量子コンピュータの能力を引き出すアルゴリズムとその検証技術

量子コンピュータは，既存の計算原理に基づく計算機の延長線上では得られない超高速な計算を実現し，情報処理に革命を起こすと期待されています．このためには，量子ハードウェアとともに，その能力を引き出すための量子アルゴリズムが不可欠です．本稿では，量子アルゴリズムとそれを支える量子回路最適化技術，および，その実行の信頼性を高めるための検証技術に関する最近の成果について紹介します．

谷　誠一郎（たに　せいいちろう）
秋笛　清石（あきぶえ　せいせき）
竹内　勇貴（たけうち　ゆうき）
NTTコミュニケーション科学基礎研究所

中核技術としての量子アルゴリズム

現代社会で使用されているコンピュータと同様に，量子コンピュータにおいても，ハードウェア上で走らせるソフトウェア（計算手順＝アルゴリズム）の良し悪しが計算性能を大きく左右します．この意味で，量子アルゴリズムは，量子コンピュータの有用性を決定付ける中核技術といってよいでしょう．

古典問題を解く高速量子アルゴリズム

私たちの日常生活に密接に関係している問題のほとんどは，量子の概念とは一切関係のない問題（古典問題）です．もし，量子コンピュータを用いて，既存の計算原理に基づくコンピュータ（＝古典コンピュータ）よりも圧倒的に速く，古典問題を解くことができれば，私たちの生活・社会に大きなインパクトを与えられると期待されています．

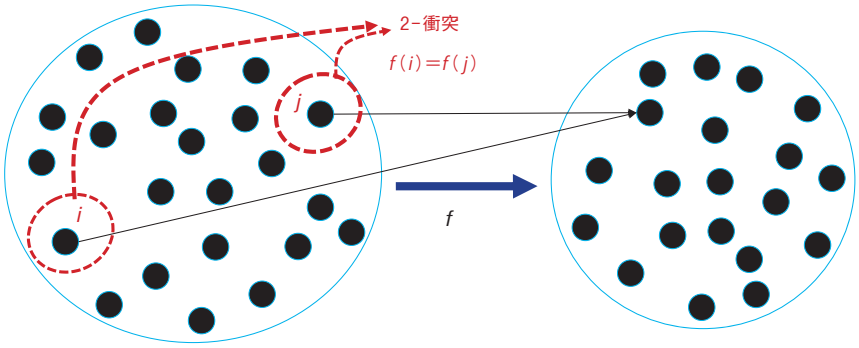
これまでの研究により，量子コンピュータを用いて計算を高速化できる古典問題が次々と明らかになってきました[(1)]．特に，衝突発見問題は，量子ウォークに代表される，さまざまな量子アルゴリズム技術を生み出す際に中心的な役割を演じました．ここで生み出されたアルゴリズム技術を基礎として，行列乗算など応用上重要な多くの古典問題に対する高速量子アルゴリズムが考案されました．以降では，衝突発見問題を例に，量子アルゴリズム技術を，少し異なる観点，すなわち，情報通信の安全性の観点から考えてみます．

高い計算能力を期待されている量子コンピュータは，良いことに使われるばかりでなく，「暗号を破る」という悪いことにも利用されるおそれがあります．このため，近年，量子コンピュータによる強力な攻撃を考慮した，暗号の安全性評価が求められています．この安全性評価を行うためには，攻撃者の攻撃能力を知る必要があり，したがって，具体的な攻撃手法を考える必要があります．量子コンピュータを用いた攻撃手法とは，量子アルゴリズムにほかなりません．

私たちは，これまで培ってきた量子アルゴリズムの基礎技術を基に，暗号の中核技術であるハッシュ関数に関して，量子コンピュータを用いた最高速攻撃手法を考案しました[(2)]．

ハッシュ関数とは，長いデータを入力として，短いデータを出力する関数です．ただし，暗号では，出力データから入力データの推測が難しいものが使われます．ハッシュ関数の応用範囲はとても広く，例えば，電子署名や公開鍵暗号など，私たちの生活に密着したものにも使われています．

では，ハッシュ関数に対する攻撃とは何か，ということを「衝突」という概念を用いて説明します．ハッシュ関数 f により同じ値に移される複数の要素を衝突と言います（**図1**）．一般に，ハッシュ関数 f により同じ値に移される ℓ 個の要素を ℓ-衝突と言います．また，ℓ を衝突の多重度と言います．例えば，図1の場合，2つの要素 i, j が f によって，同じ値に移されているので，(i, j) は衝突であるといえます．



要素のペア（i, j）が関数fにより同じ値に移されるとき（$f(i)=f(j)$），ペア（i, j）を2-衝突と言う．
同様に，fにより同じ値に移されるℓ個の要素をℓ-衝突と言う．（例えば，3-衝突の場合，$f(i)=f(j)=f(k)$）

図１　ハッシュ関数の衝突

1. 部分集合$I\subset[N]$をサンプルし，Iの像$f(I)$を計算（$[N]\equiv\{1,\cdots,N\}$）
2. Iの要素とともに2-衝突を構成する部分集合$J\subset[N]\setminus I$を量子探索し，像$f(J)$を計算
3. IおよびJの要素とともに3-衝突を構成する要素$k\in[N]\setminus(I\cup J)$を量子探索
4. 得られた3-衝突（i, j, k）を出力

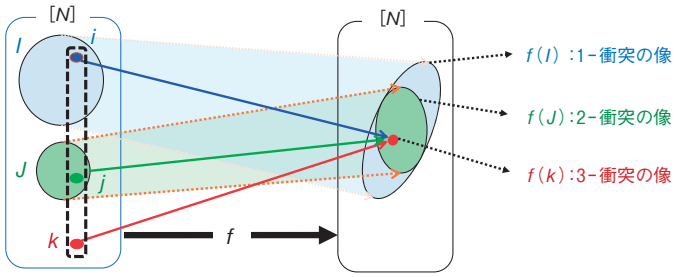


図２　量子アルゴリズムの動作（3-衝突発見問題の場合）

ℓ（多重度）	2	3	4	5	…	ℓ
既存手法［HSX17］	$N^{\frac{1}{3}}$	$N^{\frac{4}{9}}$	$N^{\frac{13}{27}}$	$N^{\frac{40}{81}}$	…	$N^{\frac{1}{2}\left(1-\frac{1}{3^{\ell}-1}\right)}$
提案アルゴリズム	$N^{\frac{1}{3}}$	$N^{\frac{3}{7}}$	$N^{\frac{7}{15}}$	$N^{\frac{15}{31}}$	…	$N^{\frac{1}{2}\left(1-\frac{1}{2^{\ell}-1}\right)}$

［HSX17］A. Hosoyamada, Y. Sasaki, and K. Xagawa. Quantum multicollision-finding algorithm. In Proceedings of the 23rd International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2017, Part II, pp.179-210, 2017.

図３　既存アルゴリズム［HSX17］との計算速度比較（各多重度（ℓ）に対する，ハッシュ値の総数（N）と多重衝突を発見するために要する時間の関係）

衝突を発見できると，例えば，同じ認証データを持つ別の文書に改ざんできてしまう可能性があります．このため，ハッシュ関数fを暗号に使うためには，衝突発見の困難性（＝膨大な時間を要するかどうか）を評価する必要があります．この評価のために，衝突を発見するアルゴリズムが必要となります．私たちは，任意の多重度ℓに対して，ℓ-衝突を発見する高速量子アルゴリズムを考案しました（**図２**）．提案アルゴリズムの計算速度は，すべての多重度において，理論限界を達成しており，これにより，ハッシュ関数を用いた暗号の，より正確な安全性評価が可能になると期待されます．

図３は，各多重度（ℓ）に対する，ハッシュ値の総数(N)と多重衝突を発見するために要する時間の関係を既存の手法と比較したものです．数学的には，Nは，ハッシュ関数の値域のサイズです．多重度２の場合の計算時間が両手法で同じ理由は，既存手法が理論限界を達成しているからです．多重度３以上では，すべての場合において，既存手法より高速になっています．

具体的な数値例を考えてみます．多重度$\ell=3$，ハッシュ値の総数Nが2000 bit値の場合，既存手法の計算時間に比べ，提案手法の計算時間は10億倍程度高速になっています．

量子アルゴリズムを高速に実行するには量子回路レベルでの最適化が必要です．次に量子回路の最適化技術に関する成果を紹介します．

量子回路のコンパイル技術

光子や電子など，どのような量子系についても，その状態の変化の様子はユニタリ行列で表現されます．それゆえに，量子アルゴリズムから量子コンピュータに送られる「命令」も本質的にはユニタリ行列のかたちで与えられます．例えば，素因数分解を効率的に解くことで知られるShorのアルゴリズムに登場する重要な命令として，量子フーリエ変換と呼ばれるユニタリ行列が挙げられます．ところが，雑音に弱いという量子系の特性から，それらのユニタリ行列（が表現する状態変化）を完全な精度で実現することはできません．そこで通常は，高精度に実現できる数種類のユニタリ行列（これらを基本ゲートと呼びます）を適切な順序で実行することで所望のユニタリ行列を実現します．したがって，(a)基本

ゲートの総数＝(b)命令数×(c)1命令分のユニタリ行列を実現するための基本ゲート数，という関係が成り立ちます．量子アルゴリズムの実行時間はおおむね(a)の基本ゲートの総数で見積もることができるので，総数を減らすための最適化手法が数多く提案されてきました．それらは大まかに，各々のアルゴリズムの構造を活かして(b)の命令数を削減する手法と，アルゴリズムの構造とは独立に(c)の基本ゲート数を削減する手法に分類することができます．ここで，アルゴリズム設計時に基本ゲートを1つの命令だとみなせば，後者の最適化は不要に思われるかもしれません．しかし，基本ゲートは量子コンピュータをどのような量子系で実装するかによって変わってくることと，個々の量子系に依存しない直感的な命令群でアルゴリズムを設計したいことを踏まえると，後者の最適化が必須となります．

(c)の最適化では，連続自由度を持つユニタリ行列を有限個の基本ゲートの列で厳密に実現するのは不可能なので，許容誤差内で近似的に実現できる基本ゲートの列を探索します（これをコンパイルと呼びます）．適切に選ばれた基本ゲートの十分長い列を用いれば，任意のユニタリ行列を任意の精度で実現できることが知られています．したがって，そのような基本ゲートの列のうち，与えられたユニタリ行列を許容誤差内で近似できるもっとも短いものを出力することが(c)の最適化の目標となります．多くの先行研究ではもっとも短い1つの基本ゲート列を探索する（これを決定的コンパイルと呼びます）ことを目標としていたのに対し，近年，確率的に基本ゲート列を実現する（これを確率的コンパイルと呼びます）ことで，ゲート列の長さを増やさずにユニタリ行列の近似誤差を改善できることが発見されました．これは，同じ許容誤差の下では確率的コンパイルを行うことで，従来の決定的コンパイルと比較してより短い基本ゲート列でユニタリ行列を近似できることを意味します（**図4**）．しかし，さまざまな関連研究がある一方，確率的コンパイルの限界能力は分かっていませんでした．

今回私たちは，確率的コンパイルが達成し得る近似誤差の理論限界を解明しました[3]．また，効率的に実行できる確率的コンパイルの手順も考案し，既存の確率的コンパイラと比較して，最小の近似誤差を達成できることを理論的に示しました．いくつかの具体的な例で計算したところ，この確率的コンパイラにより(c)の基本ゲート数を，決定的コンパイラの場合と比較して，50%程度削減できることも分かりました．確率的コンパイルを解析するための理論は，コンパイルにおいて実用的な価値があるだけでなく，今後，古典・量子ハイブリッド型の情報処理を探求していくうえで，幅広い応用が期待されています．

量子アルゴリズムの実行の信頼性を高めるためには，コンパイラで得られた量子回路が実際のデバイスでどの程度正確に実現されているかを検証する必要があります．

量子コンピュータの検証技術

量子コンピュータは，雑音等に起因するエラーが発生しやすいという性質があります．発生したエラーに対処するための代表的な2つの手法として，「量子エラー訂正・抑制」と「量子計算の検証」があります．これら2つの手法は，お互いの欠点を補い合う相補的な関係にあります．量子エラー訂正・抑制はエラーが発生した際に訂正または抑制できる代わりに，どのようなエラーがどの程度発生しているのかをある程度知っている必要があります．一方で，量子計算の検証はエラーが未知の場合でも適用可能ですが，エラーを訂正することはできず，量子コンピュータの計算結果にエラーが発生

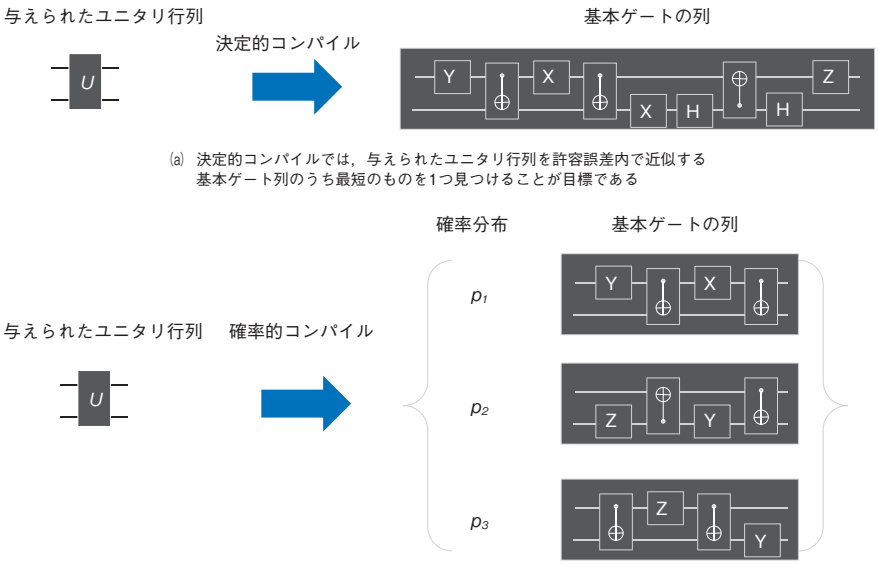


図4　確率的コンパイルによる基本ゲート数の削減

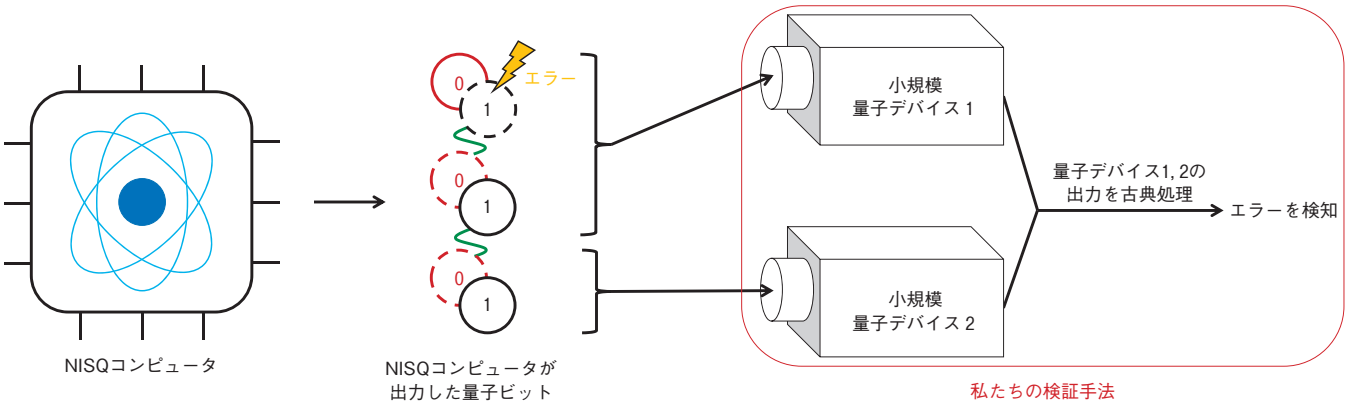


図 5　NISQ コンピュータを検証するための私たちの手法

しているかどうかを判断することしかできません．しかし，エラーの有無を判断できれば，エラーが発生していないときの計算結果だけを抽出することで正しい計算結果を知ることができるため，有用なエラー対処法になり得ます．特に，遠隔地の量子コンピュータに通信を介してアクセスするクラウド量子計算ではエラーが未知の場合が多いため，量子計算の検証が威力を発揮します．また，近年では，量子計算の検証を量子エラー抑制に応用するという研究も行われています．以降では，量子計算の検証に関する最近の私たちの成果について紹介します．

これまで，量子計算の検証を行うためのさまざまなプロトコルが提案されてきましたが，そのほぼすべてがエラー訂正可能な大規模量子コンピュータを想定したものでした．一方で，現在実現している，また今後数年間で実現すると予想されている量子コンピュータは NISQ（Noisy Intermediate-Scale Quantum）コンピュータと呼ばれており，エラー訂正を行う能力がありません．そこで，このギャップを埋めるため，私たちはNISQコンピュータ用の検証手法を構築するという研究に取り組みました(4)．単純な検証手法では，NISQコンピュータを検証するためには，それと同サイズの別の量子コンピュータが必要になってしまいます．ここでは，量子コンピュータのサイズは扱える量子ビット数を意味しています．この問題を解決するために，私たちは検証用の量子コンピュータを２つの小規模量子デバイスに分割するというアイデアを用いました（**図 5**）．その結果，NISQコンピュータを小規模量子デバイスで効率良く検証する新規な手法を提案することに成功しました．

今後の展開

本稿で紹介した技術は，さまざまなサイズの量子コンピュータに適用できるスケーラブルな技術です．これを可能にしているのは，私たちが得意とする数理科学的アプローチです．今後，量子コンピュータの開発が進むにしたがい，このようなスケーラブルな技術は，ますます重要になってきますが，今なお解明すべき点が多いのが実情です．私たちは，引き続き必要な基礎技術構築に取り組んでいきます．

■参考文献

(1) 谷・高橋：“高速量子アルゴリズムの開発，”電子情報通信学会 基礎・境界ソサイエティ Fundamentals Review，Vol. 14，No. 1，pp. 15-27，2020.
(2) A. Hosoyamada, Y. Sasaki, S. Tani, and K. Xagawa: “Quantum algorithm for the multicollision problem,” Theoretical Computer Science, Vol. 842, pp. 100-117, 2020.
(3) S. Akibue, G. Kato, and S. Tani: “Probabilistic unitary synthesis with optimal accuracy,” arXiv:2301.06307，2023.
(4) Y. Takeuchi, Y. Takahashi, T. Morimae, and S. Tani: “Divide-and-conquer verification method for noisy intermediate-scale quantum computation,” Quantum, Vol. 6, p. 758，2022.

（左から）谷　誠一郎/ 秋笛　清石/
竹内　勇貴

NTT研究所は，爆発的に増大するデータを，ネットワーク上で超高速に分析・処理するため，量子コンピュータのハードウェアから超高速計算能力を引き出すことを可能にする基礎理論の確立に貢献します．

◆問い合わせ先
NTTコミュニケーション科学基礎研究所
メディア情報研究部　情報基礎理論研究グループ
TEL　0774-93-5020
FAX　0774-93-5026
E-mail　cs-liaison-ml＠hco.ntt.co.jp