子計算[16)] の観点から、PHが注目されている。量子計算で高確率（＝誤り確率が高くない）かつ多項式時間で計算可能な決定問題のクラスをBQP（Bounded-error Quantum Polynomial time）と呼ぶ。量子計算の計算能力を数学的に明らかにすることは、量子計算量理論の観点からばかりでなく、現在開発が進められている量子計算機の適用分野を明らかにする上でも、極めて重要である。それは、まさにBQPを古典計算量クラスとの関係の中で特徴付けることに他ならない。特に、BQPがPHを構成する各階層に対して、どのような関係にあるかを明らかにすることは、最重要な問題の一つとなっている。

これまでの研究で、高確率（上記BQPと同じ）かつ多項式時間で古典計算可能な決定問題（BPP：Bounded-error Probabilistic Polynomial time）[12)] は、量子計算でも高確率かつ多項式時間計算可能であることが証明されている。一方、BQPは、多項式時間の古典計算で（低確率かもしれないが）計算可能であることが証明されている（PPは、後者の古典確率計算に対応する決定問題クラス[12)]）。しかし、BQPとPHの関係は現時点で不明である。

❸ 量子超越性

ある計算タスクにおいて、量子計算が、古典計算より真に高速であること（量子優位性）を示すことは、量子計算の研究が始まって以来、究極の目標の一つである。これは、チャーチ・チューリングの提唱の拡張（計算量版）を否定することとも捉えられる。これまでの研究で、通信計算量やオラクル計算など一部のモデルでは、量子の優位性が証明されてきたが、最も基本的な量子計算モデルでは、いまだ証明がなされていない。これに対し、近年、量子優位性を示す対象を、必ずしも意味のある計算タスクに限定せず、人工的なタスクも含む、より広い範囲に拡張して考える機運が高まってきた。量子超越性とは、このような意味での量子優位性を指すことが多い。多くの場合、量子計算機の出力分布を、古典計算機で効率的に再現（サンプリング）できるかどうかで、量子超越性の有無を定義する。

最近、量子計算機の実機開発が活発に行われるようになるにつれ、物理実装可能な量子計算機に対する量子超越性の有無が注目を集めている。そのような量子計算機の数理モデルはいくつか存在するが[17]、現在において、最も重要なモデルは、ボソンサンプリング[18]とランダム量子回路[19]である。前者は、適応的な観測を含まない、線形光学素子を用いた回路による計算モデルであり、比較的実装しやすいと考えられている。一方、後者は、Google[20]が発表した量子超越性で用いた手法をより数学的に厳密化した計算モデルである。

これらのモデルに対して量子超越性を示す手法は、大筋において共通しており、その基盤はAaronson–Arkhipov[18]とBremner–Jozsa–Shepherd[21]により築かれた。それは「PHは無限の階層を持つ」（❷多項式階層の項目参照）という計算複雑性の研究者の多くが正しいと信じている予想に矛盾することを示すアイデアである。この証明には、戸田の定理やStockmeyerによる近似数え上げ手法など、計算量理論の分野で発見された高度な知識が使われている。

現時点での大きな課題の一つは、量子計算の数理モデルを、（ノイズ等を考慮した）より現実的なものに近づけると、上記の予想に加えて、これまで十分に研究されたことのない新たな計算量的仮定を置く必要がある点である。より完成された理論にしていくためには、仮定を必要としない新たな枠組みを生み出す方向と仮定を証明する方向と考えられるが、いずれにしても、計算量理論に新たな研究テーマを提供しつつあると考えられる。

さらに大きな課題としては、量子計算機の出力分布を古典計算機で再現する問題に関する量子超越性が、実用的な問題、あるいは少なくとも、解を出力させる問題に関する量子超越性に知見を与えられるかと言うことがある。この点については、部分的な結果はあるものの、今後の研究の進展が期待される。

❹ 耐量子計算機暗号

暗号技術は、データの盗聴を試みる攻撃を防ぐ暗号化、データが改ざんされていないことを検証できるデジタル署名などの要素技術をもとにして、著作権保護、電子投票、仮想通貨と言った幅広い暗号応用を実現することができる。

データの暗号化では、送信者と受信者が同じ鍵で暗号化および復号する共通鍵暗号（AESなど）が広く使われているが、離れた送受信者が所有する同じ鍵は公開鍵暗号を用いて事前に配送されている。公開鍵暗号では、受信者が暗号化と復号の鍵ペアを生成して、その暗号化の鍵を公開することにより不特定多数の送信者が暗号化できる方式である。最も普及している公開鍵暗号として、1978年に提案されたRSA暗号[22]および1980年代に発表された楕円曲線暗号[23), 24)]があり、暗号通信プロトコルTLSなどで広く利用されている。また、デジタル署名では、署名生成者が署名生成と署名検証の鍵ペアを生成して、公開鍵暗号と同様に署名検証の鍵は公開する。署名者はデータMに対して署名生成の鍵を用いて署名Sを生成し、検証者はデータMと署名Sに対して公開されている署名検証用の鍵によりデータが改ざんされていないことを確認できる。ここで、通常のデータは鍵長より大きなサイズとなるため、暗号学的ハッシュ関数により特定の短い長さに圧縮したデータに対して署名が付けられる。最も普及しているデジタル署名としてRSA署名

やECDSA、暗号学的ハッシュ関数としてはSHA-256などがある。

RSA暗号・署名の安全性は、大きな整数の素因数分解が困難であることを安全性の根拠としている。最も高速な素因数分解アルゴリズムとして数体篩法[25]が知られており、素因数分解する合成数Nに対して準指数時間の計算量となる。並列計算機による大規模実験が多く実施されており、例えば768ビットの合成数を標準的なPC 1台換算で約1500年の計算時間で素因数分解した記録などがある。さらにはスーパーコンピューターの長期的な性能向上性（ムーアの法則）などを踏まえて、2030年までは2048ビットの合成数が安全に利用可能であると評価されている。一方、楕円曲線暗号やECDSAの安全性は、楕円曲線上の離散対数問題ECDLPの困難性を根拠としている。 ECDLPに対しては、数体篩法を適用する方法は知られておらず、ρ法[26]と言われる指数時間のアルゴリズムが最も高速となる。そのため、楕円曲線暗号やECDSAでは楕円曲線の群位数が256ビットのパラメーターが利用されており、RSA暗号・署名と比較して短い鍵長を持ち、より効率的な処理性能を実現している。

一方で、上記で述べた公開鍵暗号の安全性を支える素因数分解問題や離散対数問題は、Shor[27]により量子計算機による多項式時間のアルゴリズムが提案され、RSA暗号・署名や楕円曲線暗号・ECDSAは量子計算機により危殆化する状況にある。そのため、量子計算機に耐性のある数学問題を利用した耐量子計算機暗号（Post-Quantum Cryptography）[28]の研究が産官学をあげて活発に研究されている。代表的な耐量子計算機の方式としては、最短ベクトル問題（SVP）をもとにした格子暗号、誤り訂正符号を用いた符号暗号、多変数多項式求解（MQ）問題をもとにした多変数多項式暗号、楕円曲線の同種写像問題をもとにした同種写像暗号、ハッシュ関数の衝突困難性をもとにしたハッシュ関数署名などが挙げられる。

❺ 量子誤り訂正符号

いわゆる qubit 系に代表される有限次元ヒルベルト空間で表される量子系を素子として、そのコピーが複数集まってできる系（いわば量子版のレジスタ）における量子情報処理を、デコヒーレンスのような量子的な情報劣化にあらがって実現すべく考えられたものが量子誤り訂正符号である[29]。初めて考案された量子誤り訂正符号も古典の線形符号を利用していたのだが、古典の線形符号のうち、それを与えると自動的に量子誤り訂正符号が決まるクラスも分かっている（文献30）等）。それはシンプレクティック符号と呼ばれるクラスであり、基本的な研究対象である。シンプレックティック符号と上記の量子系との数学的に厳密なつながり[31), 32)]には文献30）で扱っている代数構造の全てが必須というわけではない。

（4）注目動向

[新展開]

❶ 計算可能性と圏論

近年まで、チューリング次数等の計算的複雑度の概念を圏論的に扱うことは難しいと考えられていた。専門家の間では、具体的な構成ベースの技法と、圏論のような抽象的技法は相性が良くないと考えられていたためである。近年の新たな動向として、トポス理論におけるグロタンディーク位相の論理学的成分を抽出したある種の様相概念を用いて、計算問題の複雑度の概念を捉えられることが明らかになった。これによって、高度に複雑化した計算可能性理論を、トポス理論的に見通しよく整備できるという期待が高まっている。

❷ 多項式階層

BQPとPHを無条件に分離することは、理論計算機科学における長年の未解決問題（PとPSPACEの分離）を導くので、極めて困難と考えられる。このため、現在の技術レベルで可能なアプローチとして、BQPとPHのオラクル分離が試みられてきた。最近（2019 年）になって、Raz-Tal[33]により、オラクル設定のもとで、BQPはPHに含まれないことが証明された。この結果は、オラクルを使わない通常の設定での、

BQPの特徴付けを与えるものではないが、ある種の状況証拠を与えるものと考えられている。

❸ 耐量子計算機暗号

同種写像暗号に関連して、乱数発生やハッシュ関数の構成への応用を見込んだ拡散性が高いエクスパンダーグラフが注目されている。いわゆるラマヌジャングラフはその中で特に重要であるが、これはそのグラフゼータ関数がリーマン予想を満たすことに由来している。

❹ 量子誤り訂正符号

注目すべき動向としては、シンプレクティック符号のサブクラスであるCaldarbank–Shor–Steane符号が量子鍵配送プロトコルの安全性を示すのに応用されている。

［注目すべき国内外のプロジェクト］

計算可能性理論、計算可能解析学、構成的数学等と深く関わる国内大型プロジェクトとしては、研究拠点形成事業A. 先端拠点形成型「数理論理学とその応用の国際研究拠点形成」が2015年度から2021年度まで実施されていた。現在は国内では複数の中型プロジェクトが並行に行われている。国外では、EUプロジェクトの “Computing with Infinite Data”（2017–2023）などが代表的である。このプロジェクトは、計算可能性理論、特に計算可能解析学を中心とするが、型理論などの研究者も深く関わっているため、計算可能性理論の圏論的観点からの理論的整備のみならず、厳密な連続量計算の実装面での開発研究も大きく進むことが期待されている。

多項式階層に関連する国内大型プロジェクトとしては、科研費学術変革領域（A）「社会変革の源泉となる革新的アルゴリズム基盤の創出と体系化（AFSA）」（領域代表：湊真一 （京都大学））が進行中である。AFSAのアルゴリズム応用も含む広い領域であるが、計画班として、関連分野の国内を代表する研究者が集結し、研究を推進している。また、海外では、Simon foundationからのファンディングを受け、UC BerkleyにSimons Institute for the Theory of Computingが2012年に設立された。以来、理論計算機科学の基礎を深めるとともに、他の科学分野（物理学、生物学、経済学等）における現象に内在する新たな計算理論の探究を目指している。

量子超越性は、数理科学的な研究と実験科学的な研究を両輪として進められている。実験科学的なアプローチは、量子計算機ハードウェアの開発と密接に関連しており、最近では、Googleが自社開発した量子計算機実機における量子超越性を発表した[20]。一方で、これが刺激になり、古典計算機による量子計算のシミュレーション技術の進展も著しい。実験的な意味での量子超越性の有無は、量子・古典双方のテクノロジーの進展にしばらくは依存することが予想される。また、IBMなどが一般向けに提供している量子計算サービスを用いて、量子化学計算などに代表される特定の応用について、量子超越性を実証する研究も近年活発に行われている。量子計算機全般に関して、世界各国の政府系ファンドが多く関わっており、国内では、文部科学省Q–LEAPや内閣府ムーンショット（目標6「誤り耐性型汎用量子コンピュータ」）が代表的である。

耐量子計算機暗号に関しては、2016年から米国国立標準技術研究所NISTは耐量子計算機暗号の標準化プロジェクト（https://csrc.nist.gov/Projects/post-quantum-cryptography）を進めてきており、2022年7月には格子暗号の暗号化方式CRYSTAL–KyberおよびデジタルCRYSTAL–DilithiumとFalcon、ハッシュ関数署名SPHINCS+が標準化方式として選出された。また、日本では、デジタル庁・総務省・経済産業省が運営する電子政府推奨暗号プロジェクトCRYPTREC（https://www.cryptrec.go.jp/）において、耐量子計算機調査ワーキンググループ（WG）や量子計算機時代に向けた暗号の在り方タスクフォース（TF）などが立ち上がっており、2018年は耐量子計算機暗号の研究動向調査、2019年には量子計算機が共通鍵暗号の安全性に及ぼす影響の調査に関する報告書を発表している。また、JST CRESTにおいて、2021年から研究課題「ポスト量子社会が求める高機能暗号の数理基盤創出と展開」が開始された。

（5）科学技術的課題

計算論的ランダム性の研究については、その解析学・幾何学的側面の理解が大きく進んでいるため、フラクタル幾何学や超越数論のみならず、数学の多様な分野へと応用の幅を広げていくことが課題である。また、計算可能性理論のより発展的なトピックを圏論およびトポス理論を用いて現代的に見通しよく整備することも重要な課題である。計算可能性理論の入り組んだ構造を圏論・トポス理論的に解きほぐすことによって、さまざまな計算的問題に対する新たな知見を得ることが大きな目標である。特に計算複雑性の理論のトポス理論的分析を経由した、構成的型理論や構成的集合論の観点からの複雑性解析が期待される。

多項式階層の研究において、BQPを古典計算量クラスとの関係の中で特徴づけることが簡単でない理由の一つは、量子計算の性質がまだ十分に解明されていないことも一因である。近年、古典計算理論の代表的成果である、PHや確率的検査可能証明（PCP）の量子版を構築しようとする研究が進んでいるが、これは量子計算の理解をより深めることに貢献することが期待される。同時に、量子物理や量子化学との関連もあることから、他分野との相互作用を通して、量子計算理論自体を拡張していくことが重要になってくる。一方、これらの知見をツールとして、古典計算理論にフィードバックしていく研究も期待される。

量子超越性に関する数理科学的・理論計算機科学的研究により得られた（あるいは今後得られる）成果を基礎として、量子計算機の実機を用いて量子超越性を実証するためには、量子計算機の出力分布から、量子超越性の有無を効率的に判定する手法に関する理論の整備が課題である。さらに、野心的な課題として、出力分布ばかりでなく、何らかの数値解を出力する問題に対する量子超越性の理論構築が望まれる。

耐量子計算機暗号に関しては、耐量子性を有する公開鍵暗号やデジタル署名で用いられる基本計算問題の困難性評価が重要な課題となっており、大規模解読実験を通して安全に利用するための暗号パラメーターの導出などの研究が進展している。更には、実利用の環境に適した効率的な実装アルゴリズムの研究開発が、産業界も巻き込み活発に行われている。耐量子計算機暗号を専門に議論する国際会議PQCryptoも毎年開催されるようになっている。

量子誤り訂正符号に関しては、最小距離を評価基準とした伝統的符号理論の観点からはおおよそ以下の課題に集約できる。（3）で述べたことから、直ちに得られる技術課題は従来から考えられてきた線形符号構成の問題をシンプレクティック形式に関する自己直交性という新たな制約下で解くというものである。個々の符号長、エンコードする情報量などのパラメーターに関して良い符号を構成する等の課題は古典の符号理論と同様に無限に存在する。最小距離の評価基準を用いた漸近論では、シンプレクティック符号構成の文脈で、Tsfasman–Vladut–Zink下界を達成する古典的な意味で自己直交な代数幾何符号の多項式時間構成という古典的符号理論の枠組みで述べられる課題が（暗に）示唆されていたが、これは濵田[34]が肯定的に解決した。想定する適用先によっては最小距離以外の評価基準も考えるべきであろう。実際、Shor[29]はシャノンの通信路容量にあたるものを量子誤り訂正について求める問題を提起しており、その後の発展を促した。

（6）その他の課題

数理科学の一分野としての計算理論領域を捉えると、基礎数学に属する計算可能性の研究から、量子技術に直結する量子超越性や耐量子計算機暗号の研究まで、幅広い分野と研究形態が含まれる。技術に直結する応用分野の研究であっても、一般に、課題解決型研究の探求範囲や発想を超える大きなブレークスルーが数理科学から生まれることが期待されている。そのため 、数学的研究方法の深い理解と素養に基づいた基礎科学としての自律的発展を担うと同時に、最新の科学技術の動向に調和して、境界領域に対する幅広い関心と知識を兼ね備えた人材の育成が望まれる。例えば楕円曲線に関しては、ミレニアム懸賞問題の一つであるバーチ・スウィンナートン＝ダイアー予想（BSD予想）が未解決のままである。このような純粋数学の課題が、今後の暗号研究に直接・間接的に影響を与えるであろうことは、研究人材の育成という意味でも重要なことである。

理論計算機科学全般については、科研費の大型プロジェクトを中心に安定的に研究助成が行われているが、

これについては、仮想的な研究組織による5年程度の時限的な研究活動となっている。恒久的な大型組織は存在せず、主に工学系・情報科学系の学科に分散的に所属する個々の研究室で研究者の自由な発想に基づく研究が行われている。一方、欧米では、理論計算機科学が、しばしば数学の一分野として扱われ、他の数学分野との垣根が低いことが革新的な結果を生み出す要因になっている側面もある。今後、日本においても、数学（数理科学）系研究者との交流を、より一層活発化していくことが望まれる。

一方で、近年、各国で研究が推進されている量子計算理論については、わが国では、量子計算機開発の国家プロジェクト（Q-LEAP、Moonshot等）の一部として推進されているが、開発チーム優先のプロジェクトの中では、数理科学者の参加は限定的である。また、これらは時限的なプロジェクトであるため、長期的視野に立った人材育成という観点からは、その役割は限定的である。このため、ある程度の規模を持った、量子計算理論の恒久的な育成システムが望まれる。

将来の量子計算理論研究者の育成には、量子物理学者や古典の計算理論・理論計算機科学（アルゴリズム理論や計算量理論）の研究者との研究交流が欠かせない。しかし、現状では、これらの分野との交流は、極めて限定的である。このため、このような大きなプロジェクトにおいて、既存の分野ごとのコミュニティーにとらわれない、若手数理科学研究者の参加、育成を積極的に促進する仕組みが望まれる。また、恒久的な研究者育成システムの観点からも、近年のデータサイエンス教育の普及に匹敵するような規模で量子技術や量子科学に関する基礎教育の普及も望まれる。

2021年にMIP*=RE定理という量子計算量理論におけるブレークスルーが伝えられた[35)]。この内容は、系として作用素環（フォン・ノイマン環）におけるConnesの埋め込み予想が否定的に解決されることを導く。このConnesの埋め込み問題は、量子情報のTsirelsonの問題と同値であることが知られている。この量子計算量理論によるConnesの埋め込み問題の否定的解決は、作用素環論と量子計算量理論とのこれまでにない新しいつながりを生み出し、量子計算に関わる全く新しい数学分野の創出の契機となる可能性がある。

新しい数学分野という観点からは、代数的数を広げる（単に超越数だと片付けてしまわない）ことに関するKontsevichとZagierの予想（2001）がある[36)]。この種の数学者の興味や関心が、計算機の格段の発達によってなされた新しい学問である計算理論と無関係でいられるわけではなく、10年20年先からバックキャストをするという期待からは、無視し得ない。

（7）国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	○	→	・計算可能性の研究では、研究者数が他国と比べて少ない中、国際的な存在感を保っている。国際誌 Computabilityの掲載論文数は世界 6位である。2022年の国際数学者会議で、計算可能性理論の招待講演者（1枠）に日本の横山啓太（東北大学）が選出された[37)]。 ・理論計算機科学については、科研費の大型プロジェクトを中心に、安定的に重要な成果を創出。恒久的な大型組織は存在せず、個々の大学研究室に委ねられている。 ・量子計算理論については、量子計算機開発の国家プロジェクト（Q-LEAP、Moonshot等）の一部として推進。これらは期限付き研究プロジェクトであり、恒久的な育成システムは極めて小規模。将来の量子計算理論研究者の育成に不安がある。 ・耐量子計算機暗号の研究では、大学だけでなくNTTや産業技術総合研究所（産総研）など研究機関からトップカンファレンスにおいて多くの論文発表がある。

	応用研究・開発	○	↗	・量子計算機開発および応用研究について、Q-LEAP、Moonshot等の国家プロジェクトを中心に推進。プロジェクトでは、NEC、富士通、日立などのメーカーも協力し、産学連携が進む。 ・企業による、量子技術に関する協議会QSTARも創設された。 ・耐量子計算機暗号では、デジタル庁・総務省・経済産業省が運営する電子政府推奨暗号プロジェクトCRYPTRECにおいて、産官学の研究者が参加する形で最先端の研究成果や実用研究が議論されている。
米国	基礎研究	◎	→	・計算可能性理論に関しては、国際誌 Computability、Annals of Pure and Applied Logic、Journal of Symbolic Logic、Journal of Mathematical Logic 等の掲載論文数は毎年、世界一であるが、近年は米国発の注目すべき研究は出ていないように見える。 ・理論計算機科学に関しては、トップ級論文誌・国際会議において、長年に亘って、他国を圧倒する貢献度。 ・Simons Institute for the Theory of Computing など、理論計算機科学の組織的な研究推進。 ・耐量子計算機暗号の基盤方式となる格子暗号を提案したグループがCourant Institute of Mathematical Scienceにあり世界をリードする研究をしている。
	応用研究・開発	◎	↗	・量子超越性に関しては、以下のように民間企業による研究・開発が顕著である。 −Googleの量子計算機実機による量子超越性の実証。 −IBMの量子計算実機の公開および、それを用いたアプリケーションの研究開発。 ・耐量子計算機暗号に関しては、米国国立標準技術研究所NISTにより標準化プロジェクトが進められており、2031年以降に実用化される次世代標準暗号が決定する予定である。
欧州	基礎研究	◎	→	・計算可能性研究については、国際誌 Computability の掲載論文数の世界2～4位は、順にドイツ、英国、フランスである。EUプロジェクト“Computing with Infinite Data”[38] などの大型プロジェクトが実施され、計算可能性理論の圏論的基礎などの注目度の高い研究を多数創出。 ・計算理論、量子理論の基礎研究で長い歴史。 ・理論計算機学においては、ドイツ、英国、フランス、スイスを中心として、トップ級論文誌・国際会議で、長年に亘り、顕著な実績。 ・暗号の基礎研究は大学だけでなくIBMなど企業においても活発に行われている。
	応用研究・開発	○	↗	・量子計算機開発の大型プロジェクトが進行中であるが、ハードウェア開発が中心。 −UK National Quantum Technologies Programme −EU Quantum Technology flagship ・耐量子計算機暗号に関しては、欧米の暗号研究者を中心として提案した方式が、米国国立標準技術研究所NISTが進める標準化プロジェクトにおいて採用された。
中国	基礎研究	○	↗	・計算可能性理論に関しては、国際誌 Computability の掲載論文数は世界13位であり、他の主要誌の論文数も同程度である。特筆すべき研究は出ていない。 ・中国科学院による量子情報科学の基礎研究拠点。 ・米国等で活躍した理論計算機科学の世界的な研究者（A. Yao等）が帰国し、精華大学・企業等で研究をけん引。 ・トップ級論文誌・国際会議における貢献度では、米国・ヨーロッパに及ばないが、近年、増加傾向。 ・数理情報分野の主要な国際会議の予稿集を含むSpringer LNCSにおける論文数は、過去5年で米国を上回り中国が1位となっている。
	応用研究・開発	○	↗	・66量子ビットの量子計算機実機による量子超越性実証。 ・Alibabaなどが量子計算機ハードウェア、アプリケーションの開発。 ・精華大学が応用数学の研究を進めるYanqi Lake Beijing Institute of Mathematical Sciences and Applications（BIMSA）を立ち上げ世界中から優秀な研究者を集めている。

韓国	基礎研究	△	→	・目立ったアクティビティが見られない。
	応用研究・開発	△	↗	・耐量子計算機暗号に関しては、ソウル大学校を中心として、格子暗号をクラウドコンピューティングに応用する技術で特徴的な研究成果がある。
その他の国・地域	基礎研究	○	↘	・計算可能性理論においては、ニュージーランド、シンガポール、ロシアが強力な地域として知られている。 国際誌Computabilityの掲載論文数は順に、5位、9位、8位である。国際数学者会議招待講演の計算可能性理論枠は、2006年の Rod Downey、2010年のAndre Niesと連続でニュージーランドであった[39]。特にアルゴリズム的ランダム性の理論の世界的研究をけん引している。近年も安定した成果を上げているものの、勢いは落ち着きつつある。
	応用研究・開発	―	―	基礎研究がもっぱらで、評価できる段階ではない。

（註1）フェーズ

基礎研究：大学・国研などでの基礎研究の範囲

応用研究・開発：技術開発（プロトタイプの開発含む）の範囲

（註2）現状　※日本の現状を基準にした評価ではなく、CRDS の調査・見解による評価

◎：特に顕著な活動・成果が見えている　　○：顕著な活動・成果が見えている

△：顕著な活動・成果が見えていない　　×：特筆すべき活動・成果が見えていない

（註3）トレンド　※ここ1～2年の研究開発水準の変化

↗：上昇傾向、→：現状維持、↘：下降傾向

関連する他の研究開発領域

・量子コンピューティング・通信（HW）（ナノテク・材料分野 2.3.5）

参考文献

1）Kurt Gödel, “On Undecidable Propositions of Formal Mathematical Systems,” in *The Undecidable: Basic Papers On Undecidable Propositions, Unsolvable Problems And Computable Functions*, ed. Martin Davis（Raven Press, 1965）, 39-74.

2）Alonzo Church, “An Unsolvable Problem of Elementary Number Theory,” *American Journal of Mathematics* 58, no. 2（1936）: 345-363, https://doi.org/10.2307/2371045.

3）Alan Mathison Turing, “On Computable Numbers, with an Application to the Entscheidungsproblem,” *Proceedings of the London Mathematical Society* s2-42, no. 1,（1937）: 230-265., https://doi.org/10.1112/plms/s2-42.1.230.

4）Whitfield Diffie and Martin E. Hellman, “New directions in cryptography,” *IEEE Transactions on Information Theory* 22, no. 6（1976）: 644-654., https://doi.org/10.1109/TIT.1976.1055638.

5）David Deutsch, “Quantum theory, the Church-Turing principle and the universal quantum computer,” *Proceedings of the Royal Society A* 400, no. 1818（1985）: 97-117., https://doi.org/10.1098/rspa.1985.0070.

6）Peter W. Shor, “Algorithms for quantum computation: discrete logarithms and factoring,” in *Proceedings 35th Annual Symposium on Foundations of Computer Science*（IEEE, 1994）, 124-134., https://doi.org/10.1109/SFCS.1994.365700.

7）Rodney G. Downey and Denis R. Hirschfeldt, *Algorithmic Randomness and Complexity*, Theory and Applications of Computability（New York: Springer, 2010）., https://doi.org/10.1007/978-0-387-68441-3.

8）Vasco Brattka and Peter Hertling, eds., *Handbook of Computability and Complexity in Analysis*, Theory and Applications of Computability（Springer Cham, 2021）., https://doi.org/10.1007/978-3-030-59234-9.
9）Jack H. Lutz and Neil Lutz, “Who Asked Us? How the Theory of Computing Answers Questions about Analysis,” in *Complexity and Approximation: In Memory of Ker-I Ko*, eds. Ding-Zhu Du and Jie Wang, Lecture Notes in Computer Science 12000（Springer Cham, 2020）, 48-56., https://doi.org/10.1007/978-3-030-41672-0_4.
10）Jaap van Oosten, *Realizability: An Introduction to its Categorical Side*, Studies in Logic and the Foundations of Mathematics 152（Elsevier Science, 2008）.
11）Andrej Bauer, “The Realizability Approach to Computable Analysis and Topology,” PhD thesis, School of Computer Science, Carnegie Mellon University, http://reports-archive.adm.cs.cmu.edu/anon/2000/CMU-CS-00-164.pdf,（2023年3月8日アクセス）.
12）Sanjeev Arora and Boaz Barak, *Computational Complexity: A Modern Approach*（Cambridge: Cambridge University Press, 2009）., https://doi.org/10.1017/CBO9780511804090.
13）Albert R. Meyer and Larry J. Stockmeyer, “The equivalence problem for regular expressions with squaring requires exponential space,” in *13th Annual Symposium on Switching and Automata Theory (swat 1972)*（IEEE, 1972）: 125-129., https://doi.org/10.1109/SWAT.1972.29.
14）Lance Fortnow, “Beyond NP: the work and legacy of Larry Stockmeyer,” in *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*（New York: Association for Computing Machinery, 2005）, 120-127., https://doi.org/10.1145/1060590.1060609.
15）Seinosuke Toda, “PP is as Hard as the Polynomial-Time Hierarchy,” *SIAM Journal of Computing* 20, no. 5（1991）: 865-877., https://doi.org/10.1137/0220053.
16）Michael A. Nielsen and Isaac L. Chuang, *Quantum Computation and Quantum Information*, 10th anniversary ed.（Cambridge: Cambridge University Press, 2010）., https://doi.org/10.1017/CBO9780511976667.
17）Aram W. Harrow and Ashley Montanaro, “Quantum computational supremacy,” *Nature* 549（2017）: 203-209., https://doi.org/10.1038/nature23458.
18）Scott Aaronson and Alex Arkhipov, “The Computational Complexity of Linear Optics,” *Theory of Computing* 9（2013）: 143-252., https://doi.org/10.4086/toc.2013.v009a004.
19）Adam Bouland, et al., “On the complexity and verification of quantum random circuit sampling,” *Nature Physics* 15（2019）: 159-163., https://doi.org/10.1038/s41567-018-0318-2.
20）Frank Arute, et al., “Quantum supremacy using a programmable superconducting processor,” *Nature* 574（2019）: 505-510., https://doi.org/10.1038/s41586-019-1666-5.
21）Michael J. Bremner, Richard Jozsa, and Dan J. Shepherd, “Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy,” *Proceedings of the Royal Society A* 467, no. 2126（2011）: 459-472., https://doi.org/10.1098/rspa.2010.0301.
22）Ronald Linn Rivest, Adi Shamir and Leonard Max Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communication of the ACM* 21, no. 2（1978）: 120-126., https://doi.org/10.1145/359340.359342.
23）Neal Koblitz, “Elliptic curve cryptosystems,” *Mathematics of Computing* 48, no. 177（1987）: 203-209., https://doi.org/10.1090/S0025-5718-1987-0866109-5.
24）Victor S. Miller, “Use of Elliptic Curves in Cryptography,” in *Advances in Cryptology: Proceedings*

of CRYPTO '85, Lecture Notes in Computer Science 218（Berlin, Heidelberg: Springer, 1985）, 417-426., https://doi.org/10.1007/3-540-39799-X_31.
25）Arjen K. Lenstra and Hendrik W. Lenstra, eds., *The Development of the Number Field Sieve*, Lecture Notes in Mathematics 1554（Berlin, Heidelberg: Springer, 1993）., https://doi.org/10.1007/BFb0091534.
26）John M. Pollard, "A monte carlo method for factorization," *BIT Numerical Mathematics* 15（1975）：331-334., https://doi.org/10.1007/BF01933667.
27）Peter W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Journal on Computing* 26, no.5（1997）：1484-1509., https://doi.org/10.1137/S0097539795293172.
28）Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen, eds., *Post-Quantum Cryptography*（Berlin, Heidelberg: Springer, 2009）., https://doi.org/10.1007/978-3-540-88702-7.
29）Peter W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Physical Review A* 52, no. 4（1995）：R2493-R2496., https://doi.org/10.1103/PhysRevA.52.R2493.
30）A. Robert Calderbank, et al., "Quantum error correction via codes over GF（4）," *IEEE Transactions on Information Theory* 44, no. 4（1998）：1369-1387., https://doi.org/10.1109/18.681315.
31）Hermann Weyl, *The Theory of Groups and Quantum Mechanics*（Dover Publications Inc., 1950）.
［Translation from the second German ed., 1931］.
32）Julian Schwinger, "Unitary Operator Bases," *PNAS* 46, no. 4（1960）：570-579., https://doi.org/10.1073/pnas.46.4.570.
33）Ran Raz and Avishay Tal, "Oracle separation of BQP and PH," in *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*（New York: Association for Computing Machinery, 2019）, 13-23., https://doi.org/10.1145/3313276.3316315.
34）Mitsuru Hamada, "A polynomial-time construction of self-orthogonal codes and applications to quantum error correction," in *2009 IEEE International Symposium on Information Theory*（IEEE, 2009）, 794-798., https://doi.org/10.1109/ISIT.2009.5205647.
35）https://cacm.acm.org/magazines/2021/11/256404-mip-re/fulltext
Zhengfeng Ji, et al., "MIP* = RE," *Communications of the ACM* 64, no. 11（2021）：131-138., https://doi.org/10.1145/3485628.
36）Maxim Kontsevich and Don Zagier, "Periods," in *Mathematics Unlimited-2001 and Beyond*, eds. Björn Engquist and Wilfried Schmid（Berlin, Heidelberg: Springer, 2001）, 771-808., https://doi.org/10.1007/978-3-642-56478-9_39.
37）International Mathematical Union, "International Congress of Mathematicians 2022," https://www.mathunion.org/icm/virtual-icm-2022,（2023年3月8日アクセス）.
38）Computing with Infinite Data（CID）, http://cid.uni-trier.de,（2023年3月8日アクセス）.
39）International Mathematical Union, "ICM Plenary and Invited Speakers," https://www.mathunion.org/icm-plenary-and-invited-speakers,（2023年3月8日アクセス）.