

2022年ノーベル物理学賞に 量子もつれと量子情報科学

根本香絵 | OIST（沖縄科学技術大学院大学）
国立情報学研究所



ノーベル賞の受賞者発表は10月恒例の一大ニュースで、インターネットでも世界中を駆け巡ります。ただ、コンピュータ科学・情報科学の研究環境にいと、いまひとつ無関心な雰囲気も漂っていて、いわば隣町のお祭りのような感じでしょうか。ひと昔前、ヨーロッパから共同研究に来たコンピュータ科学の教授が、ノーベル賞メダルチョコレートをお土産に持ってきてくれたことがあり、物理学者の私たちがやんわりとからかったりと、「ちょっと他人事」というのがいい距離感でもあります。物理学者にとっては、ノーベル賞はそれなりに身近で、ノーベル賞が発表されるころになると、「今年の受賞者は？」はよくある雑談のテーマです。今回も、大学のカフェテリアの横のテラスで研究室のメンバとランチをしていると、誰ともなく「明日のノーベル物理学賞は誰だろう」と言い出し、各自の予想話に展開しました。私は、Anton Zeilinger先生はどうかと言っ、その後予想が当たったとみんなに言われたのですが、どちらかという、予想というよりもそろそろ量子情報でもよいかと思ったのです。ここ20年ほどは、量子科学に関するノーベル物理学賞も多くなっていましたが、量子情報科学と明確化したものはまだなかったので、いつかなと楽しみにしていた研究者も多かったのではないかと思います。この数年で量子情報は情報科学としても大きく動き出し、新しいステージを迎えています。その分

野の成長を記念するかのようなノーベル賞、物理学賞ですがコンピュータ科学、情報科学を巻き込んだ受賞に心からお祝いを申し上げます。

さて、2022年ノーベル物理学賞の受賞理由を改めて見てみます。そこには、受賞者3名の功績として、「量子もつれ状態の光子を用いた実験によるベルの不等式の破れの実証と、量子情報科学における先駆的研究」とあります。ここでキーワードは3つ、「量子もつれ」、「ベルの不等式」、そして「量子情報科学」でしょうか。ベルの不等式の破れの実験が初めて行われたころは、まだベルの不等式が示す重要な量子性である非局在性と、量子もつれのような量子物理学の世界にあるさまざまな相関関係とは区別がついていませんでした。そんな中で、これらの実験研究は、量子情報的な性質を実験で実証することができることを示し、量子情報の可能性を大きく拓いたと言えます。それではまず、「量子もつれ」から見いきましょう。

量子もつれとは

量子もつれは、量子計算がそのパワーを出すためには必要となる性質のため、量子コンピュータ研究でも頻出用語で、最近では社会一般に浸透した用語となってきました。量子もつれとは、量子的な相関のひとつで、たとえば複数の量子ビットの間で現れ

る性質です。量子ビットが1つしかないときには、量子もつれを議論することはできません。たとえば、2つの量子ビットの間に量子もつれがあるときには、2つの量子ビット全体での状態は決まっていますが、その間にある量子相関のため、一つひとつの量子ビットの状態を決定することができません。決定しようとする、量子相関を壊してしまうからです。量子計算が量子計算の優位性を発揮するためには、量子計算の途中で量子もつれの量が増えることが必要ですが、これを行うために量子ビット間の相互作用や相互作用に匹敵するゲート操作を準備します。ゲート操作によって、量子ビットの状態を変化させ、その量子ビットが担う「量子情報」を「処理」することができます。ゲート操作を行う量子ビットの数で、1量子ビットゲート、2量子ビットゲートなどと呼ばれ、量子力学の数学的体系ではユニタリー演算に相当します。1量子ビットゲートが量子もつれを生成することはなく、量子もつれには2量子ビットゲートが必要となるため、その実装に直接的または間接的な相互作用が必要となります。物理的にはこれを高い精度で実装することは今でもなかなか大変です。量子ビット間の相互作用があると、それらの量子ビットの状態が一緒に時間的に変化するので、1量子ビットゲートでの時間発展とは異なる時間発展が生み出され、量子もつれの量を変化させることができます。このようなゲート操作ではCNOTゲートが有名です^{☆1}。

ただ、量子もつれがあればよい、というものでもないことも分かっています。GK (Gottesman-Knill) 定理¹⁾は、CNOTゲートがあっても、Clifford群に属するゲートだけから成る量子計算は、古典計算機でも効率的に計算できることを示しました。量子

情報の初期のころには、量子もつれが量子計算を量子計算たらしめるものとして使えるのではないかという期待もあったわけですが、量子もつれは必要であるけれども、十分ではないことが分かり、量子計算を特徴づけるのは簡単にはいかないのだなということになりました。また、「量子もつれ」と言っても、ではどう「もつれて」いるのかには実にさまざまな形態があることも分かってきて、量子ビットの数が増えると、それだけ種類も指数的に増えていくので、量子もつれの世界も一筋縄ではいきません。その上、量子もつれを実験で測ろうとすると、そこにもまた量子ビットの数が増えるに従って指数的なコストがかかります。それを回避するために、量子もつれ witness という量子もつれがあることだけを示す指標の研究も数多く生まれました。

ベルの不等式は破れるか

さて、次は「ベルの不等式の破れ」です。ベルの不等式は、確率変数間の相関に関する不等式で、ベルの不等式が破れるとき、量子非局在性があると考えます。非局在性はEinsteinをも悩ませた性質として有名で、量子力学の本質的な性質のひとつで1964年にJohn Stewart Bellによって導かれました。すでにベルの不等式の破れは半世紀以上にわたり知られているのですが、量子もつれに比べるとメディアに登場する回数は少なめで、あまり馴染みがないかもしれません。

ベルの不等式に始まった非局在性の定式化では、非局在性を強く破るにはどういう不等式を考えればよいかなどの考察が進み、さまざまな形が提案され定式化されています。実は量子もつれの方も、量子もつれの度合いを示すさまざまな指標が考えられました。エントロピーを使ったエンタングルメント(量子もつれ)・相対エントロピーや取り出せる量子もつれを示す量などがあります。ベルの不等式の破れ度合いや量子もつれの程度を筆頭に、一般的

^{☆1} CNOTゲートは、Controlled-NOTゲートの略で、コントロール量子ビットと呼ばれる量子ビットの状態が0のときは、ターゲット量子ビットの状態にアイデンティティ演算を、1のときは0と1を反転させる演算を行うゲートです。量子ビットは、0と1の重ね合わせ状態を取るため、コントロール量子ビットが0と1の重ね合わせ状態の場合に、量子もつれの量が増えます。

に量子相関について考えるとき、ノイズのない理想的な状態を考えているときは、比較的数値計算も行って、理解しやすいことが多いです。一方で、実験では必ずノイズの影響を受けてしまいます。そこに、実験で検証する難しさがあり、同時に理論上もそんなに簡単にはいかないのです。ベルの不等式の破れの実験では、破れがあることを示すだけでは十分ではないという考え方もあって、局所的実在性の仮説の抜け穴をすべて塞ぐことも実験で続けられてきました。そのような抜け穴をすべて塞ぐことができた場合を指して、Loophole-free ベルの不等式の破れと言います。

歴史を振り返ると、1960年代から今日まで、日本では量子物理学を用いた新しい産業、半導体産業や光産業に力を注ぎ、大きな貢献をしてきました。一方で、欧米諸国では同じ産業的成長を見ながら、量子力学基礎という分野が発展を続け、ベルの不等式の破れを筆頭に、量子力学の理解を深めていったのです。量子コンピュータや量子計測、量子暗号などもその学問的な土壌から生まれてきたものです。残念ながら日本では、ベルの不等式や測定を大学の講義で扱うということはしてきませんでした。ここに、量子現象を応用するという域を超えて、量子の世界にさらに踏み込み、量子状態を直接的に操作するという発想への動機と理解を欠いており、個々には素晴らしい研究はあっても、全体として大きな新しい研究の流れを生み出すことができなかつたように思います。

ベルの不等式や量子計算の初期的な概念、量子暗号への応用などは、量子力学基礎論がまだ発展途上だったところに生まれてきました。まだよく分からない学問領域は、日本では敬遠されがちです。特に物理学では固体物理のように確立したいわゆる伝統的な領域に人気があり、新しい学問領域はややもすると「怪しい学問」と言われてしまったりして、評価の定まらない研究は日本ではまったくと言っていいほど人気がありません。まだよく分かっていない概

念を科学的に扱うには、しっかりとした科学的な方法への理解と数学的な素養、そしてそこに踏み込む勇気が必須で、とても高度でやりがいのある分野であることを、研究者自身が理解することも大事です。そして今回のノーベル賞が象徴するように、20世紀後半を通して続けられてきた、未知の領域における研究者達の十分な議論があり、これが今の量子情報技術の発展に結びついていることの中から、私たちは研究を育てる研究支援の方法についても再考し、より良い方法を実践していく必要があると改めて感じます。

量子相関と量子非局在性

ところで、受賞理由の1つ目は、「量子もつれ状態の光子を用いたベルの不等式の破れの実証」でした。ここで、量子もつれ状態とベルの不等式の破れはどう関係しているのでしょうか。「量子的にもつれているか」を問うためには2つ以上の対象、たとえば2つの量子ビットなど、を必要とします。2つの量子ビット間に量子もつれがあるかどうか、ということ問うからです。量子もつれがなければ、それぞれの量子ビットを別々に議論して、片方がないものとしても、まったく問題は生じません。反対に、量子もつれがあれば、全体の状態は決まっても、一つひとつの量子ビットの状態を決定することはできないので、お互いに見えなくなり、その意味で、量子もつれも非局在的な性質と言えます。実際、2000年初めぐらいまでは、量子もつれとベルの不等式の破れの間にはどのような関係性があるのか、ということが研究されてきました。研究が進むにつれて、この2つはむしろ異なる性質を持つことが分かってきました。たとえば、量子もつれの度合いが高くても、ベルの不等式を破りにくい状態があったりと、ベルの不等式の破れの程度と量子もつれの度合いとの関係は単純ではないことが分かってきたからです。量子コンピュータでは、非局在性そ

のものが重要な尺度ではないため、量子ビット間の関係性を直接的に見る量子もつれが多用され、一方で、非局在性が重要な役割を持つ量子暗号など、量子通信・セキュリティでは、ベルの不等式が用いられることが多いです。

また、ここで忘れてはならないのが、ベルの不等式の破れを実験で実証したことです。このような量子性の本質の実証を積み重ねることによって、ミクロな世界の理論と言われていた量子力学は、大きな舞台へと出ていくこととなります。それが、次のキーワード、「量子情報科学」へつながっていきます。

いよいよ量子情報科学へ

その量子情報科学ですが、まず「量子もつれ状態の光子を用いた実験によるベルの不等式の破れの実証」は、「量子情報科学における先駆的研究」とどう繋がっているのでしょうか。

ベルの不等式が定式化されたころには、それを実験的に実証することは困難でした。それをやってみようというノーベル賞の対象となった研究も、当時は相当クレージーであったに違いありません。ただ、そこにはそれまでにはない技術の進展があったことは事実です。たとえば、光子ひとつを生成する、量子的にもつれた光を生成する、また光子ひとつを高精度で捉えるということも、簡単ではなかったわけです。そのような量子制御の技術的な発展が、実証実験を可能にしたと言えるでしょう。量子もつれという当時は新しい考え方を使って、非局在的な状態の光を作り出す、そしてそれを使ってベルの不等式の破れが初めて実験的に検証できた、と読み解くことができます。

20世紀に定式化されたり理論提案された現象が実験的に検証され、ノーベル賞へつながる例はこの20年、30年間よく見てきました。中には理論提案はほぼ100年前というものもありました。今回は、それがいよいよ量子現象から、量子情報へと踏み込

んできたというところに新しさを感じさせます。また、同時に、量子制御技術の発展によって、量子物理や量子情報における理論提案と実験検証の周期が短くなってきていることも大きな特徴のひとつです。短いといっても、100年ぐらいかかったのが、数十年という単位ですので、これを2、3年と勘違いしてはいけません。ただ、理論にとっても実験にとっても、アイデアを実際に「動かせる」時代になったということで、私たちが運良くエキサイティングな時代に生きていることは間違いないのです。

情報処理の観点から

ここで、少し量子情報科学の発展を、情報処理の観点から考えてみたいと思います。「量子」と頭に付いてはいても、量子コンピュータは現在のコンピュータ、量子通信なら現在の通信の理論体系に基づいて発展してきたということはできるでしょう。量子コンピュータを考えると、状態の初期化、そして読み出しがあります。読み出し、つまり量子コンピュータの量子ビットの状態を測定して初めて、量子コンピュータの計算の結果を取り出すことができます。「情報」として扱えるのは情報理論で定義され得る量であって、量子情報、つまり量子状態が担っている情報は、必ずしも「情報」としては取り出せないのが、厳密には情報ではありません。ただ、量子状態が担っている情報をどう呼べばいいのか困るので、便宜上量子情報と呼ばれるようになりました。このことは、量子コンピュータが、現在のスパコンでも計算できないような複雑なことを実現している、ということと、その過程を計算力として取り出せるかということはまた別の問題であるということと関連しています。

量子コンピュータでは、現在のコンピュータの理論体系に習い、基本となるゲート集合を定めて、それらのゲートの組合せで量子回路（ゲート列）を作り、任意の量子計算を実装します。この考え方とは

異なるものとして量子アニーラーが広く知られていますが、こちらはむしろ一定の問題を解くことに重きがおかれています^{☆2}。任意の量子計算を数少ない決まったゲート操作を実装し、繰り返し使うというこの考え方は、計算ごとに違う量子操作を実装するのは大変であるため、実装上も理にかなったものと言えます。さらに、2つの量子ビット間の相互作用は比較的実装が容易ですが、3つ、4つと複数の量子ビットをその都度ごとに相手を変えて実装するのは困難至極なため、物理的には1量子ビットと2量子ビットのゲートだけで、任意の量子計算が行えるということには、一定の意味があります。

この「どんな量子計算も行えるか」という点は、選んだゲート集合のユニバーサルリティで担保します。量子系の時間発展はユニタリー演算子で書くことができるので、初期状態から、計算の解となっている終状態への状態間のマップをユニタリー演算子で書くことができると、任意のユニタリー演算子を構成できるかどうかでユニバーサルリティを問うことができます。選んできたゲート集合の要素だけで任意のユニタリー演算子を任意の精度で再構成できるとき、そのゲート集合はユニバーサルリティを満たすと言います。これも通常のコンピュータの理論を援用した概念ですが、連続的に取り得るユニタリー演算子を再構成するという点は、実はかなり無理もしているのです。ユニタリー演算の中の連続パラメータを任意の精度で実行するには、それなりに長い量子回路が必要になるわけです。これは量子計算の深さから考えるとあまり歓迎できない、厄介な要素と言えます。

それを回避するには、たとえば1量子ビットゲートをHadamardゲートやTゲート($\pi/8$ ゲート)のように決まった離散的なものだけでなく、連続パラメータで動かすようにすればよいのではないかと考えるかもしれません。実際、1量子ビットゲート

の実装では、パラメータの値によって簡単になったり複雑になったりするわけではないので、決まった値にする必要性は実装上はありません。ところが、量子誤り訂正符号を実装した論理量子ビットでは、数少ないゲートしか実装できないことが分かっており、離散的なゲート集合を取らざるを得ません。

量子ビットは測定して誤りを直すというわけにはいかないこともあり、エラーは時間とともに段々と蓄積してしまいます。最近話題になっている数十から数百程度の量子ビットから成る量子プロセッサはNISQ (Noisy Intermediate-Scale Quantum) プロセッサと呼ばれていますが、名前のおりノイズがあることを特徴とします。量子誤り訂正符号を実装するには量子ビットの数が足りないため、物理量子ビットをそのままデータを担う量子ビットとして用います。このため量子プロセッサ内のデータ量子ビット上のエラーは時間とともに増えていきます。最終的なエラーをなるべく小さくするために、任意の1量子ビットゲートを実装し、量子回路を短くしてノイズの影響を小さくすることになります。一方、量子誤り訂正符号を用いて論理量子ビットでデータを担うようにしたフォールトトレラント量子コンピュータでは、ゲートは離散化して、ユニタリー演算子の連続パラメータはこれらのゲートの組合せで実装します。そのため、フォールトトレラント量子コンピュータは、NISQプロセッサのような物理量子ビットに情報を載せる場合に比較して、計算時間はだいぶ長くなるのが理論的に予想されます。

ここに登場する、量子計算のユニバーサルリティ、量子計算の計算量、量子誤り訂正や量子コンピュータアーキテクチャなどは、どれも現代的な研究分野であり、量子もつれ状態の光子を用いた実験によるベルの不等式の破れの実証を目指した当時はまだ拓かれていなかった研究分野です。また、現代的な課題としては量子計算に絡む新しい問題、たとえば量子コンピュータ言語やコンパイラ設計、量子回路圧縮に絡む課題などが次々と出てきています。一方で、

^{☆2} 量子アニーラーは、断熱量子計算を横磁場のあるイジングハミルトニアン(固体物理に登場するモデル)をノイズのある環境で実装するものを現在の指し、内在する量子性の程度についても今後議論が進むことが期待されます。

量子情報科学は量子計算にとどまることなく、量子計測や量子暗号など ICT 全般にわたって新しい技術の創出や、量子物理学の新奇現象の発見と実証、また新しい数学的な構造の発見から新しい数学も生まれてきています。これら私たちの量子コンピュータの現在の課題を見るだけでも、量子情報科学が当時からどれだけの大きな発展を遂げたのかが実感されるのではないのでしょうか。

日々の研究から

ノーベル賞をもたらす研究が、私たち人類にとって大きな一歩であることは間違いないにしても、その研究に取り組んでいる時点では、その他の数多くある研究のうちのひとつにしかすぎません。昨今、評価や注目度などばかりが重要視されがちですが、ノーベル賞受賞のニュースという機会は、研究における長期的な視点の重要性を年に一度認識し直す良い機会であるように思います。翻って、今なによりも大切なことは、将来のノーベル賞に匹敵するような成果へつながる研究の種をいかに多く蒔き、育てることができるかです。量子情報科学が学問を超えた収穫をもたらすには、まだ時間がかかります。ここまで育ってきた量子情報科学をさらに発展させ、社会への還元を図るのと同時に、今こそ新しい種を蒔き、大事に育てていきたいと思うのです。研究が持つ長い周期を理解して、どのような研究支援が必

要なのかを考えていくことは、今後ますます重要になっていくと考えられます。

2022 年のノーベル物理学賞は、情報処理と物理の研究者が一緒にお祝いできるノーベル賞となりました。このノーベル賞を記念して本会に寄稿させていただくことに、とても深い感慨を覚えます。そうすると夢も膨らんで、今度は、計算科学、情報科学の研究者が量子情報科学の分野でノーベル物理学賞を受賞するのも夢ではない気もしてきます。その日が来たときには、量子情報科学はどのような姿になっているのでしょうか。そう考えると、もう今から楽しみでなりません。

参考文献

- 1) Gottesman, D. : The Heisenberg Representation of Quantum Computers, Group22: Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics, eds. S. P. Corney et al, (Cambridge, MA, International Press, 1999), p.32, quant-ph/9807006.

(2023 年 3 月 14 日受付)
(2023 年 4 月 19 日 note 公開)

根本香絵 (正会員) kae.nemoto@oist.jp

理論物理学者、博士 (理学)。沖縄科学技術大学院大学教授、OIST 量子技術センター長。国立情報学研究所にて量子情報国際研究センター長および JFLI 日本ディレクターを兼任。米国物理学会 (APS) および英国物理学会 (IOP) フェロー。