量子計算、量子アルゴリズムと有限群の表現論

Quantum computation, quantum algorithms and representation theory of finite groups

縫田　光司 (NUIDA, Koji)
産業技術総合研究所 (AIST)　情報セキュリティ研究センター (RCIS)

Abstract. "Quantum computation" is a notion for computation based on quantum mechanical phenomena. Recently, quantum computation and "quantum algorithms" (algorithms for quantum computation) are studied very actively, with deep connections to computer science, information theory, cryptography, etc. In one of the main research subjects on quantum algorithms, problem formulations and standard ways of approach are closely related to finite groups and their representation theory, such as certain asymptotic properties of irreducible characters of symmetric groups. This talk aims at giving a brief overview of the theory of quantum algorithms and their connection to representation theory.

1　導入

「量子計算」とは、Turing 機械に代表される従来の計算モデルと根本的に異なり、量子力学的な物理現象の性質に基盤を置く新しい計算モデルである。（量子計算と対比する意味で、従来の計算原理はしばしば「古典計算」と称される。）状態の重ね合わせの原理や量子もつれ状態の存在など、古典計算には現れない量子力学に顕著な性質を利用することで、少なくともある種の問題については古典計算を遥かに凌ぐ効率的な計算が可能となることが期待されており、またいくつかの問題については実際にそれが証明されている。同じく量子力学的現象に基礎を置く情報理論である「量子情報理論」と並んで、量子計算は現在の計算機科学分野における一つの重要な研究テーマとなっている。

量子計算を含む量子情報理論に関する標準的教科書（の邦訳）[1] の記述を基に、量子計算の歴史について簡単に触れておく。Feynman は 1982 年に、量子力学系をシミュレートする問題の困難性に関連し、量子力学の原理に基づく計算機を構築することの有用性を示唆した。Deutsch は 1985 年に、計算理論における基本的な哲学である Church-Turing の提唱[1]もしくはその改良版を理論的に導出するという大目標への一歩として、量子力学的現象に立脚した計算機（今日で言うところの量子計算機）の理論モデルを考案した。これらの出来事が、その後の量子計算に関する活発な研究の幕開けとなったものと考えられる。量子計算に関する研究成果のうち恐らく一般的に最も有名なものは、1994 年に Shor が提案した素因数分解を行う**多項式時間**量子アルゴリズム [2] であろう。古典計算による巨大な自然数の素因数分解については現在に至るまで効率的な（より正確には、入力サイズの多項式時間の）アルゴリズムは知られておらず、素因数分解の困難

[1]「いかなる計算過程も Turing 機械によってシミュレート可能であろう」という主張のこと

性は RSA 暗号 [3] をはじめ現在実用に供されている多くの暗号システムの安全性の根拠とされている。Shor の結果は、標語的に言えば「量子計算機が作られれば RSA 暗号が破られる」ことを意味するため、当時の暗号および情報セキュリティ分野に与えた衝撃が極めて大きかったであろうことは想像に難くない。事実、現在の暗号分野においては、量子計算機が実現した後も安全な（“post-quantum” な）暗号システムが一大研究テーマとなっている[2]。このように量子計算の概念は、理論的興味のみならず実学的な観点からも注目を集めている。

しかしながら、量子力学的現象という非常に繊細な現象に立脚した量子計算機を現実に構築するには技術的な困難さと多大なコストが壁となるため、量子アルゴリズムに対しては通常、何らかの意味で古典計算を本質的に上回る性能が要求される（そうでなければ従来の計算機をそのまま使えばよい）。それに加え、分野自体の歴史の浅さと量子力学の直感的理解の困難さも相まって、現在までに有効な量子アルゴリズムの構築に成功している問題の種類はまだ少数に留まっている。その数少ない成功例の一つが、上述の Shor によるアプローチを参考に素因数分解問題[3]を一般化した「隠れ部分群問題」に対する多項式時間量子アルゴリズムの構成である。隠れ部分群問題は（有限）群とその部分群に関するある種の決定問題であり、基礎となる群が可換群 [4] や Weyl-Heisenberg 群 [5] などいくつかの群の場合には多項式時間アルゴリズムが知られているものの、応用上も有用な他の群、例えば対称群や二面体群の場合には未だ多項式時間アルゴリズムは得られていない。実際のところ、隠れ部分群問題に関する既存の（話者の知る限り）全ての効率的アルゴリズムは本質的に Shor の手法の一般化である。その標準的手法は群上の離散 Fourier 変換の量子計算による実装に基づき、群上の離散 Fourier 変換は表現論的な記述を持つことから、隠れ部分群問題の定式化やその研究においては有限群およびその表現論が随所に登場している。一方、対称群上の隠れ部分群問題の効率的アルゴリズムについてはある種の（部分的な）不可能性定理が得られている [6, 7] が、その証明においても対称群の既約表現のある種の性質が決め手となっている。このように現在の量子計算および量子アルゴリズムの研究には有限群とその表現論が密接に関わっている。本発表では量子計算の基礎的事項について簡単に解説した上で、有限群の表現論との関連について紹介を試みる。

2　量子計算のための量子力学

本節では、本発表で量子計算の紹介をするのに必要な範囲で量子力学の基礎的事項を整理する。とはいえ、話者自身も実際のところ量子力学自体をきちんと理解しているわけではなく、量子計算に必要な範囲で公理化された数学的事項をただ利用しているだけである。そのような読者でも（日本語で）読める教科書として、上述の [1] やより近刊の [8] を参考書として挙げておく。

なお、本稿では量子系として有限次元のものだけを考えるため、量子系の記述に用いられる Hilbert 空間 $\mathcal{H}$ は単なる有限次元複素ベクトル空間 $\mathbb{C}^n$ とすれば充分である。

2.1　Dirac の記法

量子力学の定式化に用いられる所謂 Dirac の記法については数学者の視点では少々もやもやする点も感じられるが、利便性のためここで導入しておく。ケットベクトル (ket vector) $|0\rangle, |1\rangle, \ldots$

[2] RSA 暗号以外の現在中心的な暗号システムとして「楕円曲線暗号」をご存知の方もおられると思うが、楕円曲線暗号の安全性基盤は有限巡回群上の「離散対数 (discrete logarithm) 問題」の困難性にあり、一方 Shor の結果によって素因数分解とともに有限巡回群上の離散対数問題に対する多項式時間量子アルゴリズムも与えられている。そのため楕円曲線暗号を用いても問題の本質的解決にはならない。

[3] より正確には、4 節で述べるように、素因数分解のある部分問題

や $|\varphi\rangle, |\psi\rangle, \ldots$ は $\mathcal{H} = \mathbb{C}^n$ の列ベクトル ${}^t(x_1, \ldots, x_n)$ を表わす。ここでケット記号 $|\ \rangle$ の中身はベクトルの名前（添字）であり、$|0\rangle$ が必ずしも $\mathcal{H}$ の零元を表わすわけではないことに注意されたい。一方、ブラベクトル (bra vector) $\langle\varphi|$ はケットベクトル $|\varphi\rangle$ の転置共役 $|\varphi\rangle^\dagger = \overline{{}^t|\varphi\rangle}$ を表わす。従って $\langle\varphi|$ は行ベクトルである。ブラベクトル、ケットベクトルと行列の積が現れた際には常にそれらの行数や列数に関する整合性が取れているものと仮定する。以上の約束により、例えば $\langle\varphi|\varphi\rangle$（これは $\langle\varphi||\varphi\rangle$ の略記）はベクトル $|\varphi\rangle$ のノルムの自乗を表わし、また $|\varphi\rangle$ が正規化された（つまりノルム 1 の）ベクトルのとき、$|\varphi\rangle\langle\varphi|$ は $|\varphi\rangle$ の張る 1 次元空間への射影作用素を表わす。

2.2 純粋状態と混合状態

ある（有限次元）量子系 $\mathcal{Q}$ における一つの「純粋状態」は、$\mathcal{Q}$ に対応する空間 $\mathcal{H}$ のある正規化されたベクトル $|\varphi\rangle$ で記述される。$|\varphi\rangle$ とそのスカラー倍 $\alpha|\varphi\rangle$ ($\alpha \in \mathbb{C}, |\alpha| = 1$) が表わす状態は、それらを物理的に区別する手段が無いであろうとの理由から通常同一視される。一方、より一般の状態である「混合状態」は、$\mathcal{H}$ 上のトレース 1 の半正値 Hermite 作用素 ρ（「密度作用素」と呼ばれる）で記述される。密度作用素による記述では、純粋状態 $|\varphi\rangle$ は射影作用素 $|\varphi\rangle\langle\varphi|$ によって表わされる。ρ の固有値分解 $\rho = \sum_j \lambda_j |j\rangle\langle j|$ の存在は、任意の状態 ρ が純粋状態 $|j\rangle$ たちの重み λ_j での確率的重ね合わせにより実現されることを意味する。

2.3 状態の時間発展

閉じた量子系の時間発展は $\mathcal{H}$ 上の unitary 作用素を用いて記述される。具体的には、状態 ρ が ρ' へ時間発展した場合、時間発展を表わす unitary 作用素 U によって $\rho' = U\rho U^\dagger$ と表わされる。特に、閉じた量子系の時間発展は可逆である。

2.4 状態の測定

量子力学においては状態の「測定」という操作が重要な役割を果たす。本稿では測定結果の種類が有限個である場合のみを扱う。この場合、ある一つの測定操作は「測定オペレータ」の集合 $\{M_m\}_m$（添字 m は取り得る測定結果を動く）で記述される。各 M_m は $\mathcal{H}$ 上の作用素で $\sum_m M_m^\dagger M_m = I$ を満たすものであり、状態 ρ に対してこの測定を行ったとき結果 m が得られる確率は

$$p(m) = \mathrm{tr}(M_m \rho M_m^\dagger) = \mathrm{tr}(M_m^\dagger M_m \rho)$$

で与えられる（特に、量子力学における測定結果は一般には確率的にしか定まらない）。また、量子力学における測定の持つもう一つの顕著な特徴は、一般に測定前の状態と測定後の状態が異なることである（測定による状態の収縮などと呼ばれる）。上記の測定によって測定結果 m を得たとき、測定後の状態 $\rho^{\langle m\rangle}$ は

$$\rho^{\langle m\rangle} = \frac{M_m \rho M_m^\dagger}{\mathrm{tr}(M_m \rho M_m^\dagger)} = \frac{M_m \rho M_m^\dagger}{p(m)}$$

で与えられる。

後の節でも現れる具体的な測定の例を与える。$|0\rangle, |1\rangle, \ldots, |n-1\rangle$ を $\mathcal{H}$ の正規直交基底、$\mathcal{I}_1 \sqcup \cdots \sqcup \mathcal{I}_k$ を $[n-1] = \{0, 1, \ldots, n-1\}$ の分割とし、$m \in [n-1]$ について $M_m = \sum_{j \in \mathcal{I}_m} |j\rangle\langle j|$ とおくと $\{M_m\}_m$ は一つの測定を定める。このとき $M_m^\dagger M_m = M_m$ であるので、状態 ρ に対して

$$p(m) = \mathrm{tr}(M_m \rho) = \sum_{j \in \mathcal{I}_m} \mathrm{tr}(|j\rangle\langle j|\rho) = \sum_{j \in \mathcal{I}_m} \langle j|\rho|j\rangle$$

$$\rho^{\langle m \rangle} = \frac{\sum_{j,k \in \mathcal{I}_m} |j\rangle\langle j|\rho|k\rangle\langle k|}{p(m)} = \sum_{j,k \in \mathcal{I}_m} \frac{\langle j|\rho|k\rangle}{p(m)} |j\rangle\langle k|$$

である。特に、ρ が純粋状態 $\rho = |\varphi\rangle\langle\varphi|$（ただし $|\varphi\rangle = \sum_{j=0}^{n-1} \alpha_j |j\rangle \in \mathcal{H}$）のとき、

$$p(m) = \sum_{j \in \mathcal{I}_m} \langle j|\varphi\rangle\langle\varphi|j\rangle = \sum_{j \in \mathcal{I}_m} |\langle j|\varphi\rangle|^2 = \sum_{j \in \mathcal{I}_m} |\alpha_j|^2$$

$$\rho^{\langle m \rangle} = \frac{\sum_{j,k \in \mathcal{I}_m} \langle j|\varphi\rangle\langle\varphi|k\rangle \cdot |j\rangle\langle j|}{p(m)} = \sum_{j_0, k_0 \in \mathcal{I}_m} \frac{\alpha_{j_0} \overline{\alpha_{k_0}}}{\sum_{j \in \mathcal{I}_m} |\alpha_j|^2} |j_0\rangle\langle k_0|$$

となる。

2.5　合成系と状態の縮約

空間 $\mathcal{H}_A$ と $\mathcal{H}_B$ に対応する量子系 $\mathcal{Q}_A$ と $\mathcal{Q}_B$ が与えられたとき、それらの「合成系」$\mathcal{Q}_A \otimes \mathcal{Q}_B$ をテンソル積 $\mathcal{H}_A \otimes \mathcal{H}_B$ に対応する量子系として定義する。各々の量子系が互いに相関の無い状態 ρ_A と ρ_B を持つ場合、合成系における対応する状態は $\rho_A \otimes \rho_B$ と記述される（この形で表わされる合成系の状態を separable と呼ぶ）。

逆に、合成系 $\mathcal{Q}_A \otimes \mathcal{Q}_B$ の状態 ρ が与えられたとき、ρ を一方の系 $\mathcal{Q}_B$ に制限した状態というものを考える。この操作を部分系 $\mathcal{Q}_B$ への状態の「縮約」と呼び、状態の縮約を与える写像 $\mathrm{tr}_A : \mathcal{Q}_A \otimes \mathcal{Q}_B \to \mathcal{Q}_B$（「部分トレース」と呼ばれる）は以下の性質を持つ線型写像

$$\mathrm{tr}_A(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) = \mathrm{tr}(|a_1\rangle\langle a_2|) \cdot |b_1\rangle\langle b_2| = \langle a_2|a_1\rangle \cdot |b_1\rangle\langle b_2|$$

として記述される。特に separable な状態 $\rho = \rho_A \otimes \rho_B$ について $\mathrm{tr}_A(\rho) = \mathrm{tr}(\rho_A)\rho_B = \rho_B$ となる。以上は三つ以上の量子系の合成系に対しても同様に定義される。

3　量子計算

以上の準備の下、本節では量子計算の手短な導入を行う。現在の一般的な量子アルゴリズムの研究は、古典計算における（Turing 機械ではなく）回路モデルを念頭に置いたモデルに基づいている[4]。計算の舞台は、固定された正規直交基底（「古典基底」ないし「計算基底」と呼ばれる）$|0\rangle, |1\rangle, \ldots, |N-1\rangle$ を持つ空間 $\mathcal{H}$ に対応する量子系 $\mathcal{Q}$、もしくはそれらの合成系 $\mathcal{Q}_1 \otimes \cdots \otimes \mathcal{Q}_k$ である。各々の系 $\mathcal{Q}_j$ の状態が、古典計算における bit や digit の役割を果たすとも考えられるが、量子計算において現れる状態は separable なものだけではないため、全体の状態が古典計算における「bit 列」と単純に対応するとは限らないことに注意されたい。

[4]「量子 Turing 機械」も定義され盛んに研究されているようであるが、本稿ではそれには触れない。

量子計算の 1 回のサイクルは、適当な始状態 ρ_{input} に対して適当な unitary 作用素 U を作用させ（時間発展）、得られた状態 $\rho = U\rho_{\text{input}}U^\dagger$ に適当な測定 $\{M_m\}_m$ を行って測定結果 m と状態 $\rho^{\langle m\rangle}$ を得て、さらに $\rho^{\langle m\rangle}$ に対して適当な時間発展と測定を施し、…といった具合に進行する。量子力学における測定の結果は確率的であるため、一般には上記のサイクルを充分な回数繰り返し、得られた測定結果に対して（古典計算で）事後計算を行って最終的な計算結果を得ることが多い[5]。

ここで、量子アルゴリズムの「効率」を議論するためには、量子アルゴリズムにおいて許される始状態、unitary 作用素、測定の種類を定めておく必要がある（そうでなければ、極端な話全ての計算が 1 ステップで実行可能となってしまい、「効率」が意味をなさなくなってしまう）。通常、計算基底の要素のテンソル積、もしくはそれから効率的に構成できることがわかっている状態を始状態として用いる。unitary 作用素としては、二つの計算基底で張られる部分系（「量子ビット」などと呼ばれる）へ作用する三つの作用素「Hadamard ゲート」$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$、「位相ゲート」$S = \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}$、「$\pi/8$ ゲート」$T = \begin{pmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{pmatrix}$ と、2 量子ビットの合成系へ $|a\rangle\otimes|b\rangle \mapsto |a\rangle\otimes|a\oplus b\rangle$ $(a, b \in \{0, 1\}$、ここで排他的論理和 $\oplus$ は 2 を法とする和を表わす）で作用する「制御 NOT ゲート」からなる集合が量子計算における基本ゲート集合の一つと看做されている。（任意の unitary 作用素はこれらの基本ゲートの組合せで近似できることが知られている。）また測定としては、2.4 節で例示した計算基底の分割に対応する測定を考える（他の測定は unitary 変換とこの測定の組合せで実現できる）。なお、任意の効率的（多項式時間）古典アルゴリズムは効率的な量子アルゴリズムにより実現できる[6]ため、多項式サイズの実行時間の差を気にしない計算量理論の流儀に従う限りにおいては、量子アルゴリズムの構成の際に（効率的な）古典アルゴリズムを自由に活用してよいことを注意しておきたい。

本節の最後に、計算理論における「オラクル」という概念を紹介しておく。オラクルとは、ブラックボックスもしくはサブルーチンと似たようなもので、中の構造は窺い知れないものの入力に対してある（既知の）規則に基づき出力を返してくれる存在である。オラクル $\mathcal{O}$ が与えられた計算モデルにおいては、話者の知る限り、$\mathcal{O}$ の実行時間を 1 ステップ（計算時間の最小単位）と規定することが多い。このような概念は奇異に感じられるかもしれないが、「ある問題が簡単であるという仮定の下で別のある問題がどれだけ難しいか」を論じる際に役立つ概念であり、計算量理論や暗号理論において頻繁に用いられる[7]重要な概念である。古典計算のみならず量子計算においてもこのようなオラクルを含むモデルを考えることができる。後の節で紹介する「隠れ部分群問題」の定式化には、このオラクルの概念が本質的に関係している。

4 Shor のアルゴリズム

本稿の冒頭で述べた通り、Shor が 1994 年に発表した素因数分解に対する多項式時間量子アルゴリズムの発見は、量子計算にまつわる現時点で最も有名な研究成果と言えるであろう。しかし、

[5] すぐ後に述べるように量子計算では古典計算を効率的にシミュレートできるため、原理的には事後計算の過程も量子計算として記述可能である。

[6] 量子計算の基本ゲートは全て可逆だが、適当な「補助量子ビット」を導入することで、非可換な古典アルゴリズムをシミュレートすることが可能となる

[7] 暗号理論分野における暗号の安全性証明は、多くの場合「ある問題 P（例えば素因数分解）が難しい」という前提の下で与えられる。標準的な安全性証明の手続きを大雑把に説明すると、「ある暗号システムを破れる（仮想的な）攻撃者」としてオラクル $\mathcal{O}$ を定義し、$\mathcal{O}$ が与えられた状態で問題 P に対する効率的なアルゴリズムを構成する。すると問題 P が難しいという元々の前提に矛盾するため、背理法によりそのような攻撃者が存在しない、即ち件の暗号システムが安全であることが証明される、という具合である。

Shor のアルゴリズムのうち**量子アルゴリズムとして**本質的な部分は素因数分解そのものではなく、ある（未知の素因数を持つ）N に対する群 $(\mathbb{Z}/N\mathbb{Z})^*$ において任意の元の位数を求める問題に対するアルゴリズムである。実際、この位数計算問題に対する効率的量子アルゴリズムと追加の古典計算を組み合わせることで以下の通り素因数分解の効率的アルゴリズムが得られる。素因数分解は非自明な因数を見つける問題に帰着されるため、因数発見問題に対するアルゴリズム（[1] の 5.3.2 節を参照）を記しておく。（入力が偶数の場合は簡単なため、入力は奇数と仮定する。）

入力： 奇数 $N > 1$

出力： N の非自明な因数、または「N は素数」という結果

1. N が正整数の整数べき a^b、$b \geq 2$ の形に書けるならば a を出力して終了

2. 1 から $N-1$ までの x を一様ランダムに選び、$\gcd(x, N) > 1$ ならばその数を出力して終了

3. **位数計算アルゴリズム** を用いて、$x^r \equiv 1 \pmod{N}$ となる最小の $r > 0$ を計算

4. r が偶数で $x^{r/2} \not\equiv -1 \pmod{N}$、かつ $\gcd(x^{r/2} - 1, N)$ または $\gcd(x^{r/2} + 1, N)$ のいずれかが N の非自明な因数であればその因数を出力して終了

5. 手順 2. から 4. までを充分な回数（詳細は省略）繰り返す

6. 「N は素数」と出力して終了

図 1 は Shor の位数計算アルゴリズムの回路図の概略を表わす（回路図は左から右へ読む）。このアルゴリズムの入力は正整数 N と $\gcd(x, N) = 1$ なる整数 $1 \leq x \leq N-1$ である。ρ^{uni} は N 次元空間 $\mathcal{H}_1$ 上のベクトル $\sqrt{N}^{-1} \sum_{j=0}^{N-1} |j\rangle_1$ に対応する状態である（$|j\rangle_k$ は k 番目の空間 $\mathcal{H}_k$ の計算基底の要素を表わす）。まず合成系 $\mathcal{Q} = \mathcal{Q}_1 \otimes \mathcal{Q}_2$ 上の状態 $\rho^{\mathrm{uni}} \otimes |1\rangle\langle 1|$ を準備し、x に応じて定まるある（合成系上の）unitary 変換 U_x を施す。その結果の部分系 $\mathcal{Q}_1$ の部分に離散 Fourier 変換 FT（後述）の逆変換を施した上で、$\mathcal{H}_1$ の基底に対応する測定 $\mathcal{M} = \{M_m\}_m$（2.4 節参照）を行う。（以降では部分系 $\mathcal{Q}_2$ は使わないので $\mathcal{Q}_1$ へ縮約した状態（2.5 節参照）で考えてよい。）この測定結果を基にある古典計算 C を行い、最終的な結果を得る。

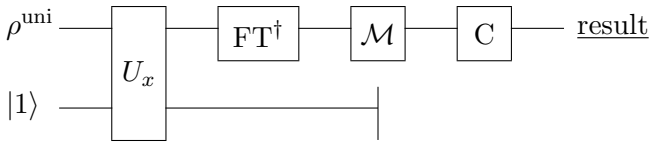

図 1: 位数計算アルゴリズムの回路図（概略）

U_x や C の詳細な構造は本稿では本質的でないので割愛するが、重要なのは「離散 Fourier 変換（の逆変換）を施してから基底による測定を行う」という一連の流れである。後の一般化もこの特徴に着目する形でなされている。ここで N 次元空間 $\mathcal{H} = \bigoplus_{j=0}^{N-1} \mathbb{C}|j\rangle$ 上の離散 Fourier 変換 FT は

$$\mathrm{FT} : \sum_{j=0}^{N-1} x_j |j\rangle \mapsto \sum_{k=0}^{N-1} y_k |k\rangle \,,\; y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i jk/N} \tag{1}$$

で定められる（通常の離散 Fourier 変換の量子計算による実装）。Shor のアルゴリズムの詳細については、例えば [1] の 5 章を参照されたい。

5　隠れ部分群問題

さて、やや天下り的ながら、ここで本稿の主題である「隠れ部分群問題」の定式化を与えることにしよう。この問題がどのように Shor の考えた問題と結び付くかについては後述する。

G を有限群、$\mathcal{C}_1, \ldots, \mathcal{C}_c$ を G の部分群からなる互いに排反な族とする。今、これらの族のいずれかのある要素 $H \leq G$ と、有限集合 X、さらに以下の条件

$$g_1, g_2 \in G\,,\ f(g_1) = f(g_2) \Leftrightarrow g_1 H = g_2 H$$

を満たす写像 $f : G \to X$ が与えられているものとする。つまり f は、G の元が互いに H による同じ剰余類に属するかどうかを判定する写像である。この状況で H が $\mathcal{C}_1, \ldots, \mathcal{C}_c$ のどの族に属する部分群であるか判定せよ、という問題が**隠れ部分群問題** (Hidden Subgroup Problem, HSP) である。

この問題を量子計算の枠組みで扱うために、G の元と対応付けられた基底 $\{|g\rangle = |g\rangle_G\}_{g\in G}$ を持つ空間 $\mathcal{H}_G$ と、X の元と対応付けられた基底 $\{|x\rangle = |x\rangle_X\}_{x\in X}$ を持つ空間 $\mathcal{H}_X$ を準備し、以下の性質を持つオラクル U_f を考える：U_f は $\mathcal{H} = \mathcal{H}_G \otimes \mathcal{H}_X$ 上の unitary 変換であり、ある固定した $x_0 \in X$ について

$$U_f(|g\rangle \otimes |x_0\rangle) = |g\rangle \otimes |f(g)\rangle\,,\ g \in G$$

（つまり、U_f は写像 f を計算してくれるオラクルである）。このオラクルを用いて H がどの族の要素か判定せよ、という形で量子計算としての隠れ部分群問題が定式化される。

隠れ部分群問題には、量子情報理論や純粋数学としての興味だけでなく、計算機科学におけるいくつかの重要な問題との関連というより応用的な動機も存在する。前述の通り、素因数分解問題は整数剰余環の乗法群における位数計算問題に帰着される。1 節の注釈で触れた「離散対数問題」とは、抽象群としては有限巡回群 C_N と同型である群 G とその生成元 g、任意の元 h が与えられたとき、$h = g^r$ となる整数 r を求める問題である[8]。“κ-unique SVP”（SVP は “Shortest Vector Problem” の略、日本語では「最短ベクトル問題」）とは、$\mathbb{R}^N$ の格子 Λ が条件「Λ 上の最短な非零ベクトルの長さが、その次に短い非零ベクトル[9]の長さの κ^{-1} 以下である」を満たすという前提で、Λ 上の最短な非零ベクトルを求める問題である。離散対数問題と κ-unique SVP はともに暗号分野において非常に重要な問題である。また「グラフ同型問題」とは、二つの有限グラフが与えられたとき、それらが互いに同型であるかどうかを判定する問題である。この問題は計算量理論の分野において、計算量クラス P と NP の「間」に属すると信じられている代表的な問題である。以上の問題は全て応用上も重要な問題であり、古典計算の範囲では多項式時間アルゴリズムが知られていない（し、存在しないと信じられている）が、これらの問題は全て量子計算の範囲ではある特別な群における隠れ部分群問題に帰着されることが知られている（表 1）。（具体的な帰着方法を含め、隠れ部分群問題の詳細については、数年前の論文であるが優れた概説論文 [9] があるのでそちらを参照されたい。）以上のような事情もあり、現在の量子アルゴリズム分野において隠れ部分群問題は特に重要な問題と認識されている。

隠れ部分群問題に関する肯定的な結果としては、Shor の結果を包含する形で、G が有限可換群の場合に Kitaev [4] が多項式時間アルゴリズムを与えた。Kuperberg [10] は、G が二面体群 D_N の場合に準指数時間アルゴリズムを与えた。これは多項式時間ではないが、この場合に対応する κ-unique SVP が非常に難しい問題であるため、充分優れた結果と考えられている模様である。ま

[8] 離散対数問題の困難さは G の抽象群としての構造以外にその表示のされ方に大きく依存する。例えば G が加法群 $\mathbb{Z}/N\mathbb{Z}$ であれば自明な問題となるが、一方 G が有限体上の楕円曲線群である場合には一般に離散対数問題は困難な問題である（と信じられている）。

[9] 前者と平行なベクトルを除いて

表 1: 隠れ部分群問題に帰着できる他の問題

問題	群 G	部分群 H	現状
素因数分解 （位数計算問題）	$(\mathbb{Z}/N\mathbb{Z})^*$	$\mathcal{C}_k = \{C_k \leq G\}$ $(1 \leq k \leq \lvert G\rvert)$	多項式時間 (Shor [2])
離散対数問題	$(\mathbb{Z}/N\mathbb{Z})^2$	$H = \langle (l, -ls) \rangle$ $(l, s \in \mathbb{Z}/N\mathbb{Z})$	多項式時間 (Shor [2])
（参考）	有限可換群	任意	多項式時間 (Kitaev [4])
κ-unique SVP	D_N	$H = \langle r \rangle$ （$r \in G$ は鏡映）	準指数時間 (Kuperberg [10])
グラフ同型問題	S_{2n}	$\mathcal{C}_1 = \{1\}$ $\mathcal{C}_2 = \{\langle\sigma\rangle \mid \sigma; \text{cycle type } (2^n)\}$	未解決
	$S_n \operatorname{wr} S_2$	$\mathcal{C}_1 = \{1\}$ $\mathcal{C}_2 = \{\langle((\sigma, \sigma^{-1}), \tau)\rangle \mid \sigma \in S_n, \tau \neq 1\}$	未解決

た、表 1 に含まれていないいくつかの群についても多項式時間アルゴリズムが与えられている（例えば Weyl-Heisenberg 群の場合には Krovi & Rötteler [5]）。

一方、表 1 にも含まれる重要な場合である G が対称群 S_{2n}（もしくは対称群の wreath 積 $S_n \operatorname{wr} S_2$）の場合には、目覚しい肯定的結果がほぼ何も得られていない状況である。そのため G がこれらの群である場合が、現在の隠れ部分群問題の研究における主要な未解決問題となっている。

6 対称群上の隠れ部分群問題

本節では、上述した $G = S_{2n}$ もしくは $S_n \operatorname{wr} S_2$ の場合における隠れ部分群問題の研究状況と、対称群の表現論との関連を紹介する。

6.1 Strong Fourier Sampling

4 節で紹介した Shor のアルゴリズムの主要部分は、離散 Fourier 逆変換（を実現する unitary 変換）とそれに引き続く標準基底による測定であった。実のところ、より一般の隠れ部分群問題においても、既存のアルゴリズムは（話者の知る限り）全て同様の発想で構成されたものである。G が対称群の場合にも状況は同様なので、まずこの標準的手法（“Strong Fourier Sampling” などと呼ばれる）について述べておくことにする。

一時的に、G を任意の有限群とし、$\mathcal{H}$ を基底 $\{|g\rangle \mid g \in G\}$ を持つ複素ベクトル空間とする。つまり $\mathcal{H}$ は G の群環 $\mathbb{C}[G]$ と、また G 上の複素数値関数全体の集合と自然に同一視される。ここで $\mathbb{C}[G]$ は G の（非同値な）既約表現空間上の全行列環たちの直和に分解されるので、$\mathcal{H}$ は組 (λ, j, k)（$\lambda \in \widehat{G}$、$j, k \in \{1, 2, \ldots, d_\lambda\}$、ここで d_λ は既約表現 ρ_λ の次元）で parameterize される別の基底 $\{|\lambda, j, k\rangle\}$ を持つ。以上の状況で、写像 $\mathrm{FT} : \mathcal{H} \to \mathcal{H}$、

$$\mathrm{FT}(\sum_{g \in G} f(g)|g\rangle) = \sum_{\lambda \in \widehat{G}, 1 \leq j,k \leq d_\lambda} \sqrt{\frac{d_\lambda}{|G|}} \sum_{g \in G} f(g) \rho_\lambda(g)_{j,k} |\lambda, j, k\rangle \tag{2}$$

（ただし $\rho_\lambda(g)_{j,k}$ は行列 $\rho_\lambda(g)$ の j 行 k 列成分）は G 上の Fourier 変換に対応する unitary 変換となる[10]。また、その逆変換 $\mathrm{FT}^\dagger$ は

$$\mathrm{FT}^\dagger\Big(\sum_{\lambda\in\widetilde{G},1\le j,k\le d_\lambda} a_{\lambda,j,k}|\lambda,j,k\rangle\Big) = \frac{1}{\sqrt{|G|}}\sum_{g\in G}\sum_{\lambda\in\widehat{G}}\sqrt{d_\lambda}\mathrm{tr}(A_\lambda\rho_\lambda(g^{-1}))$$

（ただし A_λ は (j,k) 成分が $a_{\lambda,j,k}$ となる行列）で与えられる。G が加法群 $\mathbb{Z}/N\mathbb{Z}$ のときには (2) 式は (1) 式に一致することを確認されたい。

この状況で、G 上の隠れ部分群問題における Strong Fourier Sampling とは図 2 の回路図で表わされる手順を指す。ρ^{uni} は $\mathcal{H}_G = \bigoplus_{g\in G}\mathbb{C}|g\rangle$ 上のベクトル $\sqrt{|G|}^{-1}\sum_{g\in G}|g\rangle$ に対応する状態、x_0 は X の固定した元、U_f は 5 節で導入した写像 $f : G \to X$ を計算するオラクル、$\mathcal{M}$ は $\mathcal{H}_G$ の基底 $\{|\lambda,j,k\rangle\}_{\lambda,j,k}$ のある分割に対応する測定である。図 1 に示された位数計算問題の回路図との類似性に注意されたい。なお、位数計算問題の場合と異なり、一般の隠れ部分群問題の場合にはこの手順 1 回だけでは充分な情報が集まらないため、必要な情報が得られるまでこのサイクルを複数回繰り返すことになる。この手法で隠れ部分群問題の多項式時間アルゴリズムを得るには、サイクルの繰り返し回数が多項式回に収まり、かつ G 上の Fourier 逆変換 $\mathrm{FT}^\dagger$ と測定 $\mathcal{M}$ の準備（対応する分割の計算）と測定結果たちに施す事後計算の全てが多項式時間で行える必要があることに注意されたい[11]。

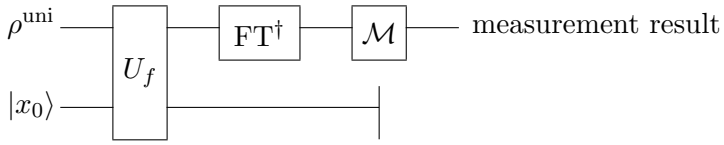

図 2: 隠れ部分群問題の標準的アルゴリズム（の 1 サイクル）

6.2 対称群上の隠れ部分群問題のある「不可能性定理」

6.1 節で紹介した標準的手法である Strong Fourier Sampling を用いることで、5 節で述べた通り色々な群上の隠れ部分群問題の多項式時間（もしくは準指数時間）アルゴリズムが得られている。一方、グラフ同型問題と関連する対称群上の隠れ部分群問題については、以下に紹介するような Strong Fourier Sampling のある種の「限界」が理論的に証明されている。

表 1 にあるように、$G = S_{2n}$ とし、部分群 H は自明な群であるか、または cycle type (2^n) を持つある置換 $\sigma \in S_{2n}$ で生成される位数 2 の群であるかのいずれかと仮定し、H が前者のタイプであるか後者のタイプであるかを判定できれば良いという状況を考える。Moore, Russell & Schulman は、このような制限された状況においても、Strong Fourier Sampling を用いたのでは多項式時間での H の識別が不可能であることを証明した [6]。本稿ではこの証明の中身にまで踏み込むことはしないが、証明においては対称群の既約表現の性質が随所に用いられているため、具体的にどのような性質が用いられているかを紹介しておく。なお、以下では $\widehat{S_n}$ 上の確率分布として Plancherel 分布を採用する。

[10] この unitary 変換は量子アルゴリズムの分野では「量子 Fourier 変換」(quantum Fourier transform) と呼ばれているが、いかにも表現論のどこかの用語と衝突していそうな用語なので本稿では用いないことにする。

[11] 「事後計算が多項式時間」という条件を外すと、(Fourier 変換を用いずに) 全ての有限群 G について U_f を多項式回用いれば隠れ部分群問題が解けることが知られている [11, 12]。

- ([13]) ある正の定数 c_1 と c_2 が存在して、$\lambda \in \widehat{S_n}$ とするとき

$$\lim_{n\to\infty} \Pr[e^{-c_1\sqrt{n}}\sqrt{n!} \le d_\lambda \le e^{-c_2\sqrt{n}}\sqrt{n!}] = 1 \ .$$

- ([13]) ある正の定数 c_1 と c_2 が存在して、全ての $n \ge 1$ について

$$e^{-c_1\sqrt{n}}\sqrt{n!} \le \max_{\lambda\in\widehat{S_n}} d_\lambda \le e^{-c_2\sqrt{n}}\sqrt{n!} \ .$$

- ([6, Lemma 6]) $\delta = \pi\sqrt{2/3}$ とおくと、充分大きい任意の n について

$$\Pr[d_\lambda \le e^{-\delta\sqrt{n}}\sqrt{n!}] < e^{-\delta\sqrt{n}} \ .$$

- ([6, Lemma 6]) 任意の $0 < c < 1/2$ について、$\Pr[d_\lambda \le n^{cn}] = n^{-\Omega(n)}$ が成り立つ[12]。

- ([14]) 以下を満たす定数 $b > 0$ と $0 < q < 1$ が存在する：任意の $n > 4$ と S_n の共役類 C、$\lambda \in \widehat{S_n}$ について

$$\left|\frac{\chi_\lambda(C)}{d_\lambda}\right| \le \left(\max\{q, \lambda_1/n, \lambda'_1/n\}\right)^{b\cdot\mathrm{supp}(C)}$$

が成り立つ。ただし λ' は Young 図形としての λ の転置、$\mathrm{supp}(C)$ はある $\sigma \in C$ についての集合 $\{1 \le k \le n \mid \sigma(k) \ne k\}$ のサイズ（σ の選び方に依らない）を表わす。

6.3 「不可能性定理」の一般化

6.2 節で紹介した「不可能性定理」の一般化として、Moore & Russell は状態 $\rho^{\mathrm{uni}} \otimes |x_0\rangle\langle x_0|$ の代わりに $\rho^{\mathrm{uni}} \otimes \rho^{\mathrm{uni}} \otimes |x_0\rangle\langle x_0|$ から出発し、$G = S_{2n}$ の代わりに直積群 G^2 上の Fourier 変換を用いて Strong Fourier Sampling を行う状況を考察した。そして、そのような拡張された状況においても、多項式時間では 2 種類の部分群 H を互いに識別できないことを証明した [7]。この拡張された状況の考察においては、直積群 G^2 の Fourier 変換を考えるため、群 G の既約表現のテンソル積を既約分解する、という表現論でお馴染みの問題が深く関連してくる。論文 [7] で新たに用いられた性質は以下のようなものである。

- ([7, Corollary 14]) $\lambda = (\lambda^{(1)}, \ldots, \lambda^{(k)})$ と $\mu = (\mu^{(1)}, \ldots, \mu^{(\ell)})$ をそれぞれ $\widehat{S_n}^k$ と $\widehat{S_n}^\ell$ のランダムな要素とし（直積集合上の確率分布は積分布で定める）、表現 $\rho_{\lambda,\mu}$ を

$$\rho_{\lambda,\mu} = \bigotimes_{j=1}^{k} \rho_{\lambda^{(j)}} \otimes \bigotimes_{h=1}^{\ell} (\rho_{\mu^{(h)}} \otimes {\rho_{\mu^{(h)}}}^*)$$

で定め、その指標を $\chi_{\lambda,\mu}$ と書く。このとき任意の $\nu \in \widehat{S_n}$ について、ρ_ν の $\rho_{\lambda,\mu}$ における重複度 $\langle\chi_\nu, \chi_{\lambda,\mu}\rangle_{S_n}$ は

$$\mathrm{Ex}\left[\frac{\langle\chi_\nu, \chi_{\lambda,\mu}\rangle_{S_n}}{\dim\rho_{\lambda,\mu}}\right] \le \begin{cases} d_\nu p(n)/n! & \text{if } k = 0 \text{ and } \ell = 1 \\ (1+o(1))d_\nu/n! & \text{otherwise} \end{cases}$$

を満たす[13]。ここで $p(n)$ は n 箱の Young 図形の総数である。

[12] ここで $\Omega(n)$ は、$n \to \infty$ のとき a_n/n がある正定数で下から押さえられるような量 a_n を表わす。
[13] ここで $o(1)$ は、$n \to \infty$ のとき $a_n \to 0$ となる（特に今の場合は正の）量 a_n を表わす。

さらに Moore, Russell & Śniady は、よりグラフ同型問題に近い問題である wreath 積 $G = S_n \operatorname{wr} S_2$ 上の隠れ部分群問題（表 1 を参照）を考察し、Strong Fourier Sampling の自然な一般化である “quantum sieve” という手法の範疇では多項式時間アルゴリズムが構成できないことを証明した [15]。ここで用いられたのが以下の性質である。

- ([16]) 任意の $D > 0$ について、以下を満たす定数 A' が存在する：$\lambda \in \widehat{S_n}$ が Young 図形としてそれぞれ高々 $D\sqrt{n}$ 個の行と列からなるとき、任意の $\sigma \in S_n$ について

$$\left|\frac{\chi_\lambda(\sigma)}{d_\lambda}\right| < \left(\frac{A' \max\{1, t(\sigma)^2/n\}}{\sqrt{n}}\right)^{t(\sigma)}$$

  が成り立つ。ただし $t(\sigma)$ は σ を（隣接とは限らない）互換の積で表示した際の最短の長さを表わす。

なお、この論文 [15] についての余談として、2006 年に arXiv で発表されたプレプリント版の初版では上の性質は「予想」として記されており、上述の「不可能性定理」も「この予想が正しければ」という条件付きの結果であった。当初は Moore と Russell 二人の共著だったのだが、その後Śniady が Rattan と共にこの「予想」を解決し [16]、最新版の論文では目出度く主定理が条件付きでなくなった（そしてŚniady が共著者に加わった）という経緯がある。[15] の結果は計算機科学分野では最高峰の国際会議の一つである STOC で発表できるほどの優れた結果であるが、その中では数学者であるŚniady が本質的な貢献を果たしていた、というわけである。同じ数学者として喜ばしいことではないだろうか。少なくとも私にとっては大いに元気付けられる出来事であった。

7　結び

本稿では、現在の情報科学分野の主要研究課題の一つである量子計算、更にその中心テーマの一つである隠れ部分群問題に焦点を当て、問題と歴史的背景およびその研究状況の概略を説明するとともに、その問題の定式化や現在までの主要な研究成果において有限群の表現論がいかに深く関わってきたかを紹介した。

隠れ部分群問題のうちグラフ同型問題と関連する場合については、対称群の既約表現の性質を用いることで、既存の標準的手法を用いたのでは効率的なアルゴリズムを構成できる見込みが無いことが明らかになったわけであるが、それ以外の手法を用いた場合の構成の可能性や、他の多くの群における隠れ部分群問題の効率的アルゴリズムについては未踏の領域が残されている。本文中で紹介した成果と同様に、これら未踏の領域においても表現論をはじめとする数学の力で何らかの本質的貢献が果たされることを期待する次第である。

謝辞　本発表の機会を与えて下さった 2009 年度表現論シンポジウム世話人の先生方に深く感謝申し上げたい。なお本研究は、文部科学省科学研究費補助金（科研費）若手研究（B）（No.20700017）による援助を受けている。

参考文献

[1] M. A. Nielsen, I. L. Chuang （木村達也 訳）, Quantum Computation and Quantum Information （量子コンピュータと量子通信）, オーム社 (2004)

[2] P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in: Proceedings of 35th Annual Symposium on Foundations of Computer Science (FOCS 1994), IEEE (1994)

[3] R. L. Rivest, A. Shamir, L. M. Adleman, A method of obtaining digital signatures and public-key cryptosystems, Comm. ACM 21(2) (1978) 120–126

[4] A. Y. Kitaev, Quantum measurements and the Abelian stabilizer problem, arXiv:quant-ph/9511026 (1995)

[5] H. Krovi, M. Rötteler, An efficient quantum algorithm for the Hidden Subgroup Problem over Weyl-Heisenberg groups, in: Proceedings of Mathematical Methods in Computer Science (MMICS 2008), Lecture Notes in Computer Science 5393, Springer (2008), pp.70–88

[6] C. Moore, A. Russell, L. J. Schulman, The symmetric group defies strong Fourier sampling: Part I, arXiv:quant-ph/0501056 (2005)

[7] C. Moore, A. Russell, The symmetric group defies strong Fourier sampling: Part II, arXiv:quant-ph/0501066 (2005)

[8] N. D. Mermin （木村元 訳）, Quantum Computer Science: An Introduction （マーミン 量子コンピュータ科学の基礎）, 丸善 (2009)

[9] C. Lomont, The Hidden Subgroup Problem - review and open problems, arXiv:quant-ph/0411037 (2004)

[10] G. Kuperberg, A subexponential-time quantum algorithm for the dihedral Hidden Subgroup Problem, SIAM J. Comput. 35(1) (2005) 170–188

[11] M. Ettinger, P. Høyer, E. Knill, Hidden subgroup states are almost orthogonal, arXiv:quant-ph/9901034 (1999)

[12] M. Ettinger, P. Høyer, E. Knill, The quantum query complexity of the hidden subgroup problem is polynomial, Information Processing Letters 91(1) (2004) 43–48

[13] A. M. Vershik, S. V. Kerov, Asymptotic behavior of the maximum and generic dimensions of irreducible representations of the symmetric group, Funk. Anal. i Prolizhen 19(1) (1985) 25–36. English translation in: Funct. Anal. Appl. 19 (1989) 21–31

[14] Y. Roichman, Upper bound on the characters of the symmetric groups, Invent. Math. 125 (1996) 451–485

[15] C. Moore, A. Russell, P. Śniady, On the impossibility of a quantum sieve algorithm for Graph Isomorphism, in: Proceedings of the thirty-ninth annual ACM Symposium on Theory of Computing (STOC'07), ACM, pp.536–545, 2007. arXiv:quant-ph/0612089v3

[16] A. Rattan, P. Śniady, Upper bound on the characters of the symmetric group for balanced Young diagrams and a generalized Frobenius formula, Adv. Math. 218(3) (2008) 673–695. arXiv:math.RT/0610540 (2006)