量子計算の指数時間古典シミレーション

平成 31 年 4 月 11 日

量子計算はもちろん古典計算機では効率的にシミレートできないと信じられており、だからこそ量子計算は存在意義があるわけですが、現在実験的実現が目指されている小〜中規模サイズの量子計算機の場合、スパコン等で頑張ってシミレートできてしまいます。古典計算機で量子計算機をシミレートすることにより、実験で作った量子計算機の検証や性能評価ができますし、また、量子計算と古典計算の境界を探る上でも、量子計算機がどのくらい古典に「負ける」か、ということを知るのは重要です。さらに、量子計算というのは量子多体系のダイナミクスにすぎないので、量子計算機を古典計算機でシミレートするアルゴリズムを開発していくと、その過程で、物性物理や統計物理等の量子多体系の数値シミレーションの新しいアルゴリズムのヒントが得られるかもしれません。つまり、これまでは物性系や高分子系等が数値シミレーションの対象だったわけですが、量子計算機というのも、数値シミレーションの面白い対象なのです。このような理由から、近年、量子計算の古典シミレーションについて多くの研究が成されています。[1]特に、これから説明するような stabilizer rank アルゴリズム [1, 2] をはじめとする、いろいろな指数時間古典シミレーションの新しいアルゴリズムが提案されています。

クリフォードゲート

$$\begin{aligned} H &\equiv |+\rangle\langle 0| + |-\rangle\langle 1|, \\ S &\equiv |0\rangle\langle 0| + i|1\rangle\langle 1|, \\ CZ &\equiv |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z \end{aligned}$$

と T ゲート

$$T \equiv |0\rangle\langle 0| + e^{\frac{i\pi}{4}}|1\rangle\langle 1|$$

[1]そもそも、量子計算の古典シミレートの研究は Gottesman-Knill やマッチゲート等、量子計算の初期のころからありますが、基本的に一般的抽象的な議論が多かったです。また、多項式時間シミレーションを考えるものが多かったです。近年、具体的な NISQ マシンができつつあるということもあり、もう少し具体的な構造やノイズモデルを仮定したマシンの古典シミレーションをするアルゴリズムがいろいろ考えられています。また、そもそもマシンが実在しなかった時代には指数時間シミレーションというのはあまり意味がないと考えられていましたが、小〜中規模マシンが登場しつつある今、指数時間シミレーションも正当化され、現在研究が非常にアクティブで多くの新しい結果が出てきています。

はユニバーサルゲートセットです。つまり、これらを組み合わせれば任意の量子計算が可能です。一方で、Gottesman-Knill の定理 [3, 4] でよく知られているように、クリフォードゲートだけの量子計算は古典で効率的にシミレート可能です。[2]ということはある意味、T ゲートが量子高速化において重要な役割を果たしているリソースであると考えることができます。逆に考えると、クリフォードと T からなる量子計算を古典計算でシミレートしようとした場合、T ゲートの個数が増えれば増えるほど大変になる、といえます。今、クリフォードゲートと t 個の T ゲートからなる量子回路を考えましょう。これを古典シミレートしようとしたとき、シミレートに必要な計算時間は t に対してどうスケールするでしょうか？

それを考えるために、T-gadget という方法を使って、回路の T ゲートを取り除きます。magic state と呼ばれる状態

$$|T\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + e^{\frac{i\pi}{4}}|1\rangle)$$

を定義しましょう。ある N-qubit 量子状態 $|\psi\rangle$ の第一量子ビットに T ゲートを作用させたいとします。magic state を一つ「消費」すれば、次のような方法でクリフォードゲートのみで T ゲートを実現できます。

1. magic state を $|\psi\rangle$ にくっつける：

$$|\psi\rangle \otimes |T\rangle = (\alpha|0\rangle \otimes |\psi_1\rangle + \beta|1\rangle \otimes |\psi_2\rangle) \otimes (|0\rangle + e^{\frac{i\pi}{4}}|1\rangle)$$

ここで、α, β はある複素数。$|\psi_1\rangle, |\psi_2\rangle$ はある N-qubit 状態。

2. $|\psi\rangle$ の第一量子ビットと magic state に CNOT をかける：

$$\alpha|0\rangle|\psi_1\rangle|0\rangle + \alpha e^{\frac{i\pi}{4}}|0\rangle|\psi_1\rangle|1\rangle + \beta|1\rangle|\psi_2\rangle|1\rangle + \beta e^{\frac{i\pi}{4}}|1\rangle|\psi_2\rangle|0\rangle$$

3. magic state を $|0\rangle$ に射影する：

$$\alpha|0\rangle|\psi_1\rangle|0\rangle + \beta e^{\frac{i\pi}{4}}|1\rangle|\psi_2\rangle|0\rangle = (T \otimes I^{\otimes N-1})|\psi\rangle \otimes |0\rangle$$

つまり、T ゲートを一つ実現したいときは、magic state を一つもってきてクリフォードゲートでエンタングルメントを作り、最後に magic state を測定して消費すればよいのです。

したがって、いま、クリフォードと t 個の T ゲートからなる N-qubit 量子回路を U とするとき、あるクリフォードゲートのみからなる量子回路 V で

$$\langle 0^N|U|0^N\rangle = \sqrt{2^t}\langle 0^{N+t}|V(|0^N\rangle \otimes |T\rangle^{\otimes t}) \tag{1}$$

[2]古典シミレートの定義にはいろいろなものがありますが、この原稿では簡単のため、一貫して最も簡単な strong simulation というものを考えます。これは、量子計算機がある値を出す確率を計算せよ、というものです。要するに、N-qubit 量子回路 U が与えられたとき、$\langle 0^N|U|0^N\rangle$ の値を計算しろ、ということです。他によく考えられるものとして、weak simulation というものがあります。これは、量子計算機が出す確率分布をサンプルしろ、というものです。weak simulation の結果については原論文等を参照してください。

を満たすものを t の多項式時間で作ることが出来ます。今、$|T\rangle^{\otimes t}$ が

$$|T\rangle^{\otimes t} = \sum_{i=1}^{k} c_i |\phi_i\rangle \tag{2}$$

と書けるとします。ここで、c_i はある複素係数、$|\phi_i\rangle$ はスタビライザー状態とします。（スタビライザー状態とは、クリフォードゲートのみからなるある量子回路 C を用いて $C|0^t\rangle$ と書けるような状態のことです。）すると、式 (2) を式 (1) に代入すると

$$\langle 0^N|U|0^N\rangle = \sqrt{2^t} \sum_{i=1}^{k} c_i \langle 0^{N+t}|V(|0^N\rangle \otimes |\phi_i\rangle)$$

となります。$\langle 0^{N+t}|V(|0^N\rangle \otimes |\phi_i\rangle)$ の部分は Gottesman-Knill の定理により $N+t$ の多項式時間で計算できます。したがって、各 i に対しそれを計算し、それらの和（k 個ある）を計算すれば $\langle 0^N|U|0^N\rangle$ が求まるので、計算時間は全体で $poly(N+t)k$ となります。

k はどのくらいの大きさになるのでしょうか？$|T\rangle^{\otimes t}$ は例えば計算基底で展開すると

$$|T\rangle^{\otimes t} = \frac{1}{\sqrt{2^t}} \sum_{x\in\{0,1\}^t} e^{\frac{i\pi|x|}{4}} |x\rangle$$

となりますので、$k = 2^t$ であり、したがって、$2^t poly(N+t) \sim 2^t$ 時間で量子計算がシミレートできることになります。これはある意味、brute force に計算する方法といえるでしょう。[3]

$|T\rangle^{\otimes t}$ をもっと賢い方法で分解して、k が小さくできれば、より高速に古典シミレートできるわけです。k を減らすことはできるのでしょうか？論文 [2] において、$k \leq 2^{0.468t}$ となるようなノントリビアルな $|T\rangle^{\otimes t}$ の分解方法が提案されました。したがって、クリフォードと t 個の T からなる量子回路は $\sim 2^{0.468t}$ 時間で古典シミレートできることになります。これは brute force の方法の計算時間 $\sim 2^t$ と比べると指数時間ではあるものの、ちょっと高速になっています。

もっと小さい k が見つかれば、より高速化できるわけです。k をどこまで小さくできるでしょうか？それを調べるために、stabilizer rank [2, 5] という量を定義します。t-qubit 状態 $|\psi\rangle$ の stabilizer rank $\chi(|\psi\rangle)$ とは、$|\psi\rangle$ を

$$|\psi\rangle = \sum_{i=1}^{k} c_i |\phi_i\rangle$$

[3] Gottesman-Knill の証明を知っている人は、クリフォードはパウリをパウリに移すが、T は X と Y をそれらの和に移すため、T を一回かけると項の数が 2 倍になりえることが分かるでしょう。したがって、T を t 回かけると、項の数が 2^t になりえるので、$\sim 2^t$ 時間かかるわけです。

と書いた時の最小の k です。ただし、c_i は複素数、$|\phi_i\rangle$ はスタビライザー状態です。[4] すると、$\langle 0^N|U|0^N\rangle$ を古典計算機で計算するのに必要な時間の上限は $poly(N+t)\chi(|T\rangle^{\otimes t})$ であるということになります。論文 [2] で示されたのは $\chi(|T\rangle^{\otimes t}) \leq 2^{0.468t}$ ということです。したがって、量子計算が $\sim 2^{0.468t}$ 時間で古典シミレートできることになります。ちなみにこれはどうやって示されたかといいますと、まず $|T\rangle^{\otimes 6}$ が $k=7$ 個のスタビライザー状態の和で書けることを示します。すると、

$$\chi(|T\rangle^{\otimes t}) = \chi(|T\rangle^{\otimes 6\frac{t}{6}}) \leq \chi(|T\rangle^{\otimes 6})^{\frac{t}{6}} \leq 7^{\frac{t}{6}} = 2^{t\frac{\log_2 7}{6}} \simeq 2^{0.468t}$$

となります。

このように、$|T\rangle^{\otimes t}$ の stabilizer rank は、少なくとも $\chi(|T\rangle^{\otimes t}) \leq 2^{0.468t}$ であることは分かっていますが、上記の分解は最適とは限らないので、$\chi(|T\rangle^{\otimes t})$ の真の値がどのくらいかというのはまだ分かっていません。$\chi(|T\rangle^{\otimes t}) = poly(t)$ であると、任意の量子計算が古典計算機で多項式時間でシミレートできてしまいますので、それはなさそうです。今のところ、人々は $\chi(|T\rangle^{\otimes t}) \geq 2^{\Omega(t)}$ だろうと予想しています。これは stabilizer rank conjecture と呼ばれています。最近我々は、もし exponential time hypothesis (ETH) が正しいなら、stabilizer rank conjecture は正しいということを証明しました [6]。[5]ETH 等の何らかの計算量的仮定を仮定しないで unconditional に stabilizer rank conjecture が証明できるかどうかはまだ open です。（unconditional な結果で唯一知られているのは論文 [2] で示された $\chi(|T\rangle^{\otimes t}) \geq \Omega(\sqrt{t})$ というかなり弱い下限のみです。）

もし stabilizer rank conjecture が正しくて $\chi(|T\rangle^{\otimes t}) \geq 2^{\Omega(t)}$ であったとすると、stabilizer rank アルゴリズムを使う場合、シミレーションには $2^{\Omega(t)}$ 時間かかるわけです。しかし、それは、量子計算の古典シミレートに絶対 $2^{\Omega(t)}$ 時間かかるということは意味しません。なぜなら、stabilizer rank アルゴリズムとは全く異なる新しいアルゴリズムが発見されて、量子計算が $2^{o(t)}$ 時間で古典シミレートできる可能性はまだ排除されていないからです。我々は、ETH が正しい限り、どんなアルゴリズムを考えても、$2^{o(t)}$ 時間では古典シミレートできないことを証明しました [6]。[6]

クリフォードゲートは fault-tolerant にやりやすいですが、T ゲートは難しいです。そのため、T ゲートの個数が少ないほどうれしいです。量子回路の形を変形して、T の個数を少なくするような「量子回路 optimization」とい

[4]もともとの定義 [2] では explicit に書いていませんが、i が与えられたとき、c_i と $|\phi_i\rangle$ の記述が $poly(t)$ 時間で計算できる、という条件も必要です。これがないと、non-uniform な古典シミレーションを考える必要があります。

[5]入力 i に対し $c_i, |\phi_i\rangle$ が $poly(t)$ 時間で計算できるという制限のある stabilizer rank です。原論文では explicit にそれを述べてませんが暗黙にそう仮定しているように見える文章がいくつかありますし、もともとの stabilizer rank のモチベーションを考えるとそういう制限を入れるのが自然です。

[6]最初に述べたように、ここでいう古典シミレートは strong simulation です。weak simulation についても ETH の変種を考えることにより $2^{o(t)}$ 時間シミレート不可能性がいえます [6]。また、同じ結果はアリババの量子ラボの人たちも独立に得ています [7]。

うのもいろいろやられています。論文 [6] の結果を使うと、（ETH が正しいなら）どんなに頑張っても $o(t)$ 個までは減らすことができない、ということがいえます。それはなぜかというと、上で述べたように、$2^{o(t)}$ 時間では古典シミレートできないような、クリフォードと t 個の T ゲートからなる量子回路が存在しますが、もしその回路の T ゲートの数を $t' = o(t)$ 個まで減らすことができると、その回路は brute force で $2^{t'} = 2^{o(t)}$ 時間で古典シミレートできるわけですが、それはもともとの回路が $2^{o(t)}$ 時間でシミレートできないという結果と矛盾します。

クリフォードと T の他によく使われるユニバーサルゲートセットとして Toffoli と H があります。Toffoli だけの量子回路は古典回路ですから当然古典計算機でシミレートできます。一方で H が加わるとユニバーサルになるということは、量子高速化には H が利いている、と考えることができます。そこで、Toffoli と h 個の H からなる量子回路の古典シミレートの計算時間が h でどうスケールするか、というのも興味があります。このタイプのスケールは T-スケールに比べるとあまり研究されていないようで、特に先行研究はありませんでした。我々は strong exponential time hypothesis (SETH) が正しいなら、任意の $a > 0$ に対し $2^{(1-a)h}$ 時間では古典シミレートできないことを示しました。[7]クリフォードと T の場合は、2^{bt} 時間の b の値を例えば stabilizer rank アルゴリズムを使うことにより 1 から改善できたわけですが、Toffoli と H の場合はそれができないということが示されており、対照的です。

量子計算の古典シミレーションについては他にも最近いろいろな結果がでています。特に以下の論文は面白いです。

- arXiv:1904.00102
- arXiv:1902.11257
- arXiv:1901.05003
- arXiv:1810.03176

参考文献

[1] S. Bravyi and D. Gosset, Improved classical simulation of quantum circuits dominated by Clifford gates. Phys. Rev. Lett. **116**, 250501 (2016).

[2] S. Bravyi, G. Smith, and J. A. Smolin, Trading classical and quantum computational resources. Phys. Rev. X **6**, 021043 (2016).

[7]こちらも strong simulation です。weak simulation のほうの結果については論文を参照してください。

[3] S. Aaronson and D. Gottesman, Improved simulation of stabilizer circuits. Phys. Rev. A **70**, 052328 (2004).

[4] M. Van den Nest, Classical simulation of quantum computation, the Gottesman-Knill theorem, and slightly beyond. arXiv:0811.0898

[5] S. Bravyi, D. Browne, P. Calpin, E. Campbell, D. Gosset, and M. Howard, Simulation of quantum circuits by low-rank stabilizer decompositions. arXiv:1808.00128

[6] T. Morimae and S. Tamaki, Fine-grained quantum supremacy. arXiv:1901.01637

[7] C. Huang, M. Newman, and M. Szegedy, Explicit lower bounds on strong simulation of quantum circuits in terms of T-gate count. arXiv:1902.04764