量子計算で出来ること・出来ないこと

森前智行 〈京都大学基礎物理学研究所 tomoyuki.morimae@yukawa.kyoto-u.ac.jp〉

1. はじめに

原子や光子などのミクロな世界は量子論に基づいている。量子論は我々が普段生活しているマクロな世界では目にしないような不思議な現象にあふれている。その不思議な現象をうまく制御することにより高性能な計算を実現するのが量子計算である。量子計算の始まりは、1982 年のファインマンのアイデアであるといわれており、すでに 36 年の研究の歴史がある。36 年の間に、無数の理論的・実験的結果が得られてきており、それらにより、今日では量子計算は古典計算より「速い」と信じられている。しかしながら、どういう意味で「速い」のかについては非専門家の方にはあまり正確に理解されていないように見える。とりわけ、最近の量子計算ブームのなか、かなり無茶苦茶な情報が一般の人々に流布されてしまっている[1]。本稿では、量子計算は何が出来て何が出来ない（あるいは出来ないと思われている）のかについて、現在分かっていることを整理する。

2. 量子計算の上限

まず、量子計算機はすごいといっても何でもできるわけではなく、その能力には上限がある。例えば、量子多体系の数値計算を行っている方はよくご存知だと思うが、量子多体系のダイナミクスというのは、ものすごく長い時間（粒子数の指数関数で増加する時間）をかけていいなら古典計算機で（粒子数の）多項式サイズのメモリでシミュレートできる。量子計算というのは量子多体系（スピン 1/2 の系）のダイナミクスに過ぎないので、量子計算も、古典計算機で量子ビット数の多項式サイズのメモリでシミュレートすることができる。実際、量子計算を経路積分で考えて、各経路の振幅を足し合わせればよい。一つの経路の振幅の計算は古典計算機で多項式サイズのメモリを使って多項式時間でできる。経路の数は最大で指数個あるので、全ての振幅を足し合わせるのに最大で指数時間かかる。

この考え方を使うと、BQP $\subseteq$ PSPACE という計算量理論でよく知られている結果が導かれる。まず、計算量理論というのは計算機科学の一つの分野であり、大雑把にいうと、ある問題を解くのにどのくらいのリソース（時間、メモリ等）を必要とするかを調べる学問である。計算量理論は通常の物理学科のカリキュラムではもちろん習わないが、計算機科学においては中心的な分野の一つである。計算量理論の教科書としては例えば Arora-Barak[1] 等がある。BQP というのは、量子計算機で効率的な時間（入力サイズの多項式時間）で解ける問題[2]の集合である。BQP は Bounded-error Quantum Polynomial-time の略である。Quantum と Polynomial-time は意味が分かると思うが、Bounded-error というのはよくわからないと思う。しかし、これが何かというのを説明し始めると長くなってしまうのでここでは説明しない[1]。物理だと、略語が何を略しているか聞けば、その内容も分かるが（例えば NMR は Nuclear Magnetic Resonance の略であると聞けば NMR の意味が分かる）、計算量理論の場合、略語のもとを聞いてもまったく情報が増えないことのほうが多く、略語のもとについては気にしないほうが良い。一方、PSPACE というのは古典計算機で効率的なメモリサイズ（入力サイズの多項式）で解ける問題の集合である。（こちらは、Polynomial SPACE の略なので分かりやすい。）メモリサイズについては指定しているが、計算時間については何も言っていないので、計算時間についてはどれだけかけてもいいクラスなのである。

つまり、もう一度繰り返すと、量子計算はどんなに時間をかけてもいいなら古典計算機で効率的なメモリサイズでシミュレートできるのである。逆に言うと、古典計算機で効率的なメモリサイズで解けない問題は量子計算機で効率的な時間では解けないということである。

3. NP

NP という計算量クラスは量子計算が「苦手」な類のものとして最も有名な例の一つである。量子計算が NP が「苦手」であることは、量子計算の歴史の初期の段階からすでに指摘されている[2] が、なぜか国内では全く真逆のことが広く吹聴されているようである。

次のようなストーリーを考えてみよう。太郎君は今話題のシミュレーションゲームを買った。これは、「学校に行く or 公園に行く」のように、2 択が画面に現れ、どちらかを選ぶとそれによってストーリーがさらに進み、次の 2 択がでる、というものである。どんどん 2 択に回答していき、最終的に、条件を満たすとゲームはクリアー（成功）となるが、そうでないとゲームオーバー（失敗）というものである（図 1）。太郎君は何度ゲームをプレイしても、ゲームをクリアーすることができないので、ひょっとしてこのゲームにはバグがあり、クリアーする選択肢の組み合わせはそも

[1] 一部の大学研究者がそれに加担しているのはとても信じられないことである。

[2] ここで、問題としては、YES か NO かの 1 ビットで回答することのできる問題に限定する。このような問題は判定問題と呼ばれる。計算量理論においては判定問題を考えるのが標準的である。

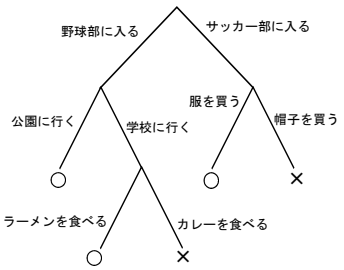

図１　シミュレーションゲームの選択肢のパターンの例。○はゲームクリア、×はゲームオーバーを意味する。

そも存在しないのではないかと疑い始めた。そこで、太郎君は次のような問題を解く必要に迫られた：このゲームにはクリアーとなる選択肢の組み合わせが少なくとも一つ存在するか、もしくは全く存在しないか？どちらか判定せよ。

仮に、この問題をクリアー問題と呼ぶことにしよう。どうすればクリアー問題が解けるだろうか。一つの方法は全ての選択肢の組み合わせパターンをしらみつぶしに調べる方法である。もちろん、これはうまくいかない。なぜならば、全ての組み合わせパターンの総数は指数的に爆発するからである。全ての組み合わせパターンをしらみつぶしに調べるというのは、物理的には、決定的古典ダイナミクスに基づく計算機で問題を解く方法の一つの例である。つまり、計算機が次にどの状態に遷移するかが、現在の計算機の状態から一意に決定されるような計算方法である。決定的古典ダイナミクスに基づく計算機で（入力サイズの）多項式時間で解ける問題の集合は P と呼ばれている。しらみつぶし以外にも何かもっと賢い方法があるかもしれないが、今のところクリアー問題が P に入るとは思われていない。

古典物理には決定的なダイナミクスだけでなく確率的なダイナミクスも存在する。確率的古典ダイナミクスに基づく計算機を考えたらどうだろうか？つまり、計算機の次の状態への遷移が現在の状態から一意に決まるのではなく、コインを振って、その結果も使って次の状態への遷移が決定されるような計算を考えるのである。このような、確率的古典計算ならクリアー問題を解けるように思うかもしれないが、やはりうまくいかない。実際、例えば、ランダムに選択肢を選んだとしても、もしクリアーする選択肢の組み合わせが一つしか存在しない場合、クリアーする確率は指数的に小さいため、十分高い確率でクリアーを得るためには結局計算を指数回繰り返さないといけない。古典の確率的ダイナミクスに基づく計算機で多項式時間で（十分高い成功確率で）解ける問題の集合は BPP と呼ばれている。将来何かものすごいアルゴリズムが見つかる可能性も否定できないが、今のところ、クリアー問題は BPP に入るとは思われていない。

「クリアー問題が解けないのは、古典論に基づく計算機を考えているからだ。自然界を記述する究極の理論は古典論ではなくて量子論である。量子論に基づいた計算機なら解けるはずだ。」と思うかもしれない。実際、よく知られているように、量子論においては、異なる状態の重ね合わせを作ることが可能である。したがって、全てのパターンの重ね合わせを作って同時に処理すれば一発で問題が解けるのではないだろうか、と思うかもしれない。しかし、これでもうまくいかない。なぜなら、重ね合わせをつくっても、それぞれの状態の確率振幅は指数的に小さいため、測定したら結局一つの状態がでる確率は指数的に小さい。また、これでは、確率的に選択肢を選ぶ古典の方法と何も違わない。

量子論においては、重ね合わせを作るだけでなく、重ね合わせた状態を互いに干渉させて打ち消すことが可能である。都合の悪い状態同士をうまく打ち消して、良い状態だけ残すようにすればいいのではないだろうか。実際、そのようにうまく量子的干渉を利用することにより、高速に計算できる量子アルゴリズムが見つかっている。しかしながら、そのようにうまくいくのは問題が持っている特別な構造をたまたま上手に利用できる場合だけであり、一般には、どうやって打ち消していいかわからず高速化できないのが現状である。実際、問題の構造を全く使えないようなブラックボックスの状況でやる場合は、量子でも指数時間必要であることがすでに数学的に証明されている[2, 3]。

このように、クリアー問題は量子計算機でも解けないだろうと思われている。ではどんな計算機なら解けるのだろうか？NP マシンという架空のマシンを考えてみよう。これはどういうものかというと、「学校に行く or 公園に行く」みたいな２択にさしかかると、二つの「並行宇宙」にぶわーっと分離することができ、それぞれの並行宇宙でさらに計算を進めることができるようなマシンである。（計算機科学においては、このように並行宇宙に分かれることを非決定性遷移 (non-deterministic transition) という。NP というのは Non-deterministic Polynomial-time の略である。Non Polynomial ではない。）２択にさしかかるたびに並行宇宙に分離するので、最終的に指数個の並行宇宙に分かれる。そしてこのマシンは、これら指数個の並行宇宙のうちどれか一つでもクリアーにたどり着いたら、全体として「クリアーする選択肢の組み合わせは存在する」という結果を出力し、もし全ての並行宇宙でクリアーできなかったら、全体として「クリアーする選択肢の組み合わせは存在しない」という結果を出力する。明らかに、この NP マシンはクリアー問題を解くことができる。しかし、この NP マシンというのはどの並行宇宙も確率１で実現できるということになってしまっているので、物理の確率保存則（全ての事象の起こる確率の和は１）を破っており、明らかに物理的ではないマシンである。逆に言うと、このような恐ろしく非物

理的な架空のマシンを持ち出してこない限り、クリアー問題をどうやって解いていいかさっぱり分からないのである。

NP マシンで（入力サイズの）多項式時間で解くことのできる問題の集合は NP と呼ばれている。計算機科学においては、NP は BQP に含まれないだろう、と信じられており、それを示唆する多くの理論的結果がでている。物理学者の視点からみてもそれは非常にリーズナブルである。なぜならば、上記で述べたように、NP マシンは恐ろしく非物理的なマシンである。一方で、量子計算機は物理理論である量子論に従った「ものすごく物理的な」マシンである。したがって、普通の物理学者であれば、量子計算機が NP マシンをシミュレートできるとは思わないだろう[3]。

4. P ≠ PSPACE の壁

ここまでは、量子計算が出来ないこと、出来ないと思われていること、について述べてきた。ここからは、量子計算が出来ることについて説明していく。量子計算は古典計算より「速い」と思われているわけだが、正確にはどういう意味なのだろうか。

計算量理論の「標準的」な意味では、量子計算が古典計算より速いというのは、つまり、BPP ≠ BQP ということである。これは実はまだ証明されていない。それどころか、これを示すのは恐ろしく難しいだろうと考えられている。というのは、これまでの説明から明らかなように P ⊆ BPP ⊆ BQP ⊆ PSPACE である。（実際、決定的古典計算は確率的古典計算の特殊な場合なので P ⊆ BPP であるし、確率的古典計算は量子計算の特殊な場合なので BPP ⊆ BQP である。さらに、BQP ⊆ PSPACE であることはすでに見た。）したがって、もし BPP ≠ BQP が証明されると、P ≠ PSPACE も証明される。ところが、P ≠ PSPACE は実は計算機科学における大未解決問題である。したがって、BPP ≠ BQP というのはそんなに簡単には証明できないだろうと信じられている。

5. 二つのアプローチ

とはいうものの、これまで、量子のほうが古典より高速であることを示唆する結果が大量に得られている。それらは、二つのタイプに分類することができる。

まず一つ目のタイプの代表例は素因数分解である。素因数分解は古典では遅いが、量子ではショアーのアルゴリズムを使えば速く解けるというのは非常に有名である。しかし、ここでいう「古典では遅い」というのは、「古典では絶対速くできません」という数学的証明があるということではなく、単に「今のところ誰も古典で高速に解く方法を知りません」というだけのものである。したがって、原理的には、明日にでも誰かが古典の高速な素因数分解アルゴリズムを発見してしまう恐れがある。そうなってしまってはもう素因数分解は量子の古典に対する優位性を示す例では無くなってしまう。

実際、最近そういう事例が起きた。顧客の購買データからおすすめ商品を見つけてくれる量子機械学習のアルゴリズムがあり、古典より速いため注目を集めていたが、つい先日、米国の１８歳の学部生が古典の高速アルゴリズムを発見してしまった[4]。このように、古典の現在知られているベストのアルゴリズムと比較して量子のほうが速い、ということを示すタイプの例は他にも量子シミュレーションなど多くあるが、このタイプは、将来、古典の高速アルゴリズムが見つかり、量子の優位性が覆されてしまうという危険がある。

もう一つのタイプはグローバーの検索アルゴリズムに代表されるタイプである。こちらは、上記で述べた一つ目のタイプと異なり、古典の上限が数学的に証明できる。（例えば、グローバーが古典より速いというのは、ありとあらゆる古典と比べて速いという数学的証明が存在する。）しかしながら、このタイプの場合、実時間を見ているのではなく、サブルーチンを呼ぶ回数しか見ていない。つまり、計算のある部分をサブルーチンとして考え、何回サブルーチンを呼んだかのみを数えた時に、量子のほうが古典よりも少ない、ということを示すのである。このように、サブルーチンの回数だけ見るのは query complexity と呼ばれ、計算量理論においてはスタンダードなアプローチであり、いろんなことが数学的にきっちり証明できるというメリットがある。しかしながら、サブルーチンを呼ぶ回数しか見ていないので、実時間でどうなるかについては分からないというデメリットがある。

6. 第三のアプローチ: 量子スプレマシー

このように、量子高速性を示す結果には、

1. 古典の現在のベストのアルゴリズムと比較して量子のほうが高速であることを示すタイプ
2. サブルーチンを呼ぶ回数を数えた時に量子のほうが古典より少なくて済むことを示すタイプ

の 2 種類があり、それぞれにデメリットがあることを見た。最近、それらに次ぐ第三の新しいアプローチとして、量子スプレマシー（量子超越性）というものが注目を集めている。最後にこれについて説明しよう。

量子スプレマシーには二つのメリットがある。まず、一つ目は、量子高速性が強力な基盤で証明される点である。前節で述べたように、素因数分解のように、現在知られてい

[3]「NP は BQP に含まれない」という数学的な証明があるわけではないので、ひょっとしたら将来超大革命が起きて、NP 完全問題を解ける量子アルゴリズムが見つかる可能性は排除できない。しかしながら、「量子計算機が NP 完全を解ける」という主張は、イメージとしては、物理の学界において「熱力学第二法則が間違っている」とか「相対論が間違っている」とか主張するような、普通はトンデモ扱いされる類の主張である。

る古典のベストと比較する場合、古典のベストが将来アップデートされる恐れがある。量子スプレマシーでは、「もし量子計算が古典計算で効率的にシミュレートできたら多項式階層が崩壊する」ということを証明する[4]。多項式階層というのは P、NP の関係を一般化したものであり、P=NP が信じられていないように、多項式階層の崩壊というのも起こらないだろうと計算機科学においては強く信じられている。したがって、多項式階層が崩壊しないと考えるなら、量子計算は古典計算で効率的にシミュレートできないのである。このように、古典に対する量子の優位性が古典計算量理論の強力な基盤で証明されるという点が量子スプレマシーの一つ目のメリットである。

量子スプレマシーのもう一つのメリットは「弱い」量子計算機であっても古典に対する優位性がデモンストレートできる点である。量子計算の研究者の究極のゴールの一つは、「量子ビット好きなだけ使い放題、任意の量子アルゴリズムが実現可能、量子誤り訂正も完璧にできる」という究極の量子計算機を実現することである。もちろん、それはすぐにできる話ではない。それどころか、素因数分解ですらそれほど簡単ではない。例えば、1024 ビットの素因数分解は現在の古典計算機ではできないだろうといわれているが、それを量子計算機でやる場合、2000 個の量子ビットと 10^{11} 個の量子ゲートが必要であるといわれている[5]。そこで、ひとまずのゴールとして、近い将来に実現できそうな「弱い」量子計算機で古典に対する優位性をデモンストレートしよう、ということを研究者は現在目指している。量子スプレマシーは、そのような「弱い」量子計算機であっても、古典に対する優位性を示すことができるという重要なメリットがあるため、実験家からも注目を集めている。例えば、ゲートがランダムに作用するような量子回路は汎用ではないが、多項式階層が崩壊しないかぎり古典でシミュレートできないことが証明されており[5)]、現在 Google が実現を目指している。

そのような「弱い」量子計算機の例として古くから知られているものに one-clean qubit モデルがある[6)]。通常の量子計算においては純粋状態 $|0\rangle$ を好きなだけ初期状態として使うことができるが、この one-clean qubit モデルは $|0\rangle$ を一個しか使えず、他は全て完全混合状態 $\frac{1}{2}(|0\rangle\langle 0|+|1\rangle\langle 1|)$ である。もともとは NMR 量子計算の数理モデルとして提案された[6)]。一見すると古典計算機で効率的にシミュレートできそうに見えるが、結び目不変量である Jones 多項式の計算等を古典のベストのアルゴリズムより高速にできることが知られているため、古典よりは多少強いモデルであろうと信じられていた。しかし、これは最初に述べたように、将来古典の高速な Jones 多項式計算アルゴリズムが発見されてしまい、one-clean qubit モデルの量子優位性が覆される恐れがあるという点で、それほど強力な基盤とは言えない。この one-clean qubit モデルについても、もし古典計算機で効率的にシミュレートできたら多項式階層が崩壊することが証明されている[7)]。

量子スプレマシーは古典に対する優位性の証明を最優先しているため、他の点を犠牲にしている。特に、確率分布のサンプルを考えているため、何か有用な問題が解けるかどうか、という点については良くわかっていない。これは今後の重要な課題である。

7. おわりに

量子計算というのは、量子論で許されるありとあらゆる操作ができるような多体系では何ができて何ができないだろう、ということを考えるれっきとした量子多体物理である[6]。そして、そのような操作が実際に実験室で実現しつつあるのである。また、量子計算で得られた結果や概念は素粒子、宇宙、物性、統計物理等にも近年輸出され、新しい成果を多く生み出している。日本の量子計算は海外にかなりの遅れをとっている。今後、国内の優秀な理論物理の若手がどんどんこの分野に参入して、日本の量子計算のレベルを押し上げてくれることを非常に強く期待している。

参考文献

1) S. Arora and B. Barak, Computational Complexity: A Modern Approach. Cambridge University Press, 2009.
2) C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, Strengths and Weaknesses of Quantum Computing. SIAM J. Comput. **26**, 1510-1523 (1997).
3) R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf, Quantum Lower Bounds by Polynomials. Journal of the ACM **48**, 778 (2001).
4) E. Tang, A quantum-inspired classical algorithm for recommendation systems. arXiv:1807.04271
5) A. Bouland, B. Fefferman, C. Nirkhe, and U. Vazirani, Quantum supremacy and the complexity of random circuit sampling. arXiv:1803.04402
6) E. Knill and R. Laflamme, Power of One Bit of Quantum Information. Phys. Rev. Lett. **81**, 5672 (1998).
7) T. Morimae, K. Fujii, and J. F. Fitzsimons, Hardness of Classically Simulating the One-Clean-Qubit Model. Phys. Rev. Lett. **112**, 130502 (2014).

(2018 年 10 月 15 日原稿受付)

[4] シミュレートの意味は、出力確率分布をある精度でサンプルする、という意味である。

[5] 量子誤り訂正等も考えるとさらに必要になる。

[6] 海外ではすでに、量子情報というのは一つの確立した物理の一分野として認識されており、多くの教員や研究グループが存在するが、日本ではまだそもそも「量子計算（量子情報）は物理である」という認識すら薄いように見える。