ユニバーサルでないが古典計算機より速い量子計算モデル

森前智行

July 12, 2015

量子計算機は本当に古典計算機よりも速いのか、という問いは量子情報・量子計算の分野において最も中心的な問題の一つである。例えば、量子計算機が古典計算機よりも速いと信じられている一つの証拠に、Shor の素因数分解アルゴリズムの存在がある。素因数分解を高速に解く古典アルゴリズムは現在のところ知られていないが、Shor のアルゴリズムを使えば、量子計算機で多項式時間で素因数分解ができてしまう。

しかしながら、素因数分解が古典計算機で効率的に解けないことはまだ証明されていない。将来誰かが高速アルゴリズムを発見するかもしれない。また、素因数分解が BPP(古典確率的計算機で効率的に解ける問題のクラス) に含まれたとしても、なにか計算機科学にとって根本的な仮定が覆される（たとえばある計算量階層の崩壊等）ということが起こる、というようなことは証明されていない。（もっといえば、量子計算機と古典計算機は等価である（BQP=BPP）ということは、起こりえないだろうと思われているにはせよ、P=NP や多項式階層の崩壊が起こらないだろう、というほどには強く信じられていない。）

また、Shor のアルゴリズムを実験的に実現するのはなかなか難しく、大きなサイズの素因数分解はまだ実現されていない。大きなサイズの量子計算を実験的に実現するには、コヒーレンスやエンタングルメントが外界からのノイズにより破壊されてしまうことを防がなければならないが、それは非常に困難な作業である。

また、量子計算の実験において最終ゴールとされているのは、ユニバーサル量子計算機、つまりどんな量子アルゴリズムでも実行できる汎用量子計算機を作ることである。しかし、実験的にユニバーサル量子計算機を作るのは非常に困難な目標である。

何か、もっと他の方法で、“古典計算よりも速い”量子計算をデモンストレートすることはできないのだろうか？ユニバーサル量子計算機でなくても良いから、なにかもうすこし簡単な量子計算モデルで、しかも、それは古典計算機では効率的にシミレートできない、というようなものはないのであろうか？

このようなモチベーションから、近年、ユニバーサルではないが、古典計算機で効率的にシミレートすることが困難であるような量子計算モデルが注目を集めている。

1 DQC1 モデル

そのようなモデルの中で最も有名なものが DQC1 モデル（あるいは one-clean qubit モデル）である。DQC1 は Deterministic Quantum Computation with One quantum bit の略であるが、単に歴史的にこう呼ばれているだけである。これは、NMR 量子計算機のモデルとして Knill と Laflamme により 1998 年に提案され

た [1]。DQC1 モデルは、図 1 に示すように、入力は 1 キュービットのみ純粋状態で他は全て完全混合状態という状態

$$|0\rangle\langle 0| \otimes \frac{I^{\otimes n}}{2^n}$$

である。ただし、$I \equiv |0\rangle\langle 0| + |1\rangle\langle 1|$ は 2 次元単位演算子。任意の多項式サイズの量子ゲートを作用させることができ、最後に 1 キュービットだけ測定を行う。

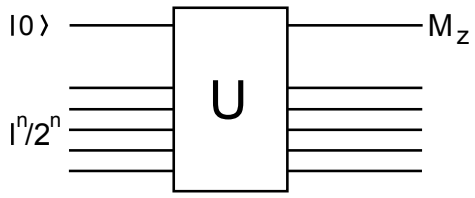

Figure 1: DQC1 モデル

明らかにこのモデルはユニバーサル量子計算機ではなさそうである。実際、リーズナブルな仮定のもとでは、ユニバーサル量子計算が実現できないことが証明されている [2]。(この論文では、DQC1 は NC1 がシミレートできることも触れている。)

それどころか、一見すると、このモデルは古典計算機で効率的にシミレートできそうである。実際、もし入力の 1 キュービットの純粋状態を完全混合状態に取り替えれば、入力は

$$\frac{I^{\otimes n+1}}{2^{n+1}}$$

となるので、任意のユニタリ U に対し

$$U\frac{I^{\otimes n+1}}{2^{n+1}}U^\dagger = \frac{I^{\otimes n+1}}{2^{n+1}}$$

であるので、トリビアルにシミレートできる。

しかし、驚くべきことに、たった一つの純粋状態の存在が、状況を大きく変えるのである。DQC1 モデルは、古典計算機では効率的に解く方法が知られていないいくつかの問題を効率的に解くことができるのである [1]。(例えば、結び目不変量である Jones 多項式の計算 [3] など。) したがって、DQC1 モデルはユニバーサル量子計算機と古典計算機の間に位置する中間的な量子計算モデルと考えられている。

DQC1 モデルは真に古典計算機より速いのだろうか?「古典計算機で効率的に解く方法が知られていない問題を効率的に解くことができる」だけでは、真に古典計算機より速いとは言えない。なぜなら、将来誰かが古典計算機を用いた効率的な解き方を見つけるかもしれないからである。DQC1 モデルが真に古典計算機より速いかどうかは長年の open problem であった。

我々は、DQC1 モデルの k 個の出力キュービットを測定するモデル (DQC1$_k$ モデル) を考え、$k \geq 3$ の場合、出力キュービットの測定結果の確率分布がもし古典計算機で効率的にサンプルできたならば、多項式階層が第 3 レベルで崩壊することを証明した [4]。多項式階層というのは、P、NP を一般化したものであり、崩壊しないだろうと計算機科学の分野では強く信じられている。(BPP=BQP よ

りもはるかに起こらないだろうと信じられている。）したがって、多項式階層が第 3 レベルで崩壊しないと仮定するなら、DQC1$_k$ ($k \geq 3$) モデルは古典計算機で効率的にシミレートできないことになる。この結果は、DQC1 モデルは古典計算機より速いだろうという長年の conjecture にたいし、計算量に基づいて証拠を与えた初めての結果である。

この結果は、ポストセレクトできる DQC1$_k$ モデル (postDQC1$_k$) は $k \geq 3$ のとき、ポストセレクトできる BQP マシン (postBQP) と等価である、すなわち、postDQC1$_k$=postBQP、ということに着目することにより得られた。ポストセレクションとは、量子状態を測定した際に、望みの結果を（たとえそれがどんな小さな確率でも）確率 1 で得ることができる、という架空の能力である。もしポストセレクションができれば、no-signaling を破ったりタイムトラベルができたりするので、ポストセレクションは実際には実現できないと考えられている。(例えば、アリスとボブがベルペアをシェアしているとする。もしアリスがポストセレクションできるなら、アリスは確率 1 でボブのもとに望みの状態を作ることができるので、アリスはボブに情報を伝えることができる。）しかし、もしポストセレクションができたら、と仮定すると、（ポストセレクションできない現実世界についてさえ）いろいろと面白い結果が分かるのである。最も有名な結果は、postBQP=PP というものである [5]。我々の上記の結果は、これと postDQC1$_k$=postBQP ($k \geq 3$) を組み合わせることにより得られた。

postDQC1$_k$=postBQP ($k \geq 3$) が成り立つことは、図 2 の回路で示すことができる。

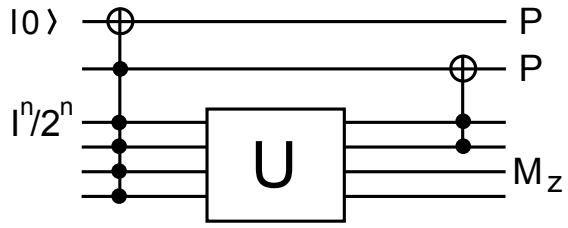

Figure 2: postDQC1$_k$=postBQP ($k \geq 3$) の証明。P はポストセレクションを示す。

この結果は、最近、$k = 1$ かつ多項式階層の第二レベル崩壊、に拡張された [6]。アイデアとしては、NQP を使う、というものである。NQP というのは NP の量子版である（QMA は NP の witness の概念を量子化したのに対し、NQP は NP のパスの概念を量子化したもの。）定義は以下のようである：ある言語 L が NQP に入るとは、ある量子回路が存在し、Yes なら $p > 0$、No なら $p = 0$。ただし、p は量子回路が Yes を出す確率。今、L が NQP に入ると仮定しよう。すると、定義のような量子回路が存在する。その回路を使った、DQC1 回路を構成することができ、それが Yes を出す確率は $\tilde{p} = p(1-p)2^{-n+2}$ となることが示せる。なので、もし、この $\tilde{p}$ をシミレートする古典回路が存在し、その出力確率を q とすると、Yes のとき、$q = \tilde{p} > 0$、No のとき、$q = \tilde{p} = 0$ となるので、これは、L が NP に入ることを意味する。　よって、NQP $\subseteq$ NP となり、NQP = CoC$_=$P であることを使うと、多項式階層の第二階層崩壊がいえる。

2　深さ４の量子回路

Terhal と DiVincenzo は、深さ４の量子回路モデルを考えた [7]。深さ４というのは、同時に作用できる量子ゲートを全てまとめても、４ステップ必要という意味である。

彼女らは、深さ４の量子回路を古典計算機でシミレートするのは非常に困難である（厳密計算は ♯P、近似的サンプリングは多項式階層が第三レベルで崩壊）ということを示した。この結果は、ゲートテレポーテーションと、ポストセレクションという二つのアイデアに基づいている。まず、ゲートテレポーテーション [8] というのは Gottesman と Chuang により提案された方法であり、テレポーテーションを使って、ゲートを回路の途中に「割り込ませる」方法である。例えば、光などの系では相互作用（2 キュービットゲート）は確率的にしか実現できない。したがって、もし光系で普通に量子計算を行ってしまうと、量子計算が成功する確率は p^n となってしまう。ここで、p は 2 キュービットゲートの成功確率、n は 2 キュービットゲートの個数である。$p < 1$ なので、量子計算の成功確率は指数関数的に小さくなってしまう。ところが、ゲートテレポーテーションのアイデアを使うとこれを回避することができる。ゲートを別のところでやっておき、成功したときだけ、テレポーテーションをつかって計算本体にねじ込むのである。こうすれば、2 キュービットゲートが確率的にしか成功しないような場合でも、ほぼ確率 1 で量子計算が成功する。

Terhal と DiVincenzo は、もしポストセレクションできれば任意の量子回路はゲートテレポーテーションを使うと深さ４で書けることを示した。（もちろん、ポストセレクション無しでは任意の量子計算が深さ４で書けない。なぜなら、ゲートテレポーテーションは確率的にしか成功せず、失敗したときは、ゲートに余計な演算がつくため、それを次のステップで修正しなければならないからである。しかし、もし、ポストセレクションできるとすると、常にゲートテレポーテーションを成功させることができるので、深さ４でも任意の量子計算が実行できる。）いま、深さ４の回路を考えよう。その出力のなかには、偶然、ポストセレクトキュービットが望みの結果に測定されているものも含まれている。そして、そのような場合には、計算結果を含んでいるキュービットは、正しい量子計算の結果をエンコードしているはずである。したがって、深さ４の回路の出力を計算するためにはそのようなものも計算しなければならない。しかし、以下に示すように、量子計算の結果の厳密な計算は ♯P であることが知られている。したがって、深さ４の回路の出力の厳密計算は ♯P なのである。

また、近似サンプル不可能性については、postBQP=PP を使う。先ほど述べたように、深さ４の回路はポストセレクトできるならば postBQP ができる。深さ４の回路が解ける問題のクラスを D4 と書くとき、これは postD4=postBQP を意味する。これと、Aaronson の結果 postBQP=PP を使うことにより、もし D4 の出力が古典計算機で効率的にサンプルできたら多項式階層が崩壊することが証明できる。

深さ４の量子回路が古典シミレート不可であることは、ゲートテレポーテーションを使わずに、測定型量子計算を使っても証明できる。実際、図 3 のように、$|0\rangle^{\otimes n}$ から出発して、４ステップで作られた状態を考える。この状態の各キュービットを計算基底で測定するとしよう。もしポストセレクションできるならば、postBQP ができることは明らかである。

最後に、量子計算の出力の厳密計算は ♯P であることの証明。ブール関数 $f : \{0,1\}^n \ni x \to f(x) \in \{0,1\}$ を考えよう。状態

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |f(x)\rangle$$

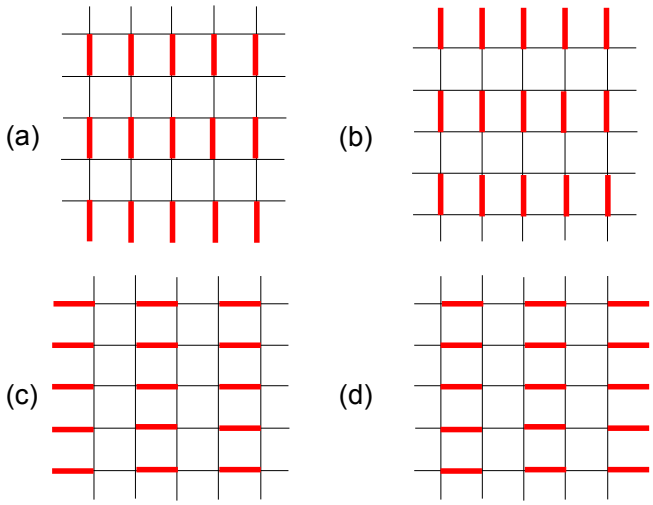

Figure 3: (a) 赤で示したところに $CZ(H \otimes H)$ を作用させる。(b) 赤で示したところに CZ を作用させる。(c) 赤で示したところに CZ を作用させる。(d) 赤で示したところに $(H \otimes H)(e^{i\theta_i Z} \otimes e^{i\theta_j Z})CZ$ を作用させる。

を量子計算機で作り、第二次レジスターを計算基底で測定すると、0 がでる確率は

$$\frac{1}{2^n}\Big(\sum_{x:f(x)=0}\langle x|\Big)\Big(\sum_{x:f(x)=0}|x\rangle\Big) = \frac{\sum_{x:f(x)=0}}{2^n}$$

なので、これが厳密に計算できるなら、♯P 問題が解ける。

3　交換するゲートのみの量子計算モデル

Bremner、Jozsa、と Shepherd は、IQP(Instantaneous Quantum Polytime) というモデルを考えた [9]。これは、入力は $|+\rangle^{\otimes n}$ であり、これに任意の可換なゲート

$$e^{i\theta_i Z_i}, \quad e^{i\theta_{i,j} Z_i \otimes Z_j}$$

を作用させ、最後に X 基底で測定する、という量子計算モデルである。明らかに、このモデルはユニバーサル量子計算機ではない。しかも、全てのゲートが可換なので、古典計算機で効率的にシミレートできそうである。

しかし、驚くことに、彼らは、このモデルの出力確率分布が古典計算機で効率的にサンプルできるならば多項式階層が第三レベルで崩壊することを示した。証明は前章の深さ 4 回路と同じである。すなわち、ポストセレクションできる IQP 回路を postIQP と書くとき、postIQP=postBQP を示したのである。

postIQP=postBQP であることを証明するのに、彼らはゲートテレポーテーションを使っているが、測定型量子計算を使っても証明できる。$|+\rangle^{\otimes n}$ でスタートし、それに CZ をかけて、各キュービットに $e^{i\theta_j Z}$ をかけ、最後に X 基底で測定するという IQP 回路を考える。これは、測定型量子計算になっている。したがって、もしポストセレクションできるなら、postBQP ができるのは明らかである。

4　相互作用無しのボソンモデル

Aaronson と Arkhipov は、相互作用無しボソンを用いた量子計算モデルも古典計算機で効率的にシミレートすることができないことを示した [10]。相互作用のあるボソンを用いた量子計算機はユニバーサルであるが、光などでは相互作用を作るのが非常に難しいという事実を考えると、この結果は面白い。

線形光学系は phase shifters と beam splitters からなる。phase shifter は

$$|n\rangle \to e^{in\phi}|n\rangle.$$

あるいは $U = e^{i\phi a^\dagger a}$ と定義される。beam splitter は $(a_1, a_2)^t$ に作用するユニタリ行列

$$U = \begin{pmatrix} \cos\theta & -e^{i\phi}\sin\theta \\ e^{-i\phi}\sin\theta & \cos\theta \end{pmatrix}$$

で定義される。これに加えて、single-photon source と、０，１，２光子数を区別できる detector も使う。ロジカルキュービットをエンコードするのに２モード使う:

$$\begin{aligned} |0\rangle_L &= |0,1\rangle \\ |1\rangle_L &= |1,0\rangle \end{aligned}$$

一つのモードに phase gate をかけると、ロジカル Z 回転ができる。

$$\alpha|0\rangle_L + \beta|1\rangle_L = \alpha|0,1\rangle + \beta|1,0\rangle \to \alpha|0,1\rangle + \beta e^{i\phi}|1,0\rangle$$

ロジカル Y 回転は θ と $\phi = 0$ の beam splitter で以下のように実現できる。

$$\begin{aligned} \alpha|0\rangle_L + \beta|1\rangle_L &= \alpha|0,1\rangle + \beta|1,0\rangle \\ &= \alpha a_2|0,0\rangle + \beta a_1|0,0\rangle \to \alpha(\sin\theta a_1 + \cos\theta a_2)|0,0\rangle + \beta(\cos\theta a_1 - \sin\theta a_2)|0,0\rangle \\ &= \alpha(\sin\theta|1,0\rangle + \cos\theta|0,1\rangle) + \beta(\cos\theta|1,0\rangle - \sin\theta|0,1\rangle \\ &= \cos\theta(\alpha|0,1\rangle + \beta|1,0\rangle) + \sin\theta(\alpha|1,0\rangle - \beta|0,1\rangle) \\ &= \cos\theta(\alpha|0\rangle_L + \beta|1\rangle_L) + \sin\theta(\alpha|1\rangle_L - \beta|0\rangle_L) \\ &= (\cos\theta + XZ\sin\theta)(\alpha|0\rangle_L + \beta|1\rangle_L) \\ &= (\cos\theta - iY\sin\theta)(\alpha|0\rangle_L + \beta|1\rangle_L) \end{aligned}$$

non-linear sign shift, NS_{-1} を定義する:

$$\alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle \to \alpha|0\rangle + \beta|1\rangle - \gamma|2\rangle$$

このゲートは、ある linear optics gate を

$$(\alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle) \otimes |1\rangle \otimes |0\rangle$$

に作用させ、第二キュービットを $|1\rangle$, 第三キュービットを $|0\rangle$ にポストセレクトすることにより実現できる。NS_{-1} gate を使えば、ロジカル CZ gate が実現できる。

したがって、ポストセレクションできれば、相互作用無しボソンモデルはユニバーサル量子計算機になるのである。これと postBQP=PP を組み合わせることにより、相互作用無しボソン量子計算機の出力確率分布が古典計算機で効率的にサンプルできたら多項式階層が第三レベルで崩壊することが導ける。

5　今後の課題

これまでの結果は全て、「古典計算機でシミレートできる」というのは、出力確率分布を厳密に計算できる、もしくは乗的エラーでサンプルできる、という意味であった。これらの定義はかなり厳しいことを要請している。スタビライザー回路や match gate 回路などのように出力の厳密計算が古典計算機で効率的にできるモデルもあるので、このような「厳しい」近似でも、古典的にシミレートすることがハードであることを示すことは十分面白く意義のあることである。しかし、もっと優しい定義で古典シミレート不可能性を示すことはできないのだろうか？

Aaronson と Arkhipov は、同じ論文 [10] で、variation distance error $\|D - D'\| \leq \epsilon$ でのサンプリングでもよいことを示した。ここで、D はボソン計算機の出力確率分布、D' は古典サンプラーの出力確率分布である。ただし、彼らの結果は、二つのまだ証明されていない数学的 conjecture を仮定している。このような仮定なしで、しかも variation distance error でボソン計算機の古典サンプリング不可能性が証明できるか、というのは非常に大きな open problem である。あるいは、そのような仮定をおいてもよいので、variation distance error でのサンプルが難しいことを、他のモデル、DQC1、深さ４回路、IQP 等、で示すことはできるだろうか、というのも重要な open problem である。

References

[1] E. Knill and R. Laflamme, Power of one bit of quantum information, Phys. Rev. Lett. **81**, 5672 (1998).

[2] A. Ambainis, L. J. Schulman, and U. V. Vazirani, Computing with highly mixed states, STOC (2000).

[3] P. W. Shor and S. P. Jordan, Estimating Jones polynomials is a complete problem for one clean qubit, Quant. Inf. Comp. **8**, 681 (2008).

[4] T. Morimae, K. Fujii, and J. F. Fitzsimons, Hardness of classically simulating the one clean qubit model, Phys. Rev. Lett. **112**, 130502 (2014).

[5] S. Aaronson, Quantum computing, postselection, and probabilistic polynomial-time, Proc. R. Soc. A **461**, 3437 (2005).

[6] K. Fujii, H. Kobayashi, T. Morimae, H. Nishimura, S. Tamate, and S. Tani (alphabetical order), Impossibility of Classically Simulating One-Clean-Qubit computation. arXiv:1409.6777

[7] B. Terhal and D. DiVincenzo, Adaptive quantum computation, constant depth quantum circuits and Arthur-Merlin games, Quant. Inf. Comput. **4**, 134 (2004).

[8] D. Gottesman and I. L. Chuang, Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations, Nature **402**, 390 (1999).

[9] M. J. Bremner, R. Jozsa, and D. J. Shepherd, Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy, Proc. R. Soc. A **467**, 2126 (2011).

[10] S. Aaronson and A. Arkhipov, The computational complexity of linear optics, STOC (2011)