量子乱数プロトコルを用いた量子計算機の安定性評価

鹿野　豊
群馬大学大学院理工学府
Institute for Quantum Studies, Chapman University
email: yshikano@gunma-u.ac.jp

2022 年 10 月 22 日

概 要

All computing devices, including quantum computers, must exhibit that for a given input, an output is produced in accordance with the program. The outputs generated by quantum computers that fulfill these requirements are not temporally correlated, however. In a quantum computing device comprising solid-state qubits such as superconducting qubits, any operation to rest the qubits to their initial state faces a practical problem. On the implementation of the scalable quantum computers, the health check (or stability check) algorithms are needed. We propose that the quantum random number generation is one of the candidates of the health check algorithms in any quantum computing devices.

1　はじめに

量子計算機に関して、量子アルゴリズムと呼ばれる計算アルゴリズムの根本的な変更により、これまで知られていた従来型の計算量とは別の量子計算量という概念を創出した。特筆すべきは、現代暗号の計算量的安全性の基盤として用いられている「素因数分解のアルゴリズム」は **NP** (Non-deterministic Polynomial time) のクラスであることは知られているが、量子コンピュータによって誤り確率が高々1/3 の多項式時間で解ける決定問題の複雑性クラスである **BQP** (Bounded-error Quantum Polynomial time) で解けるという Simon-Shor のアルゴリズムというものが知られている。そのため、量子計算機を物理系として実現するための開発のレシピを必死に模索してきており、現在は小規模ではあるが、クラウド上でユーザーが自由にアルゴリズムを実行できる量子計算機も実現している。一方で、量子状態をそのまま情報のソースとして用いるためにノイズに対して従来型のデジタル計算機より耐性がないことが知られている。このため、一つ一つの計算素子の単位である量子ビットの正確な評価を行い、物理的な原因を追跡した上で量子ビットの改善をこれまで行ってきた。しかし、このようなボトムアップでのやり方は量子ビット数が増えれば増えるほど、評価だけに時間がかかってしまうため、ユーザーが計算機として使える時間が減ってしまうということが知られている。そのため、簡易に量子計算機の評価・診断ができるプロトコルの開発が必要であるということが必要であることは必然であろう。

そこで、本論稿では、量子計算機を計算機システムの一つだと捉えると、インプットおよびアウトプットにはビット列を用いたブラックボックスモデルとシステム的な観点で考えることが出来る。この際、デジタル計算機と量子計算機の本質的な差は、インプットに対してアウトプットが確定的に出てくるデジタル計算機に対して [1]、インプットに対してアウトプットが確率的に出てくるため、何度も同じアルゴリズムを実行し、その結果から統計的な判断を加えなければならないのが量子計算機の特徴である。すると、量子計算機の特徴を調べるためには、本質的に確率的な出力を行うシステムであるということを統計的に判定する問題に落とし込むことが出来る。そのため、本論稿では、量子計算機が確率的出力を本質的にするシステムであることをチェックするためにシードのない乱数生成器 [1][2]であるということを検証する方法を検討する。

2　量子乱数プロトコル

我々の提案する量子乱数プロトコルは非常に単純である。量子状態を用意する空間として量子力学の公理より 2 次元の複素ヒルベルト空間 $\mathcal{H} := \mathbb{C}^2$ を考える。そして、初期の量子状態として

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in \mathbb{C}^2 \tag{1}$$

[1]当然、デジタル計算機にも必須なノイズがあるため、誤り訂正符号という技術を実装させ、確定的にアウトプットのビット列を出力させなければならない。

[2]シードのある乱数生成器のことの代表例はデジタル計算機の中で実装される疑似乱数生成器である。物理乱数生成器の多くは初期条件の違いに対して出力結果が鋭敏であることを利用しているため、真性乱数生成器とは呼ばれていない。

を用意する。そして、ここにアダマールゲート $H \in U(2)$ という状態を作用させると

$$|\psi\rangle := H|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} \tag{2}$$

となる。量子力学の公理より測定結果に関しては、量子状態に対して自己共役作用素 A をスペクトル分解する。今回の場合、$A = \sigma_z \in U(2)$ というパウリ行列を採用すると、

$$\sigma_z = +1|0\rangle\langle 0| + (-1)|1\rangle\langle 1| = +1\begin{pmatrix}1&0\\0&0\end{pmatrix} + (-1)\begin{pmatrix}0&0\\0&1\end{pmatrix} =: +1\hat{P}_0 + (-1)\hat{P}_1 \tag{3}$$

となる。ここで、$\langle 0| := (|0\rangle)^\dagger, \langle 1| := (|1\rangle)^\dagger$ という Dirac 記法を採用している。これは、射影作用素 $\hat{P}_0, \hat{P}_1$ に対して、それぞれに対応する固有値が測定結果として得られる。その固有値が得られる確率はボルンの確率規則より

$$\Pr\,(*) := \|\hat{P}_*|\psi\rangle\|^2,\ (* \in \{0,1\}) \tag{4}$$

となることから、今回の例においては

$$\Pr\,(0) = \Pr\,(1) = \frac{1}{2} \tag{5}$$

となる。そして、測定結果を得た後に初期状態にリセットさせる。こうすることで何度でもアルゴリズムが実行できるようになる。これは 1 量子ビットに対して、全て同じ操作を行っていることからシードのない乱数生成器と捉えることが出来る。

本論稿では、これを用意されたクラウド量子計算機の全ての量子ビットに対して、同じ操作を「同時に」[3]。次に、このアルゴリズムを 5 日間実行させ、その結果として量子ビットが安定的な確率的な出力を得ているかということを単純に実行回数に対して「1」の出た積算回数をグラフ化することにより直線になっていなければ不安定に動作したということが分かった [3]。そして、初期状態へのリセットが不十分な場合、出力されたビット列に対して時間相関が検出されてしまう可能性があるため、チェックを行ったところ、時間相関がランダムに行っている可能性が示唆された [4]。このような検定を行うことで量子計算機の安定動作に関する指標を構築できる可能性があるということを示した。

3　おわりに

量子計算機をシステムとして捉えることで、量子乱数プロトコルが量子計算機の簡易診断プロトコルになるということを指摘した。本論稿で提案したプロトコルをクラウド量子計算機で実行したところ、全て安定的に動作されていないということが統計的な処理により明らかになった。

今後、NIST Test Suites を拡張させ、バイアルのある確率出力がある場合での乱数検定手法を開発させ、更には、安定性動作指標として本論稿では実行回数に対して「1」の出た積算回数をグラフ化することにより直線になっていなければ不安定に動作したということを判定基準としたが、その他にもランダム化試験のような統計的手法を適用することが重要である。統計学的基準を利用した量子計算機の指標づくりは、これまでも行われてきたが、今後、更に重要であると予想するため理論的な側面のみならず、実際のデータ処理をした際のソフトウェアの整備まで含めて開発していかねばならない宿命である。

参考文献

[1] Y. Shikano, AIP Conference Proceedings **2286**, 040004 (2020).

[2] K. Tamura and Y. Shikano, TUCS Lecture Notes **30**, 13 - 25 (2019); Cryptology ePrint Archive, Paper 2020/078.

[3] K. Tamura and Y. Shikano, International Symposium on Mathematics, Quantum Theory, and Cryptography, Mathematics for Industry, vol 33 (Springer, Singapore, 2021) 17– 37.

[4] Y. Shikano, K. Tamura, and R. Raymond, EPTCS **315**, 18– 25 (2020).

[3] ハードウェアの制約上、同時に本当に実行されているわけではなさそうであるが、残念ながら量子ビット数を増やして動作させるという方向性に昨今は焦点が当てられており、どれくらい正確に量子操作が実行できるかという点においてはあまり改善が見られていない。特に長期的に安定的に動作できるシステムではないということは強調しておきたい。更には、2022 年 10 月現在であっても全ての乱数検定をパスするクラウド量子計算機は存在していない。