なぜ９０量子ビットなのか

～３０年の基礎研究から量子スプレマシーへ～

２０１８年8月2日

海外では、量子計算はすでに３０年以上の研究の歴史があります。その間の彼らの努力により多くの理論的結果が得られてきました。それらにより、現在では、「量子計算が古典計算より速いことは理論的には確実」とほぼ全ての研究者が信じているといってもよいのではないでしょうか。

最近、量子スプレマシーという言葉をよく聞きますが、これはいきなり湧いて出てきたよく分からないものではなく、その３０年の歴史の中で行われてきた基礎研究の延長線上に、自然な流れで生まれてきたものなのです。(つまり彼らは３０年やってきた基礎研究をいまも粛々と続けているだけなのです。そのあたりに注意しないと、お祭り騒ぎにのせられて、彼らに次の３０年のための資金を提供しただけで、気がついたら自分のところには何も残らず終わった、ということにもなりかねません。)

最近よく聞くのは、「９０量子ビットできれば古典でシミュレート不可能な領域に！」というものです。なぜ９０量子ビットなのでしょうか。ちょっと考えると不思議です。「量子計算機は、どんなに時間をかけてもいいなら、古典計算機でシミュレートできるはずじゃないか。なんで古典シミュレートできない領域とかいえるの？」と思う人がいるでしょう。あるいは、計算機科学の素養のある方なら、「計算量理論は普通は漸近的な議論（問題のサイズを大きくしていったときに計算時間がどうスケールするか）なのに、なんで具体的なキュービットの個数について何か言えるの？」と思う人もいるでしょう。

ここでは、３０年間に得られてきた量子高速性証明について簡単にまとめ、それがどう「９０量子ビットの量子スプレマシー」につながるのか説明します。

１．P≠PSPACE の壁

そもそも、量子計算が古典計算より速いことを証明するにはどうしたらよいでしょうか？量子計算機では簡単に解けるが、古典計算機では解くのにものすごく時間がかかる問題を一つ見つければよいのです。問題といってもいろいろありますが、計算量理論の分野では判

定問題というものを考えるのが標準的です。(計算量理論というのは理論計算機科学の中の一つの分野であり、問題を解くのにどのくらいのリソース（時間、メモリ等）が必要かということを研究する学問です。）判定問題というのは YES か NO で答えることのできる問題です。例えば、「１＋１は？」という問題は YES、NO で答えることができませんので判定問題ではありませんが、「１＋１は３より大きいか？」という問題は NO と答えることができますので判定問題です。もし、量子計算機では速く解けるが古典計算機では解くのに時間がかかるような判定問題が一つ見つかると、「計算量理論の標準的な定義において、量子のほうが古典より速いことが決定的に証明された」ということができます。

しかし残念ながら、そのような問題はまだ見つかっていません。というか、そのような問題を見つけるのは恐ろしく難しいだろうと考えられています。というのも、もしそのような問題が見つかってしまうと、P≠PSPACE という古典計算量理論における大未解決問題を証明できてしまうからです。したがって、「計算量理論の標準的な定義」で量子が古典より速いことを証明するのはものすごく困難だろうと研究者たちは考えています。

２．古典のベストより速い

ここで、あれ？ショアーの素因数分解アルゴリズムは？と思った人もいるかもしれません。素因数分解はたしかに「量子では速く解けるが古典では速く解けない例」として有名ですが、ここでいう「古典で速く解けない」というのは、「古典で速く解けないことが数学的に証明されている」というものではなく、単に、「今のところ誰も古典で速く解く方法を知らない」というだけのものです。つまり、単に、現在の古典のベストに量子が勝っているというだけのものです。したがって、将来誰かが古典の高速素因数分解アルゴリズムを見つけてしまう恐れはあります。(実際、客の好みにあったおすすめ商品を見つける recommendation system という量子機械学習アルゴリズムがあり、以前は古典のベストのアルゴリズムより高速でしたが、つい先日、古典の高速アルゴリズムが見つかってしまいました[1]。なんとそれを見つけたのは学部生です！）

そうはいうものの、素因数分解はとても有名な問題ですし、より高速なアルゴリズムを見つけるのは難しそうです。そこで、素因数分解を量子計算機が高速に解ける事実はやはり、量子計算が古典計算より速いことの強力な証拠であると皆考えています。

３．サブルーチンを呼ぶ回数

量子計算には、ショアーの素因数分解アルゴリズムのほかに、グローバーの検索アルゴリズムというものがあることをご存知の人も多いでしょう。グローバーの検索アルゴリズムは、

素因数分解と異なり、すでに古典のどんなアルゴリズムよりも量子のほうが速いということが数学的に証明されています。しかしながら、実はグローバーの場合、実時間を計っているのではなくて、サブルーチンを呼ぶ回数だけ見ています。つまり、計算の一部はサブルーチンとして扱い、サブルーチンの部分は１ステップで実現できるとして、サブルーチンを何回呼ぶかで見た時に、量子のほうが古典より少ない回数で済むことを示しているのです。もちろん、実際にはサブルーチンの部分は１ステップでできるわけがなく、その個所でも時間がかかるでしょうし、全体の実時間で見た時に本当に量子のほうが古典より速いかどうかは分かりません。しかしながら、このようにサブルーチンを呼ぶ回数だけ見るのは計算量理論においてはスタンダードな方法ですし、古典の上限についてきっちり証明しやすいというメリットもあり、グローバーのアルゴリズムも、量子が古典より速いことを支持する強力な結果だと考えられています。

４．量子スプレマシー

このように、量子計算が古典計算より高速であることを示す研究はショアーのように古典のベストに勝っていることを示すタイプと、グローバーのようにサブルーチンを呼ぶ回数で勝っていることを示すタイプの２種類があることを見てきました。それらには次の二つの欠点があります。

１．古典のベストに勝つことを示すタイプだと、古典のベストがアップデートされる恐れがある。したがって、もっと「安全な」基盤で量子高速性を証明したい。

２．実現が容易でない。（例えば、現在の古典計算機でできないとされる１０２４ビットの素因数分解をするには２０００量子ビットと 10^11 個の量子ゲートがいるそうです[2]。）したがって、なにかもっと近い将来に実現しやすそうなもので量子高速性を証明したい。

この２つの問題点に応えるべく、最近、盛んに研究されているのが、第三のアプローチである、「量子スプレマシー」です。もっとも古い論文は実は 2004 年にでていますが[3]、2011 年頃から研究が爆発的に盛んになったように見えます。この量子スプレマシーのアイデアは、「量子が古典より速いか？という問題を古典計算量理論の問題に帰着してしまう」というものです。つまり、「もし量子が古典より速くないなら、P=NP が成り立つ」というようなことを示すのです。P=NP が成り立つだろうとは信じられていませんので、これは量子が古典より速いことを示唆する結果となります。また、P=NP が成り立つと、現在の計算量理論はある意味、根本から崩壊しますから、そんなことになったら、そもそも量子計算が古典計算より速いか、なんてことはもうどうでもよくなってしまいます。「古典では素因数分解は高速に解けない」という仮定よりも、「P≠NP である」という仮定のほうがはるかに強

力な基盤ですから、量子高速性を従来よりもはるかに強力な基盤で証明することができるわけです。量子計算の歴史は古典計算機科学の歴史にくらべてまだ浅く、研究者の数も圧倒的に少ないので、よくわかっていないことだらけです。そこで量子計算についての何か「危険」な仮定を置くのではなく、全て古典計算量理論の「安全」な仮定だけで完結させてしまおう、ということなのです。

上記の説明では分かりやすさのために P＝NP と書きましたが、実際は、P=NP ではなく、P vs NP の関係を一般化した「多項式階層」というものが崩壊する、という結果に帰着させています。（P=NP に帰着できるかどうかは分かっていません。）計算量理論の分野においては、P≠NP 同様、多項式階層は崩壊しないだろうと非常に強く信じられています。したがって、多項式階層が崩壊しないと信じるならば、量子計算は古典計算より高速であることが保証されることになります。

量子スプレマシーにはもう一つ大きなメリットがあります。それは、フルの完全な汎用量子計算機を用意しなくてもよい点です。例えば、Knill-Laflamme-Milburn という有名な結果により、光子の間に相互作用を作れるならばユニバーサル量子計算ができることは分かっていますが、相互作用を作るのは難しいそうです。ところが、相互作用のない光子を使った量子計算でも、量子スプレマシーを証明することができます[4]。（つまり、相互作用無し光子量子計算機が古典でシミュレートできたら多項式階層が崩壊する。）また、交換するゲートのみからなるモデル[5]や、ゲートがランダムにかかるようなモデル[6]についても同様です。さらに、one-clean-qubit model と呼ばれる、きれいな量子ビットが一つしか無く、他は完全にデコヒアーしてしまったような量子ビットしか使えないような量子計算モデルも同様です[7]。これらの量子計算は、素因数分解等に比べるとかなりシンプルな量子回路でよいので、実験的な実現も容易なのではと期待されています。実際、Google はランダム回路を実現しようとしているようです。

５．なぜ９０量子ビット？

このように、「多項式階層が崩壊しない」という強力な計算量理論の基盤に基づいて量子高速性を証明することができます。しかしながら、この結果が禁じているのは、「量子計算機を古典計算機で多項式時間でシミュレートする」ことです。したがって、例えば、n^loglogloglog(n)時間なら、多項式階層を崩壊させずに古典シミュレートできるかもしれません。

すきなだけ量子ビットを大量に使えるならこういう漸近的な議論でもいいですが、そんなことは今すぐには無理なので、近い将来に目指すめやすとして何か基準が欲しいところで

す。そこで、多項式階層が崩壊しないというのよりもさらに強い仮定を設けることにより、具体的にこのくらいの量子ビットがあれば、古典でシミュレートするのは「実質不可能」だろう、という領域を見極めようとする論文が最近でています。例えば最近の論文[8]では、これまでの「多項式階層は崩壊しない」という仮定ではなく、「degree-3 polynomial non-deterministic strong exponential time hypothesis」という仮定をすることにより、交換するゲートのみからなるモデルの場合、９０量子ビットあれば、「最新のスパコンでシミュレートするのに１００年かかる」という見積を出しています。

このように、量子スプレマシーというのは多くのメリットがあるわけですが、一方で、判定問題ではなくサンプリング問題を考えており、どういう応用性があるかまだよくわからない、高い精度でサンプルすることが要求されるかあるいは追加の仮定が必要となる、といったような、デメリットもあるため、まだまだ不満点だらけであり、現在も世界中で研究者らが頑張って研究を進めているところです。しかしながら、量子スプレマシーは

１．量子計算 VS 古典計算という構図を、完全に古典計算量理論の問題に置き換えることにより、非常に「安全な」議論を可能にした。

２．とてもシンプルな量子計算モデルを使って量子優越性を示すことができるようになった。

というこれまでにない二つの点を成し遂げた、全く新しい第三のアプローチであり、量子計算理論の歴史における重要なマイルストーンの一つです。

６．まとめ

以上まとめると、量子計算が古典計算より速いことを示す研究は

１．現在知られている古典のベストより速いことを示す（ショアー型）
２．サブルーチンを呼ぶ回数が古典より少ないことを示す（グローバー型）
３．古典計算量理論の仮定に帰着させる（量子スプレマシー）

の３つのタイプに分けることができます。量子計算の３０年以上の歴史の間、上記の３つに分類されるタイプの結果が無数に得られてきており、それらのおかげで、今では、量子計算は古典計算より速いと強く信じられているのです。（ちなみに、以上の話は全て、いわゆるゲート型の話であり、量子アニーリングについてはあてはまりません。量子アニーリングについては、古典より高速であることを示唆する証拠はまだでていません。）

[1] Tang, arXiv:1807.04271
[2] Roetteler, Naehring, Svore, and Lauter, arXiv:1706.06752
[3] Terhal and DiVincenzo, Quant. Inf. Comput. 4, 134 (2004)
[4] Aaronson and Arkhipov, STOC 2011
[5] Bremner, Jozsa, and Shepherd, Proc. R. Soc. A 467, 459 (2011)
[6] Bouland, Fefferman, Nirkhe, and Vazirani, arXiv:1803.04402
[7] Morimae, Fujii, and Fitzsimons, Phys. Rev. Lett. 112, 130502 (2014)
[8] Dalzell, Harrow, Koh, and La Placa, arXiv:1805.05224