

量子コンピュータの実運用に向けた

繰り返し位相推定アルゴリズムの計算コストに関する研究

Calculating the Computational Costs of the Iterative Phase Estimation Algorithm for Practical Operations on Quantum Computers

新村 星太郎 (M2)

Shintaro Niimura

Abstract

The Iterative Phase Estimation Algorithm (IPEA) is a quantum algorithm to measure the phase of an eigenvalue given a unitary matrix and eigenstate. IPEA requires 1 measurement for each bit, or a total of N measurements to achieve a precision of 2^{-N} , and can be proved to have a success probability of over 80%. Increasing the minimum success probability requires several measurements for each bit, which secures the confidence of obtaining the bits correctly. Here we call this the Modified IPEA, and in this research we find the optimal measurements for each bit such that the computational runtime is at its minimum given a success probability to guarantee.

1. 導入

初めて古典コンピュータが導入された経緯と同様に、20世紀末で量子コンピュータが発案された当時では、あくまでも仮想上の機械として量子力学に基づいて情報処理を行う計算機があった場合は、どのようなことができるのかについて研究がされていた。この研究の中で、いくつかの問題では古典コンピュータよりも量子コンピュータの方が速く解けることが分かり[1, 2, 3], 量子コンピュータが古典コンピュータより速いという認識が根付くきっかけになった。

そして、長年の技術的發展により、量子コンピュータは着々と身近なものに近づいている。IBM や Google

らによる量子コンピュータの開発競争が世界中の様々な企業に対して展開されており、クラウド量子計算と呼ばれる、機械は手元にないがいつでもアクセスできる形へと発展している。こうした著しい発展の時代で、今まで概念として扱われてきた量子コンピュータは、現実的なものとして扱われるようになっている。しかし、仮想上の量子コンピュータの研究をそのまま現実の機械へ適用するのは危険である。

仮想上の量子コンピュータでは『速い』と言われている問題は存在するが、現実の量子コンピュータでは本当に我々が欲しい『速い』とは限らない。量子コンピュータの『速さ』は係数や定数を無視できるオーダー上の計算として取り扱われている。例えば、古典コンピュータで解こうとするとオーダー上で指数関数的に計算時間が長くなる問題が、量子コンピュータで解こうとした場合ではオーダー上で多項式時間の関数になるということを『速い』と呼んでいる。しかし、無視している係数や定数が圧倒的に大きい場合、たとえ多項式時間の計算であったとしても、ものすごく長い計算時間を要している可能性もありえる。

本研究の目的は、量子アルゴリズムの一つである改良型位相推定アルゴリズム(Modified IPEA) [4, 5] に着目し、その計算時間を見積もることにある。具体的には、ある精度、ある成功確率を保証したい場合に必要最小の計算時間がどのような値になるのかを調べる。改良型位相推定アルゴリズムの計算時間がわかれば、これを応用するアルゴリズムがどのくらいの計算時間を要するのかを見積もる一歩となる。本研究の位置づけ

はこの一歩を作ることであり、計算時間を調べることに
よって新しい知見を得ることにある。

2. 位相推定アルゴリズムについて

位相推定アルゴリズム (Iterative Phase Estimation Algorithm, IPEA)[6]では、あるユニタリー演算 \hat{U} の固有
状態 $|\Psi\rangle$ に対して、固有値方程式

$$\hat{U}|\Psi\rangle = e^{i2\pi\phi}|\Psi\rangle \quad (2.1)$$

を満たす固有値の位相 ϕ を求める。古典コンピュータが 0 と1の二進数値で情報を処理するのと同様に、
量子コンピュータでも情報は二進数で表すことができる。求めたい固有値の位相 ϕ は二進数で考えており、
以下のように表す。

$$\phi = 0.\phi_1\phi_2 \dots \phi_N + 2^{-N} \times \theta_N \quad (2.2)$$

θ_N とは小数点以下第 N 桁目(第 N bit 目)以下の値で
あり、本研究ではこれを量子化誤差と呼ぶ。

IPEA は、精度 ϵ で位相を求めたい場合、 $\epsilon \geq 2^{-N}$ を満
たす最小の N について、第 N bit 目から各 bit を順次
求めていくアルゴリズムである。任意の整数 k について、
第 k bit 目を求める IPEA の量子回路を Figure 1 に
示す。 $\text{Rot}_z(\vartheta_k)$ は、その前に求めた bit の測定結果
 $\vartheta_k = 0.\phi'_{k+1} \dots \phi'_N$ に依存しており、

$$\text{Rot}_z(\vartheta_k) = \begin{pmatrix} 1 & 0 \\ 0 & e^{-2\pi i \vartheta_k} \end{pmatrix} \quad (2.3)$$

という回転作用を表している。

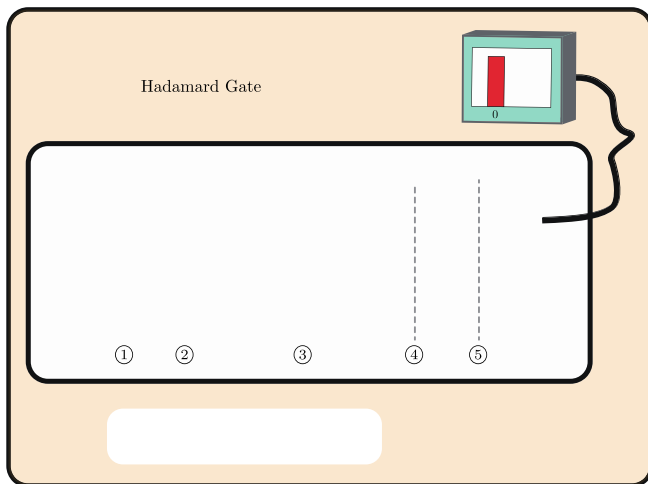


Figure 1. Quantum Circuit of IPEA

この量子回路に従って量子ビットを作用させると、
Figure 1 の ancilla 量子ビットが量子状態 $|0\rangle$ か $|1\rangle$ のど
ちらかを一回の測定で判別することで、位相の第 k bit
目が求まる。第 k bit 目を正しく得る確率は

$$\cos^2\left(\frac{\pi}{2}\theta_k - \frac{\pi}{2}\vartheta_k\right) \quad (2.4)$$

であり、間違える確率は

$$\sin^2\left(\frac{\pi}{2}\theta_k - \frac{\pi}{2}\vartheta_k\right) \quad (2.5)$$

で表される。どちらの式も量子化誤差 θ_N に依存してい
る。IPEA が式(2.2)の第 N bit 目までの bit を全て正し
く得る確率は

$$\frac{\sin^2(\pi\theta_N)}{2^N \sin^2\left(\frac{\pi\theta_N}{2^N}\right)} \quad (2.6)$$

と計算できる。一方で第 N bit 目は、精度 ϵ に対して、
 $\epsilon \geq 2^{-N}$ を満たす最小の N としているので、これを間違
えても求めたい精度内には収まる。第 N bit 目のみを
間違える確率は

$$\frac{\sin^2(\pi(1 - \theta_N))}{2^N \sin^2\left(\frac{\pi(1 - \theta_N)}{2^N}\right)} \quad (2.7)$$

であり、式(2.6)との和が精度 ϵ で位相を得る成功確率
となる。この成功確率は量子化誤差 θ_N に依存してい
り、これを Figure 2 に示す。

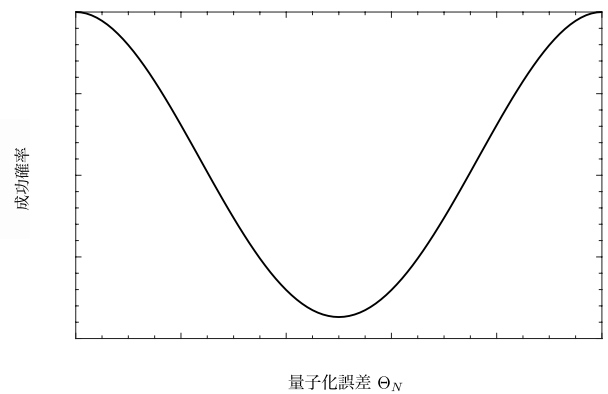


Figure 2. Success Probability of IPEA

3. 改良型位相推定アルゴリズムについて

IPEA の成功確率は量子化誤差 $\theta_N = 0.50$ のときに最小となり, どんな量子化誤差であったとしても少なくとも 80%以上の成功確率が保証されている. より高い成功確率を保証したい場合は, 各 bit を求める際, 量子状態が $|0\rangle$ か $|1\rangle$ の判定を一回の測定ではなく, 複数回の測定でより多く出た方で判定すれば良い. 本研究では, これを「改良型位相推定アルゴリズム (Modified IPEA)」と呼ぶ.

各 bit を何回測定したかを簡易的に表すために, 第 k bit 目の測定回数を r_k として表し, 測定回数ベクトル

$$\mathbf{R} = (r_1, r_2, \dots, r_N) \quad (2.7)$$

を導入する.

改良型位相推定アルゴリズムの成功確率はそれぞれの bit を求めるときに何回測定行うかに依存して変わる. 測定回数ベクトルが一つ定まった場合, 改良型位相推定アルゴリズムの成功確率は, 量子化誤差 $\theta_N = 0.50$ で

$$\prod_{k=1}^{N-1} (1 - \rho_k) \times \frac{1}{2} + \prod_{k=1}^{N-1} (1 - \rho'_k) \times \frac{1}{2} \quad (2.8)$$

それ以外の量子化誤差 $\theta_N \neq 0.50$ で

$$\prod_{k=1}^{N-1} (1 - \rho_k) \times (1 - \rho_N) + \prod_{k=1}^{N-1} (1 - \rho'_k) \times \rho_N \quad (2.9)$$

として導出できる. ただし,

$$P_N = \cos^2\left(\frac{\pi}{2}\theta_N\right) \quad (2.10)$$

$$P_k = \cos^2\left(\frac{\pi}{2^{N-k+1}}\theta_N\right) \quad (2.11)$$

$$P'_k = \cos^2\left(\frac{\pi}{2^{N-k+1}}(1 - \theta_N)\right) \quad (2.12)$$

としたときに,

$$\rho_N = \sum_{i=0}^{\frac{r_N}{2}} \binom{r_N}{i} (P_N)^i (1 - P_N)^{r_N-i} \quad (2.13)$$

$$\rho_k = \sum_{i=0}^{\frac{r_k}{2}} \binom{r_k}{i} (P_k)^i (1 - P_k)^{r_k-i} \quad (2.14)$$

$$\rho'_k = \sum_{i=0}^{\frac{r_k}{2}} \binom{r_k}{i} (P'_k)^i (1 - P'_k)^{r_k-i} \quad (2.15)$$

としている. 例えば, 各 bit を同じ回数測定した場合, すなわち,

$$\mathbf{R} = r_i (1, 1, \dots, 1) \quad (2.16)$$

であった場合, Figure 3 のように量子化誤差に対して成功確率を計算することができる.

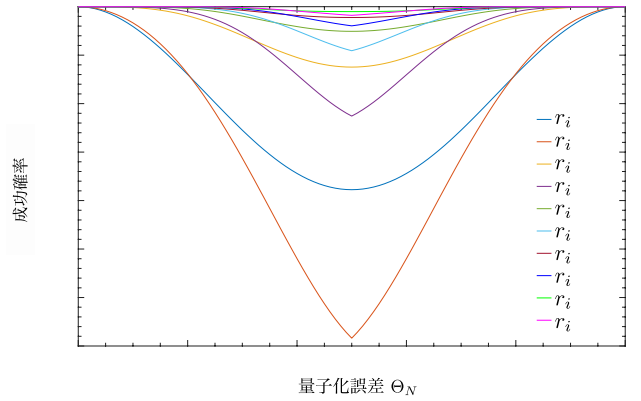


Figure 3. Success probabilities of Modified IPEA

4. 改良型位相推定アルゴリズムの計算時間

改良型位相推定アルゴリズムの計算時間は, どのような精度, どのような成功確率を保証したいかによって変わる. 故に, 精度, 成功確率を変数として, 計算時間を求めた.

計算時間は, 量子回路で表される演算を作用させるために必要な実行時間 t , 及び, 同じ量子 bit で再度演算を作用させるために必要なインターバル時間 τ とした場合,

$$T(\mathbf{R}, t, \tau) = \sum_{k=1}^N r_k (2^{k-1}t + \tau) \quad (2.17)$$

という関数を用いた.

まず, 具体的な例として, Figure 1 の「位相をエンコードする部分」を Figure 4 の量子回路と考え, [3]の論

どのような場合において、測定回数ベクトルが変化するかについても考察した。ある成功確率を保証したい場合において、第 k bit 目の測定回数を増やすより、第 $k-m$ bit 目から第 $k-1$ bit 目の m 個の bit の測定回数を増やした方が計算時間が短くなることもある。その条件は

$$k \geq \log_2 \left(\frac{\tau}{t} \right) + \log_2(m-1) + m - 1$$

であり、実行時間 t とインターバル時間 τ の比で決まる。少なくともこの比が一定である場合においては、測定回数ベクトルは同じである。比が一定でなくなる場合においては、この式を満たす bit の測定回数を増やす必要がない成功確率においては、測定回数ベクトルが変化しないとわかる。

5. 量子コンピュータのハードウェア

Figure 5, Figure 6 の結果では、[7]の論文で用いられた量子コンピュータを想定していた。前節で述べたようにある成功確率を保証する最小の計算時間を与える測定回数ベクトルは、この実行時間やインターバル時間に関連して変化することがある。別の量子コンピュータを想定した場合においては、測定回数ベクトルが変化することも考えられる。例えば、同じ量子回路を用いたとしても、Figure 8 のように保証したい成功確率によっては、[7]の論文で用いられた量子コンピュータよりも計算時間が短かったり、長かったりすることがある。

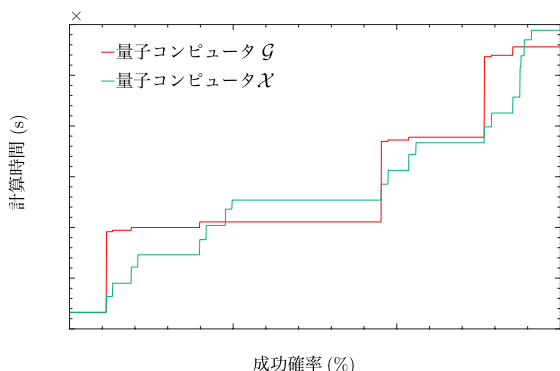


Figure 8. Comparing different quantum computers

6. 総括

量子コンピュータアルゴリズムの速さはオーダ上での議論でまともだった。それは量子コンピュータを仮想的な概念として考え、量子コンピュータがどのようなことができるのかを調べる位置づけであるためには十分であった。しかし、近年の技術的發展により量子コンピュータは、仮想上の概念ではなく、実際に身近に存在している。よって、より現実に近いように議論を拡張していく必要がある。

量子コンピュータを用いた応用先として、量子計算化学が一つの柱と考えられるが、そこでもオーダ上の計算時間の議論が行われている。位相推定アルゴリズム、繰り返し位相推定アルゴリズムを辿り、改良型繰り返し位相推定アルゴリズムが提案され、量子化学計算などへの応用が期待されている一方で、この改良型位相推定アルゴリズムが古典コンピュータで用いるアルゴリズムより早くなるのかはとても重要な問題となる。しかし、古典コンピュータと量子コンピュータではハードウェアの構造、計算手法が異なるため、これらと比較するには共通する土台である時間を用いる必要がある。

本研究では、改良型繰り返し位相推定アルゴリズムの計算時間を見積もった。ただし、量子コンピュータでは確率的にしか答えが得られないこと、及び、位相推定アルゴリズムが精度を任意に指定できることから、ある確率である精度の位相が推定できるために必要な最小な計算時間を求めた。量子回路がどのくらいの実行時間を持つのか、量子コンピュータのハードウェアの性能でインターバル時間がどのようになるのかを考えながら、計算時間を見積もらなければいけない。これはただ合計測定回数のみ、あるいは、量子回路の実行時間のみに着目した結果からは導けない結論であり、オーダ上だけでなく実際に計算時間を見積もることの重要性を示している。

改良型位相推定アルゴリズム以外にもたくさんのアルゴリズムがあり、実際にそれらの計算時間がどのくらいかかるのかは、今後応用や有用性を主張する上で

重要な問題である。量子回路の実行時間やインターバル時間を考慮し、実際の測定回数まで踏み込む議論が増えることを望み、本研究がその一歩になることを期待したい。

References

- [1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.* **26**, 1484–1509(1997).
- [2] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proc. 35th Annual Symposium on Foundations of Computer Science* (IEEE, 1994), pp. 124–134.
- [3] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th Annual ACM Symposium on the Theory of Computing* (ACM, 1996), pp. 212-219.
- [4] M. Dobšiček, G. Johansson, V. Shumeiko, G. Wendin, "Arbitrary accuracy iterative phase estimation algorithm as a two qubit benchmark," *Phys. Rev. A* **76**, 030306 (R) (2007).
- [5] E. Knill, G. Ortiz, R.D. Somma, "Optimal Quantum Measurements of Expectation Values of Observables," *Phys. Rev. A* **75**, 012328 (2007).
- [6] R. B. Griffiths and C.-S. Niu, "Semiclassical Fourier Transform for Quantum Computation," *Phys. Rev. Lett.* **76**, 3228 (1996).
- [7] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandr`a, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis, "Quantum supremacy using a programmable superconducting processor," *Nature* **574**, 505 (2019).