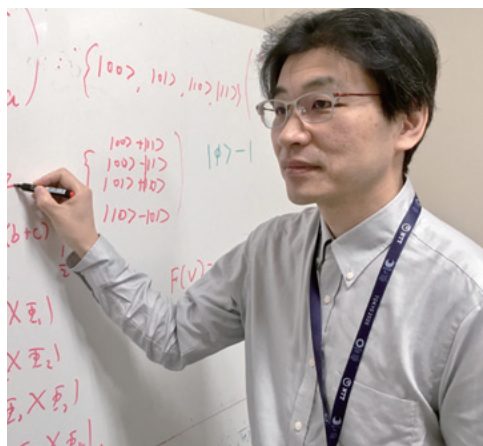




谷 誠 一 郎

上席特別研究員 NTTコミュニケーション科学基礎研究所



方向性が定まらない時期は基礎力を磨くためにある。後追いを止めて、視点を変えること

1980年代にスタートした量子コンピュータの実用化に向けての研究は、30年あまりが経過した現在、新たな段階に進みつつあります。こうした中、文部科学省は光・量子技術の推進費として32億円を概算要求に盛り込みました。今後の動向が注目される量子コンピュータ研究の現状と現在の研究成果、そして研究者に必要な姿勢について、世界初となる数々の成果を上げているNTTコミュニケーション科学基礎研究所 谷誠一郎上席特別研究員に伺いました。



第三の分野で革新的研究成果を達成。リーダ選挙問題で世界の注目を集める存在に

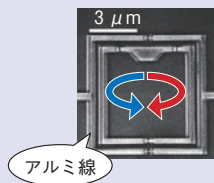
●現在手掛けている研究から教えていただけますか。

量子コンピュータについての研究を手掛けています (図

1)。量子コンピュータも従来のコンピュータ（量子コンピュータの世界では、古典コンピュータと呼ばれています）と同様にハードウェアがあり、その上にソフトウェアにあたるものがないと動きません。そのソフトウェアにあたる部分（量子アルゴリズム）のつくり方、すなわち、ハードウェアの性能を引き出すためにはどうしたら良いのか

	古典コンピュータ	量子コンピュータ
情報の単位	ビット (bit)	量子ビット (qubit)
情報の数学表現	ブール値	複素ベクトル
基本演算	ブール演算 (AND, OR, NOT)	一次変換 (ユニタリ変換)
物理的実現方法	半導体	半導体, 線形光学デバイス, 超伝導体 等

超伝導量子ビットの例⁽¹⁾



電流の向き	情報
時計回り	0
反時計回り	1

量子的な効果で、異なる向きの電流が共存 (重ね合せ)

図1 量子コンピュータとは

を理論的に考えています。研究を始めて15年ほどです。

量子コンピュータの研究の前提として知っておいていただきたいのが、すべての計算が量子コンピュータを使えば速くなるものではないということです。計算の種類によっては、古典コンピュータと同程度の速度のものも多く存在します。さらに、量子アルゴリズムの作り方が下手だと、量子コンピュータであっても、古典コンピュータよりも計算が遅くなってしまふこともあります。このような課題のもとに、量子コンピュータ上で高速計算が可能となる問題を探ること、この場合どの程度まで高速化が見込めるか、そのために真に必要な量子コンピュータの機能を見つけ、それをどのように古典コンピュータによる計算と融合するべきか、が私たちの研究の重要なテーマ、目標となっています。

量子コンピュータの概念は1980年代に提唱されましたが、研究が盛んになってきたのは1990年ごろです。この30年の間、量子コンピュータの研究はハード面・アルゴリズム面ともに、大きな進化をしてきました。私たちもその歴史においてさまざまな研究成果を上げてきました。その中でも評価が高かった成果の1つは「リーダ選挙問題を解くための量子分散アルゴリズム」の研究です(図2)。

量子アルゴリズムの研究は大きく分けて2つの流れがあります。Shorによって発見された、素因数分解を現在のコンピュータよりも指数倍速く行う量子アルゴリズムと、Groverによって発見された、膨大な数のデータの中から所望のデータを探す量子探索アルゴリズム、このそれぞれに端を発するものです(図3)。両方ともさまざまな応用や一般化について、20年にわたり研究が続けられていま

す。リーダ選挙問題を解く量子分散アルゴリズムはこの2つの大きな流れとは別のアプローチから発見されたものであり、先駆的な存在とも評されています。

リーダ選挙問題とは、ネットワーク接続されたコンピュータどうして自律的に1台のコンピュータをリーダとして選出する問題です。この問題は、多くのコンピュータの中から特定の処理を行うコンピュータを決定する場合などに用いることができます。故障などでコンピュータのアドレスの一意性が保証されない場合、この問題は古典

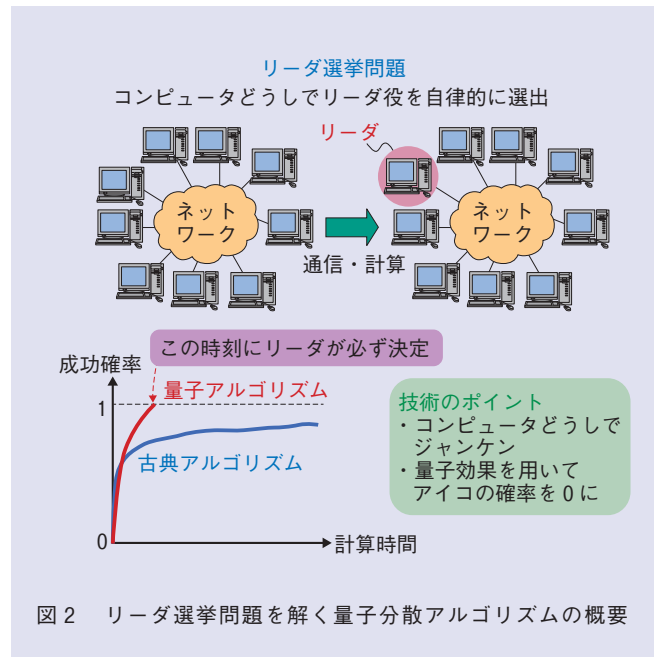


図2 リーダ選挙問題を解く量子分散アルゴリズムの概要

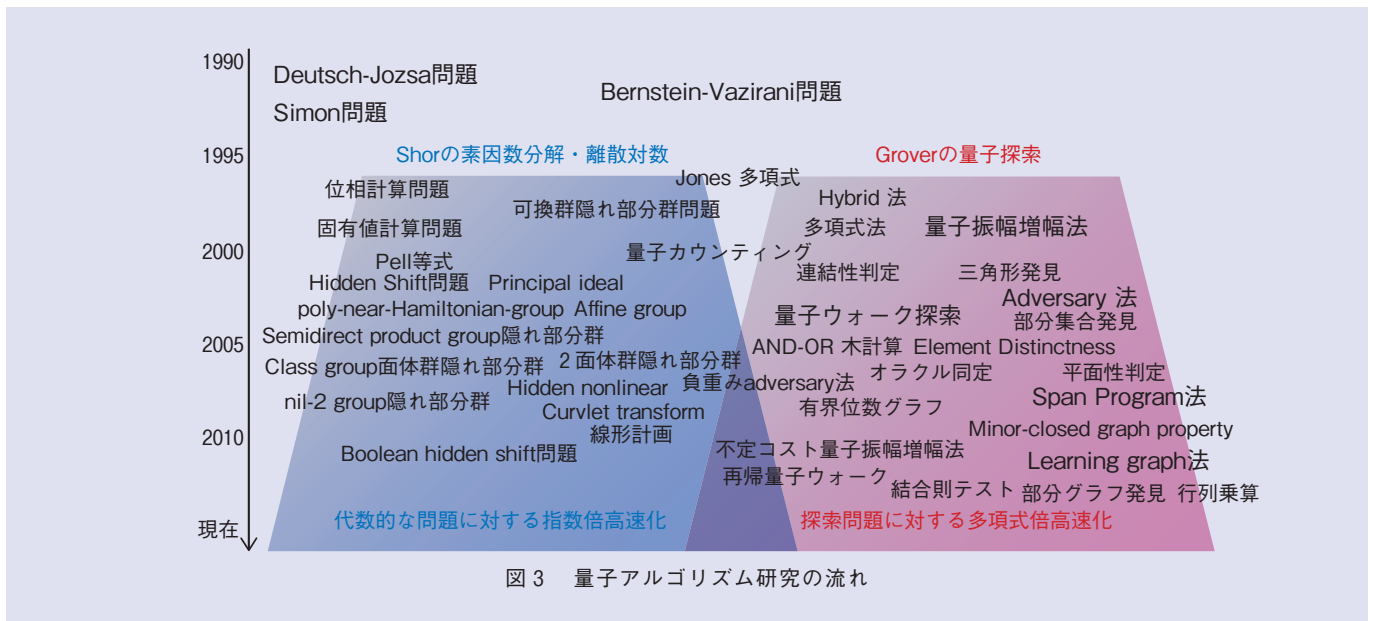


図3 量子アルゴリズム研究の流れ



挑戦する研究者たち

コンピュータで構成されるネットワークでは有限時間内に解けないことが知られています。これに対し、私たちは量子コンピュータで構成されるネットワーク上において、リーダ選挙問題を効率的に解くアルゴリズムを考案し、これが世界的に評価されました。

このアルゴリズムは、量子ビットの観測値（0または1）を用いて、複数のコンピュータでジャンケンをさせ、最後まで勝ち抜いたコンピュータをリーダとするものです。計算の過程において、ジャンケンがアイコになる確率をゼロにする手法を開発し、その結果、有限回数のジャンケン（有限時間内の計算）でリーダが選出されることとなります（図4）。

この成果は、量子コンピュータが、古典コンピュータとは本質的に異なる能力を持つことを理論的に示した点で評価されたわけですが、応用的観点からは、量子コンピュータで構成される量子ネットワークの自動セットアップに利用できると考えます。自動セットアップとは、量子コンピュータどうしを物理的に接続するだけで、ノードアドレスの自動付与、ルーティング経路の自動設定、管理権限のランダムな自動付与を可能にします。また、ネットワーク上に分散された入力データに関する計算のうち、古典コン

ピュータでは不可能だった計算も実行できるのです。

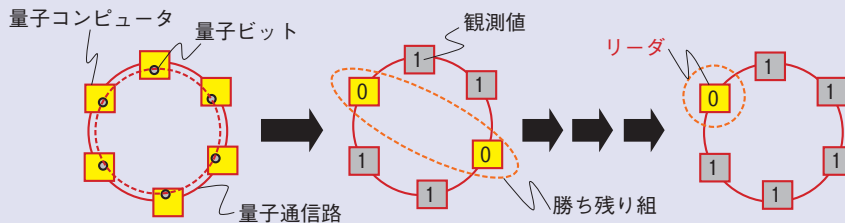
●量子コンピュータ研究の長い歴史の中で、革新的な成果を上げられているのですね。

理論分野の研究者は皆、未知のことを明らかにして今後の研究の方向性を示すことをねらいとしています。私もその1人です。リーダ選挙問題に関しては、「一番尖った部分」を出せたかなと実感しています。この研究成果に関して、日本で本格的な量子コンピュータ研究が始まって間もない時期に量子情報科学の最上位国際会議で口頭発表できたことやACM (Association for Computing Machinery) の論文誌ACM Transactionsに掲載された点で、当初のねらいは達成できたのではないかと思います。ACMのSIGACT Newsや教科書 (Rodney Van Meter著) で取り上げられたこともうれしかったですね。

ちなみに、量子アルゴリズム研究分野には私たちよりも上の世代の研究者たちは、あまり存在しません。私たちの世代が研究者として一人前になりつつある1990年代に、量子アルゴリズム研究が立ち上がりましたから、結果として、私たちの世代以降の研究者が先駆者になったともいえます。

アルゴリズムの直感的イメージ：

- (1) 量子ビットの観測値（0または1）を用いて、コンピュータどうしでジャンケン。少数派が勝ち（同数の場合、1を持つコンピュータが勝ち）
- (2) 最後まで勝ち抜いたコンピュータがリーダになる



アイコ事象を含まない重ね合せの生成手法

各コンピュータが0と1の重ね合せ状態を準備 (全体としては全事象の重ね合せ)

量子分散計算により、全事象の重ね合せ (A+B) を、アイコの事象の重ね合せ (A) と非アイコの事象の重ね合せ (B) に分離し、確率的にいずれかを選択して出力

A
アイコ事象の重ね合せを非アイコ事象の重ね合せにユニタリ変換

B

終了

アイコの確率を0にするユニタリ変換

$$U_K = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & e^{-i\pi/K} \\ -e^{i\pi/K} & 1 \end{pmatrix}$$

$$V_K = \frac{1}{\sqrt{R_K+1}} \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & \sqrt{R_K} & \frac{e^{i\pi/K}}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & -\sqrt{R_K}e^{-i\pi/K} & \frac{e^{-i\pi/K}}{\sqrt{2}} \\ \sqrt{R_K} & 0 & \frac{e^{-i\pi/K}I_K}{i\sqrt{2}R_{2K}} & -\sqrt{R_K} \\ 0 & \sqrt{R_K+1} & 0 & 0 \end{pmatrix}$$

$$R_K = \operatorname{Re}(e^{i\pi/K}) \quad I_K = \operatorname{Im}(e^{i\pi/K})$$

図4 リーダ選挙問題を解くためのアイデア



駅のホームに降り立ったとき、雷に打たれたようにひらめいた！ インパクトのある成果を得るにはメジャーに挑むべし

●リーダ選挙問題を解くアルゴリズムはどうやって誕生したのですか。

横須賀でネットワークプロトコルの研究開発を手掛けていた私が、2003年に基礎研究所に異動してきたころにはすでに中堅と呼ばれる世代でした。新人ではないですから、1年も2年も研究成果を上げずにいられるような立場ではありません。「何か結果を出さなくてはいけない、そのためには世界で誰も手掛けておらず、自分のバックグラウンドを活かせそうなものはないか」と、一所懸命テーマを探しました。量子コンピュータ研究の分野には、すでに研究者は数多く存在しましたから、新参者の後追いではなく、違う視点から取り組んでみようと思い、そのためにまずは論文を読みあさりしました。

さらに、前人未到の成果を上げたらインパクトがあるだろう、メジャーなものが良いだろうと考えて、教科書も洗い直しました。論文の片隅にあるような小さな問題ではなく教科書に掲載されるような大きな問題に絞ったところ、リーダ選挙問題を見つけたのです。リーダ選挙問題は分散計算の教科書には必ず書いてある重要な問題で、当時、量子コンピュータ分野においてあまり研究がなされていなかったネットワーク関連の課題でした。

芽が出たのはリーダ選挙問題にねらいを定めてから4カ月目くらいでした。完全に幸運だったと思います。私は量子コンピュータ分野において経験の蓄積はなく、まるでパズルのピースを埋めるような作業を繰り返していました。しかも、そのパズルも完成するとは限りません。完成すると信じて計算を試す日々が続きました。連日、ひらすら机の上の何冊ものノートと向き合って計算していました。コンピュータで計算するための理論を、コンピュータを使わずに考えて計算するという、何とも面白い世界です。

いつ完成するとも分からないパズルを解くかのごとく計算し続けて4カ月目に、核となる補題の証明がやっと完成の瞬間を迎えました。その瞬間は半信半疑でドキドキしました。量子コンピュータ研究を希望したからには何か結果を出さなければと一心不乱に頑張っていましたから、とても嬉しかったのですが、一方では突然すぎて信じられませんでした。当時、車で通勤していたのですがどうやって家に帰ったのか、覚えていません。

さらに、研究を進め、数カ月が経ちました。そのころ、また別の補題を考えていたのですが、出張の帰りに、駅の階段を下りホームに降り立った瞬間に、まるで雷に打たれたかのように、その補題を証明するカギとなるアイデアが

ひらめきました。私は、電車に乗っている（乗ろうとしている）ときは「移動」という目的を果たしているの、無駄な時間を過ごしているわけではないという安心感からか、リラックスできているように思います。このため、電車等で移動しているときに、ふっとひらめくことが多く、このときもまさにそのような状況でした。

●プレッシャーの中で見つけた研究テーマが世界に先駆けた結果につながっていったのですね。そう考えるとプレッシャーというのは適度にあったほうが良いですね。

確かに、ある程度のプレッシャーはあったほうが良いですね。研究生活をスタートしたときは小さな問題を解きながら経験を蓄積していくのですが、将来的に研究者は大きな成果をねらっていると考えると、リスクな問題に取り組むとプレッシャーは大きくなりますが、研究者としては、たとえ時間がかかっても取り組むべきだと思います。

消極的な意見ですが、理論研究は苦しいです。時間とともに研究が少しずつ進むのではなく、あるとき階段状に急に進みます。ステップを上げるタイミング、つまり結果はいつ来るのかも分からないし、上げられるのかも分かりません。そのチャンスが来るまでは何も動きのない状態で頑張らなければなりません。これは言葉以上に精神的につらいものです。もちろん、他の分野でも別のつらさが存在することを経験上知っています。要は、自分の能力を発揮できるような分野であれば、プレッシャーを力に変えやすくなるのではないかと思います。私の場合も、苦しいこと以上に研究できることの喜びが大きかったからプレッシャーに耐えられたのだと思います。

研究成果をいくつか挙げられると、「またいつかそんなときが来るさ」という根拠のない楽観視ができるような気がします。しかし、若いうちは「本当にこのままダメになってしまうのか」と悲観してしまうこともあるでしょう。結局は自分を信じるしかないのです。半年、1年考えていてもらちがあかないことがありますから、結果にこだわらず自分で期限を決めて挑むことも大切であると思います。

●ところで、なぜ研究者としての道を歩まれたのですか。

大学時代、3カ月後に卒論提出が迫っているのに、成果ゼロの状態のときがありました。必死に頑張っただけでひねり出した理論を研究室で発表したら、先輩から間違えていると指摘を受け、残り1カ月半で死に物狂いで取り組んで窮地を脱したという経験もあります。その当時は「階段を上がるタイミング」は急に来るとは知りませんでしたから、先が見えず本当につらかったです。しかし、この体験により理論研究の楽しさが増し、研究者の道も良さそうだと思います。それから、修士課程を終えての岐路で、就職か進学か悩んだときに、就職して研究するほうがカッコいいと当時の私は思ったようです。当時の先輩には企業にいな



から研究活動をしている方も多かったので、就職イコール研究から遠ざかるというイメージはなかったのです。NTTを選んだ理由は、基礎的な研究をじっくりさせてもらえるに違いないと思ったことです。実際には、NTTに入社してから大きな組織再編があり、自分がかかわる研究分野も大きく変遷しました。しかし、今になって冷静に振り返ると、学生時代に理論研究を手掛け、入社後、集積回路やネットワークプロトコルの研究などの応用分野を経験し、再び理論分野に戻るようになったわけですが、結果的にこれらの経験が結びついて今の研究成果を生み出したと思っています。



日々の研究に楽しみを感じてほしい。 100年後に残る研究をしよう

●では、若い研究者の皆様一言お願いします。

基礎研究においても、研究をするからには「有用性」を考へて研究テーマを掲げるわけですが、何かの役に立つということだけをモチベーションとして研究生活を送るのは難しいと思います。研究をしていること自体に喜びを感じられることが大切ではないでしょうか。基礎研究は基礎学問、我々の分野では、特に数学や物理が大きくかかわってきます。我々は、純粋数学をしているわけではありませんが、テクニクとして数学を使います。実は、この数学を使っていること自体を楽しそうにしている研究者は少なくありません。楽しみがプラスアルファの結果を生むのです。日々の研究に喜びを感じられることが研究者として幸せだと思ひます。

また、研究者として方向性が定まらない時期はつらいものですが、そういうときにこそ、基礎力を磨くことにエネルギーを割くことができます。将来の自分の力になる基礎の部分をしっかり和積み上げることは重要で、先ほど言ひましたように、我々の分野では、それが（広い意味で）数学になるわけですが、自分が苦勞した経験からいへば、大学学部程度の数学は最低限しっかり身につけておきたいで、研究生活を通して、学習を繰り返した今だからこそ、基礎力のレベルを上げていくことは非常に大切だと分りました。常に基礎力を向上させることによって、5年前の自分では歯が立たなかつたことが、現在の自分ならばできるようになつていたいと思ひます。

ときには、研究から離れる時間を持つことも大事だと思ひます。私はスポーツ（特にサッカー）やドライブなどをしていひます。研究ばかりに取り組んでいると袋小路に入つてしまつて精神的に疲れてしまひますので、まったく別のことをすることも大切だと思ひます。

そして、海外に行く機会があればぜひ挑戦してください。少なくとも数力月は1人で滞在してほしいで、世界中からポストドク（博士号を取得した後の非常勤研究員）などが集まる場所へぜひ行ってほしいで、彼らのギラギラした目の輝きを見ると研究に対しての姿勢が変化すると思ひます。私もカナダのウォータールー大学で2010年から1年間勉強させていただきましたが、量子コンピュータ分野のトップクラスの研究者が集まる場所で、この感覚を実感できたことが一番の財産になりました。国際会議なども同様、落ち着いて研究できる場に身を置いているからこそ、時々は刺激を受けに出られるのも良いと思ひます。

●今後はどのような展望をお持ちで、

量子コンピュータのハードの研究は少しずつで、進んでいひます。ここ2、3年のことですが、世界的に量子コンピュータ分野の研究に多額の研究資金が投入されたことで進展が早まりそうな感じがして、といへば、理想的な量子コンピュータができるまでにはまだまだ時間がかかりそうです。それまでは機能に制約がある量子コンピュータの誕生となるでしょうけれど、制約されていたとしても重要な問題が解けることはとても喜ばしいことと、近い将来に実装できると期待されている、そのような量子コンピュータで、具体的にどんな問題に挑めるかを探っていくことはますます重要と考へ、実際に手掛けている最中と、

それから、古典コンピュータに関する技術の蓄積は膨大なものがありますから、古典コンピュータで解けるものは古典コンピュータで解いてしまったほうが良いと考へますが、それを踏まえて量子コンピュータに任せるべきところはどこなのか、という判断はまだ不十分で、私はこのあたりにも興味を持って挑んでいひます。

時流に乗った仕事も大切ですが、私は研究者として「世の中に残る仕事」をしていきたいで、量子と古典の計算を俯瞰してみたいと思ひます。5年、10年で価値がなくなるものではなく、100年後も通用するものから、短期的に取り組めるものまでテーマを並行して走らせていきたいで、

■参考文献

- (1) 山口：“量子コンピュータ研究の最前線”，NTT技術ジャーナル，Vol.24，No.6，p.10，2012.