社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

量子シミュレーションの計算量理論へ

(Extended Abstract)

今井　　浩[†,††]

† 東京大学情報理工学系研究科コンピュータ科学専攻　〒113–8656 東京都文京区本郷 7–3–1
†† 東京大学ナノ量子情報エレクトロニクス研究機構
E-mail: †imai@is.s.u-tokyo.ac.jp

あらまし　量子コンピュータによる量子シミュレーションが、小規模量子コンピュータのキラーアプリケーションとして注目されている。Feynman 流の量子シミュレーションは、本質的には連続量からなる対象問題を量子コンピュータにより離散時間・離散値によりシミュレーションするものである。他の量子シミュレーションも適当な計算モデルの上での計算とみなせるとすれば、それらの難易度の解析は、対象問題を計算によって解く際に必要な時間・領域等の計算資源を解明する計算量理論の対象である。本稿では、微分方程式の解を求める問題を、実数を計算モデルの中で扱ってその計算量を論じる実数計算量理論を紹介し、それが量子シミュレーションの計算量解析に向かう方向に触れてみたい。

キーワード　量子計算、量子シミュレーション、量子計算量、実数計算量

Towards Computational Complexity Theory for Quantum Simulation

(Extended Abstract)

Hiroshi IMAI[†,††]

† Dept. Computer Science, IST, University of Tokyo　Hongo 7–3–1, Bunkyo-ku, Tokyo, 113–8656 Japan
†† INQIE, University of Tokyo
E-mail: †imai@is.s.u-tokyo.ac.jp

Abstract　Computational complexity of quantum simulations by quantum computers is viewed from the viewpoint of computational complexity theory over the reals and solving differential equations, with emphasis on precision of computation.

Key words　Quantum computing, quantum simulation, quantum complexity theory, complexity theory over the reals

1. はじめに

力学系シミュレーションをコンピュータで行うことは現代では当たり前のことで、通常は微分方程式を離散化して離散時間・有限桁数小数でシミュレーションの数値計算が実行されている。しかし、現代のコンピュータが開発された黎明期では、アナログコンピュータも実際に開発され、シミュレーションにも使われていた。さらに、より力学系シミュレーションとは何かを突き詰めていくと、物理的シミュレーションをその対象の物理現象自体が「計算している」と考えることも行われていたようであり、それを計算理論から捉えることも行われていた (たとえば [13] 参照)。

Feynman [5], [6] が提唱した量子コンピュータなら量子力学系シミュレーションが高速に行えるのではという構想は、上記のコンテキストでは後半の考えに近いといえる。ただ、Feynman の考えの先見の明があったところは、計算量にまで構想を馳せ、通例のコンピュータを用いた物理シミュレーションで微分方程式を数値的に解いていくという方法を使うだけでは指数的に時間がかかりそうなことを論じ、一方、量子力学原理によって動作する量子コンピュータは、離散時間・離散値の計算によって高速 (多項式時間) で量子力学シミュレーションが実現できるのではとしているところである。

ここで興味深いのは、量子シミュレーションを量子コンピュータで行うと言った場合、人によってはアナログ計算をイメージしそうなところを、Feynman は最初から現代のコンピュータ同様に、離散時間・離散値で量子コンピュータを動作させることを考えていたことである。物理シミュレーションをその物理現象を用いて行うというのは、アナログ計算そのもののように

思えるのにである。

現代のコンピュータは、デジタルに動作し、時間も取りうる値も離散値である。最初にも述べたように、コンピュータ開発の黎明期においては、アナログコンピュータも構想され実際に実現されたが、アナログコンピュータは現実には近似的に問題を解くコンピュータであり、その近似の精度を自由に制御することが困難なため、結局廃れたという歴史がある。

アナログコンピュータの 1 つの側面は、計算モデルとしては実数が扱えるというところにある。計算量理論の分野では、実数関数を扱う計算量の理論 (ここでは実数計算量理論と呼ぼう) も展開されている。実数の扱いについて大別して 2 つの流れ [3], [10] があるが、離散時間発展していって、計算時間が定義されているのは共通である。さらに、最近になって微分方程式を解く問題の実数計算量理論の計算困難さに関する成果 [8] もでてきている。

この実数計算量理論と、Feynman が構想した量子コンピュータによる量子シミュレーションの計算量との間の関係を調べることは、量子コンピュータをあるタイプのアナログコンピュータとみなした場合の研究ともいえ、興味深い。本稿では、この関係を将来調べていくことを念頭に、ここまでにあげた事項で量子情報技術の観点からまとめておくとよい事柄を概観することを行う。

2. 量子力学系シミュレーションと量子計算量

1981 年の MIT Physics of Computation Conference の基調講演において、会議名にも対応したものとして、Feynman は量子力学系のシミュレーションを今のコンピュータで正確にしようとすると指数爆発が起こるのに対し、量子コンピュータならその問題が起こらず効率よく実行できるであろうことについて語っている [5]。さらに、量子コンピュータについても、1984 年の CLEO/IQEC の基調講演で、量子コンピュータの原理についても検討を加えている [6]。量子力学の諸計算は現在でもスーパーコンピュータをより高速化する原動力にもなっており、科学技術計算の将来の限界と展開を見通していたといえる。

量子力学系のシミュレーションが量子コンピュータで高速に行えるという議論は、Lloyd [12] によって肯定的な解決方向が理論的に示されて以来、量子計算において量子力学シミュレーションの範囲を拡大することが研究課題となっている。一方、量子コンピュータが量子力学の問題を計算で解くことについて万能的に機能するわけではないこともわかってきた。計算量理論の MAX SAT に対応する k-Local Hamiltonian 問題が、Kitaev らによって調べられ、最終的に基底状態のエネルギーを求める問題に対応する 2-local Hamiltonian 問題が QMA-完全であることが示されている [9]。他のいくつかの重要な問題も QMA-完全やさらには QMA に属するかわかっていないが、量子多証明者対話証明計算量クラスの QMA(2)(Kobayashi, Matsumoto, Yamakami [11]) に属するという特徴的な問題もある。

以上のことから得られるレッスンは

「量子コンピュータで解く対象問題の計算困難さを示すこと」

である。Feynman の言及で量子計算量について言及されているが、2000 年頃からの量子計算量理論の研究進展によって初めて、量子計算を用いても難しそうということが示せるようになっており、今の時代ではそれを踏まえて簡単な問題をわざわざ量子コンピュータで解くのではなく、今のコンピュータで難しいとわかっている問題で量子コンピュータでどうにか解を導き出すことができそうなもの、さらには量子計算量理論で難しいと思われる問題への挑戦が必要ということである。

3. アナログ計算と実数計算量理論(注1)

物理現象の多くは、明快な微分方程式に従うことから、それを対象の微分方程式を解く自然のコンピュータとみなすこともできる。量子力学では Schrödinger 方程式が対象の微分方程式であり、磁性体はそれ自体が量子力学を解いていると考えることもできる。

微分方程式をコンピュータで解くというと、多くの場合、デジタルなコンピュータで離散化して離散時間で解くことを考えると思われる。それは、シミュレーション・数値計算・ハイパフォーマンスコンピューティングの分野で広く行われていることで、一方上のような意味で物理現象を解くコンピュータを考えるということとはかなり違う。次に数式処理によって解析解を求めると思う場合もあるかもしれないが、それは理論解を求めることにコンピュータを援用して解くことであり、再び物理現象を解くコンピュータを考えることとは違う。

物理現象では、多くの場合、変数は連続値をとる。微分方程式で記述されている場合、もちろんそうである。だとすると、物理現象を解くコンピュータでは、実数を扱えるモデルを考えるのが妥当である。「連続値＝アナログ」という意味とすると、アナログコンピュータを考えることになる。そしてこのアナログコンピュータは実数を扱えないといけない。

アナログコンピュータのモデルで、実数の扱い方については、大まかにいって 2 つの体系がある。1 つの体系は、実数がコンピュータの 1 ワードで正確に表現でき、2 つの実数の間の四則演算が正確にできるというものである (Blum, Shub, Smale [3])。しかしながら、物理現象を解くコンピュータのためのモデルとしては、結局のところ出力で実数を得るために別途方法を用意せねばならず、少なくとも今のコンピュータの黎明期に開発されたアナログコンピュータでは近似計算でしかなく、かつその近似度が思いのままに制御できないことから、デジタルなコンピュータの安定性と高性能化の前に、結局そのようなアナログコンピュータは廃れていった事実を反映しにくいように思われる。

もう 1 つの体系は Ko, Friedman [10] によるもので、実数関数を計算する問題に対して、実数値を m ビットの 2 進数でデジタル近似し、感覚的にはその m を入力サイズに入れて計算時間を定義していくものである。より高精度の近似解を得たければ、それだけ時間がかかることを表現できる一方、うまくモデル化すればあとは通常の離散の Turing マシンで、離散時間・

(注1)：本節の内容については高崎 [13], 河村 [7] を参照している

離散値の中で動作するデジタルな場合との親和性がとれる。

4. Church の提唱から量的・量子版へ、そして アナログに

計算可能性、計算量理論の大本となる提唱についても振り返ってみることが意義深い。

Church の提唱： 全てのコンピュータは Turing 機械でシミュレートできる。

これは 1930 年代に個別に構築された計算モデルが、計算可能性について全て同等であったことを踏まえてなされたものである。時代が進み、計算資源の量に着目する計算量理論の発展とともに、色々な物理実現によるコンピュータが開発される中でほぼ経験できたこととして、次の提唱が考えられている。

量的 Church の提唱： 全ての物理的コンピュータ装置は、Turing 機械によって、コンピュータ装置の資源に関して多項式ステップでシミュレートできる。

量子コンピュータでは、原理となる物理として量子力学を用い、ここまでの発展を遂げてきている。

アナログ計算の観点に戻ると、Ko, Friedman によるモデルは、実は Feynman が近似精度に関する議論を行っていることからも、その構想した量子コンピュータによく対応する。Deutch の量子 Turing マシンの定義 [4] から、クラス BQP 等での量子コンピュータの取る値の離散化に至る過程 [1], [2] とも対比していくと面白い。

5. 微分方程式に関する実数計算量理論

Ko, Friedman のアナログコンピュータでは、任意の指定された精度で微分方程式を正確に解くことが可能となる。最近 Kawamura [8] は、実関数 $h: \mathbf{R} \to \mathbf{R}$, $g: [0,1] \times \mathbf{R} \to \mathbf{R}$ に対して、

$$h(0) = 0, \quad h'(t) = g(t, h(t)), \quad t \in [0,1]$$

の計算量についての成果を得ている。この微分方程式が唯一解をもつための十分条件に Lipschitz 連続;

$$|g(t,y_0) - g(t,y_1)| \leqq Z \cdot |y_0 - y_1|, \quad t \in [0,1], \quad y_0, y_1 \in \mathbf{R}$$

が y_0, y_1, t と独立な定数 Z に対して成立することがあるが、定理として次を得ている。

定理. [8] Lipschitz 連続の条件のもと、h は PSPACE 完全でありうる。

なお、g がさらに解析的である場合、h は多項式時間で求められることがわかっている。

このように十分に性質のよい微分方程式に対しても、実数計算量の観点から計算困難さを示す結果も得ることが可能となっている。

一方、現状の実数計算量の研究では、まだ多変数実数関数の場合に対する定義部分から課題が残っており、量子計算量との間にはかなりの距離がある。

謝 辞

実数計算量を初め種々のことを教えて頂いた東京大学コンピュータ科学専攻の河村彰星氏に感謝する。本研究は文部科学省イノベーションシステム整備事業の支援により遂行された。なお、実数計算量の量子計算への展開についての研究は科研費 23240001 の助成を受けたものである。

文 献

[1] L. M. Adleman, J. Demarrais, and M.-D. A. Huang: Quantum Computability. *SIAM Journal on Computing*, Vol.26, No.5 (1997), pp.1524–1540.

[2] E. Bernstein and U. Vazirani: Quantum Complexity Theory. *SIAM Journal on Computing*, Vol.26 (1997), pp.1411-1473.

[3] L. Blum, M. Shub and S. Smale: On a Theory of Computation and Complexity over the Real Numbers: NP-Completeness, Revursive Functions and Universal Machines. *Bulletin of the American Mathematical Society*, Vol.21, No.1 (1989), pp.1–46.

[4] D. Deutsch: Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer. *Proc. Roy. Soc. London Ser. A*, Vol.400 (1985), pp.96–117.

[5] R. Feynman: Simulating Physics with Computers. *International Journal of Theoretical Physics*, vol.21, Nos.6/7 (1982), pp.467–488.

[6] R. Feynman: Quantum Mechanical Computers. *Opt. News*, Vol.11 (1985), pp.11–46; reprinted in R. P. Feynman: Quantum Mechanical Computers. *Foundations of Physics*, Vol.16, No.6 (1986), pp.507–531.

[7] 河村彰星: アナログ計算と複雑度.「計算可能性問題における極限再帰関数の役割の多角的研究」セミナー配布資料, 京都, 2009-07-29.
http://qci.is.s.u-tokyo.ac.jp/˜kawamura/papers/090722/abstract_s.pdf

[8] A. Kawamura: Lipschitz Continuous Ordinary Differential Equations are Polynomial-Space Complete. *Computational Complexity*, Vol.19, No.2 (2010), pp.305–332; a conference version in *Proceedings of the 24th IEEE Conference on Computational Complexity (CCC 2009)*, 2009, pp.149–160.

[9] J. Kempe, A. Kitaev and O. Regev: The Complexity of the Local Hamiltonian Problem. *SIAM Journal on Computing*, Vol.35, No.5 (2006) pp.1070–1097.

[10] K. Ko and H. Friedman: Computational Complexity of Real Functions. *Theoretical Computer Science*, Vol.20, No.3 (1982), pp.323–352.

[11] H. Kobayashi, K. Matsumoto, and T. Yamakami: Quantum Merlin-Arthur Proof Systems: Are Multiple Merlins More Helpful to Arthur? *Chicago Journal of Theoretical Computer Science*, Article 3 (2009), 19pp.

[12] S. Lloyd: Unviersal Quantum Simulations. *Science*, Vol.273. No.5278 (1996), pp.1073–1078.

[13] 高崎金久: 微分方程式と計算可能性. 京都大学数理解析研究所講究録, Vol.1020 (1997), pp.39–62.