Vol.2021-QS-2 No.17
2021/3/29

ノイズ付き浅層回路に於ける量子優位性

長谷川敦哉 * Francois Le Gall †

概要

量子計算の古典計算に対する優位性の証明を試みる研究は様々なアプローチで行われてきた。有名な素因数分解を多項式時間で解く Shor のアルゴリズムなどは量子計算の優位性を示唆するものである。最近 Bravyi ら (Science 2018) は前提条件なしで浅層の量子回路が古典回路よりも優れていることを示した。浅層の回路とは回路の深さがビットのサイ ズに対して小さい回路のことである。Le Gall(CCC 2019) は平均的な設定でも同じような優位性があることを示した。さらに Bravyi ら (Nature 2020) は量子回路に局所性のあるノイズがあっても量子誤り訂正を用いることで同じような優位性があることを示した。

私たちは局所性のない量子ビットの破損があっても、同じ優位性があることを示した。 小さい定数割合の量子ビットにノイズや破損があってもそれらを使わずに計算を行う。計算問題は入力と出力の関係をシミュレートするものである。入力に対して量子グラフ状態を作り基底を変えて観測し、出力はその観測結果である。Bravyi ら量子グラフ状態をグリッドグラフで考えたが、私たちはエクスパンダーグラフで考える。エクスパンダーグラフは一定の割合で任意に頂点の削除があっても、残りのグラフが大きいグリッドマイナーを含むことが言える。この削除が量子ビットの破損に対応している。エクスパンダーグラフの性質を使うことで、一定割合のキュービットに任意にノイズがあっても定数深さの量子回路が全てのその関係をシミュレートできて、古典回路は入力の大きさに対して対数深さが少なくとも一つの入力に対して必要になることを示した。

1 はじめに

1.1 背景

量子計算の古典計算に対する優位性の証明は様々な形で行われてきた。有名な Shor のアルゴリズム [13] は素因数分解が量子計算機を用いると多項式時間で解けることを主張している。その一方で素因数分解は古典計算機の一番いいアルゴリズムを用いても指数時間かかる。しかしこれは量子計算機が古典計算機より優れている証明にはならない。なぜなら古典計算機を用いて素因数分解が多項式時間で解けるアルゴリズムが発見される可能性があるからである。

また最近では 50-100 キュービットの量子計算機が実装されており、それらは規模が比較的小さくまたノイズがある事から NISQ デバイス [12] と呼ばれる。それらを用いてスーパーコンピューターに対する量子優位性 [12] が主張されている [3]。

上述のどちらも古典計算機に対して量子計算機が優れていることを示唆しているものの厳密な証明にはなっていない。クエリコンプレキシティーやコミュニケーションコンプレキシティーなどに於ける制限されたモデルでの優位性は示されている [2, 10, 6] ものの、チューリングマシンなどの一般的なモデルでは優位性の証明が行われていない。またその証明はとても難しいことが分かっている。なぜなら量子計算機ので効率良く解け

* 東京大学情報理工学系研究科
† 名古屋大学多元数理科学研究科

る問題のクラス BQP[11] と古典計算機で効率良く解ける問題のクラス P のセパレーションが証明できるとクラス P と PSPACE のセパレーションが言えてしまってそれは計算機科学における有名な未解決問題だからである。

ただし妥当な計算量のクラスの仮定があれば、回路モデルでの量子計算機の古典計算機に対する優位性は示されている。それは浅い量子回路の生成する確率分布を古典計算機でシミュレーションするのは難しいというものである [1]。さらに最近の Bravyi らの結果として計算量クラスの前提なしで浅い古典回路と量子回路の計算能力のセパレーションを示された。具体的にはある二項関係を計算する問題があって定数深さの量子回路で解てるがその一方でそれを古典回路で解こうとしすると入力サイズに対して対数深さがかかるというのもである。浅層の量子回路はノイズやデコヒーレンスに強いので近い将来実装されうる点でも上述の結果は重要である。

さらなる結果として、Bravyi らは量子回路にノイズがあっても同じ様なセパレーションが言えることを証明した [5]。彼らは立方格子のトポロジーで与えられた量子ビットの中で量子誤り訂正を使うことで定数深さで解ける問題が、古典回路だと定数深さで解けないことを示した。彼らが使っているノイズモデルは以下の様なものである。

定義 1 ([5] の Definition 9)**.** n キュービットを考える。そしてエラーとして X, Y, Z パウリゲートを考える。任意にキュービットの集合 F を取ったとき、全てのキュービットにエラーが掛かっている確率がある定数 p を使って $p^{|F|}$ 以下になる。

この定義はエラーの起こり方にある種の局所性を仮定している。ある集合を取ってきた時、それらが全てエラーが起きている確率が集合のサイズ対して指数的に小さくなるというものである。この性質は量子誤り訂正を使う時に必要である。つまりあるキュービットに起きたノイズを訂正するためには、周りにノイズの起きていないキュービットがそれなりにある必要がある。

1.2 私たちの貢献の概略

私たちがセパレーションを証明するために使う計算問題をグラス状態サンプリング問題と名付ける。この問題はグラフの関数 $\rho(G)$ として書ける。それを使って私たちの結果は以下の様に書ける。

定理 2. $\rho(G)$ はグラフ G から生成される二項関係である。頂点集合の大きさが無限に大きくなるあるグラフの族 $(G_i)_{i\in\mathbb{N}}$ があって、その 1 に近い割合の頂点を含んだ任意の誘導部分グラフ S_i を考える。i が十分大きい時、S_i のトポロジーでゲートを掛けられる量子回路が全ての $\rho(S_i)$ を定数深さで解け、その一方で高い確率で全ての $\rho(S_i)$ を解く確率的古典回路は深さが $\Omega(\log|S_i|)$ 必要になる。

この計算問題は Bravyi らの結果 [4] で使われている計算問題 2D Hidden Linear Function Problem の拡張となっている。そのため彼らの結果は次の様に書くことができる。

定理 3 ([4] の Theorem)**.** グリッドグラフ G を考える。G のトポロジーでゲートを掛けられる量子回路が全ての $\rho(G)$ を定数深さで解け、その一方で高い確率で全ての $\rho(G)$ を解く古典回路は深さが $\Omega(\log|G|)$ 必要になる。

我々はエクスパンダーグラフを考えたときのグラフ状態サンプリング問題を考える。エクスパンダーグラフとは疎かつ結合性の高いグラフである。第 2 章で我々が使うエクスパンダーグラフの性質について証明を行

う。第 3 章では三角形での量子グラフ状態における量子非局所性について説明する。第 4 章でははじめにグラフ状態サンプリング問題について定義する。そしてエクスパンダーグラフとその誘導部分グラフ S について $\rho(S)$ を考えた時に、量子回路が定数深さでそれを解けること、そして古典回路で解こうとすると第 3 章で説明される量子非局所性質が起きるので入力サイズに対して対数深さが必要になることを示す。第 5 章で我々の結果のまとめと既存の結果との比較を行う。

2 エクスパンダーグラフ

エクスパンダーグラフ [8] とは疎でかつ結合性の高いグラフのことである。エクスパンダーグラフは歴史的に数学や計算機科学で応用されてきた。はじめにエクスパンダーグラフの定義を行う。まずはそのために必要なグラフの近傍の定義を行う。

定義 4 (近傍)**.** グラフ G とその頂点集合の部分集合 U を考える。その近傍 $N_G(U)$ は V には含まれているが U には含まれていない頂点でかつ U に隣接している頂点集合である。

そして拡張係数 $h(G)$ が次の様に定義される。

定義 5 (拡張係数)**.** グラフ $G=(V,E)$ と $|U|\leq\frac{1}{2}|V|$ を満たす任意の部分集合 U を考える。そのうち最小の $\frac{|N_G(U)|}{|U|}$ が拡張係数 $h(G)$ である。

そしてそれらを使うことでエクスパンダーグラフの族が定義できる。

定義 6. グラフ $G_i=(V_i,E_i)$ の族 $(G_i)_{i\in\mathbb{N}}$ は以下の条件を満たす定数 $d\geq 1$ と $h>0$ が存在する時エクスパンダーグラフの族となる。

(1) 頂点集合のサイズ $|V_i|$ が無限に大きくなる
(2) i によらず最大次数が d で抑えられる
(3) i によらす拡張係数 $h(G_i)$ が h 以上になる。

エクスパンダーグラフのグラフマイナーの性質 [9] を使うことで、以下の定理を証明することができる。

定理 7. エクスパンダーグラフ $G=(V,E)$ と十分小さい定数 ϵ を考える。G から $\epsilon|V|$ までの頂点を任意に削除したとしても、$\frac{|V|}{2}$ 以上の頂点サイズの連結誘導部分グラフ C が残りそれは $\Omega(|V|^{\frac{1}{4}})\times\Omega(|V|^{\frac{1}{4}})$ のグリッドをマイナーとして含む。

3 量子非局所性

量子非局所性とは量子だと局所的な計算が古典では非局所的な結果となることを指す。ここではまず辺の長さが偶数の三角形 Γ の量子グラフ状態 $|\psi_\Gamma\rangle$ を考える。そして図 1 の様に三角形の角の頂点を u,v,w そして三つの辺のに当たる頂点たちをそれぞれ L,R,B と名付ける。グラフ状態 $|\psi_\Gamma\rangle$ を 3 ビットの入力 x に応じて u,v,w を X 軸で観測するか Y 軸で観測するかを決め、他の頂点を X 軸で観測した全体の観測結果を z とする。そして観測結果を端から偶数番目か奇数番目かで以下の様にまとめる。

$$z_L = \bigoplus_{i\in L_{odd}} z_i \quad z_R = \bigoplus_{i\in R_{odd}} \quad z_B = \bigoplus_{i\in B_{odd}} z_i \quad z_E = \bigoplus_{i\in R_{even}\cup L_{even}\cup B_{even}} z_i$$

するとグラフ状態のスタビライザー を考えることで以下の様な関係があることが言える。

$$x_u x_v x_w \text{によらず} \quad z_R \oplus z_B \oplus z_L = 0 \tag{1}$$
$$x_u x_v x_w = 000 \text{ の時} \quad z_E = 0 \tag{2}$$
$$x_u x_v x_w = 110 \text{ の時} \quad z_E \oplus z_L = 1 \tag{3}$$
$$x_u x_v x_w = 101 \text{ の時} \quad z_E \oplus z_B = 1 \tag{4}$$
$$x_u x_v x_w = 011 \text{ の時} \quad z_E \oplus z_R = 1. \tag{5}$$

x 受け取って z を出力する古典回路 C を考える。x と z が上の関係性を満たそうとする時、次のことが証明できる。

定理 8. L 上のキュービットの観測結果に対応する出力が x_u, x_v のうち多くとも一つにしか依存しないとする。R, B についても同じ様に三角形上で近い入力のうち一つまでにしか依存しないとする。その時 C の入出力 x と z が (1)-(5) を高い確率で満たすことは出来ない。

上の定理は量子では隣り合うキュービットにゲートを掛けて表現できる関係性が、古典で入力が三角形上で幾何的に近い出力にしか影響を及ぼせないとすると表現できないことを示している。つまり量子非局所性が現れている。

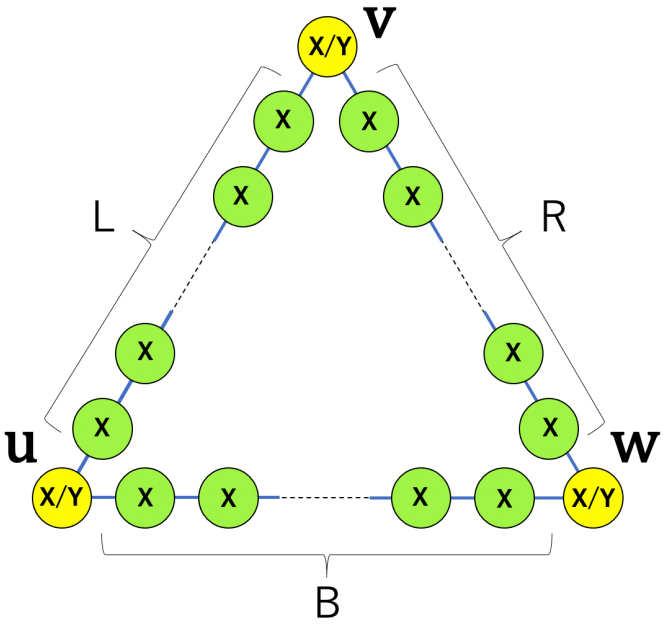

図 1　三角形の量子グラフ状態 $|\psi_\Gamma\rangle$

4 グラフ状態サンプリング問題の定義と量子優位性の証明

4.1 グラフ状態サンプリング問題の定義

グラフ状態サンプリング問題はグラフの関数 $\rho(G)$ が表す二項関係 R として定義できる。R は $\{0,1\}^{|V|+|E|} \times \{0,1\}^{|V|}$ の部分集合となっている。xRz が成り立つ時、x に応じて量子グラフ状態とそれぞれのキュービットの観測軸が定められ、z がその有り得る観測結果となる。具体的に x に対して構成される量子状態 $|\psi_x\rangle$ が

$$|\psi_x\rangle = H^{\otimes|V|} \prod_{x_v=1} S_v \left(\prod_{x_e=1} CZ_e \right) H^{\otimes|V|} |0^{|V|}\rangle$$

となってこの状態の計算基底による観測結果が z となる。つまり x に対して $p(z) = |\langle z|\psi_x\rangle|^2 > 0$ となる z が二項関係 xRz が成立する。

4.2 グラフ状態サンプリング問題を解く定数深さの量子回路

グラフ G が次数が定数で抑えられている時を考える。グラフの最大次数が Γ の時、Vizing の定理 [7] より、多くとも $\Gamma+1$ で辺彩色できる。同じ色の辺に対応する CZ ゲートは同時にかけることができるので、任意の x に対して $|\psi_x\rangle$ は多くとも $\Gamma+4$ の深さの量子回路に対応させることができる。そのため $\rho(G)$ は全て定数深さの量子回路で解くことができる。

4.3 浅い古典回路でグラフ状態サンプリング問題を解く困難性

定理２は今までの用語を使うことで次の様に書くことができる。

定理 9. グラフ G をエクスパンダーグラフとする。そして S を $G \times K_2$ の１に近い割合の誘導部分グラフとする。$|G|$ を十分大きく取るとき、全ての $\rho(S)$ が S のトポロジーでゲートを掛けられる定数深さの量子回路で解け、その一方で全ての $\rho(S)$ を高い確率で入出力として満たすファンインが定数で抑えられている古典回路の深さは $\Omega(\log|S|)$ 以上必要になる。

上の定理の証明を行う。S の次数が定数で抑えられている事から、$\rho(S)$ は定数深さの量子回路で解く事ができる。

その一方で、浅い $(O(log|S|))$ 古典回路が $\rho(S)$ を解くと仮定する。すると古典回路が浅いこととファンインが定数である事から、全ての出力のビットが多くの入力のビットに依存しないことがわかる。さらにその事から、ほぼ全ての入力のビットが多くの出力に影響を与えない事がわかる。$G \times K_2$ から S を作るのに削除した頂点と、多くの出力に影響を与えている入力ビットに対応する頂点を合わせても十分小さい線形サイズで抑えられる事がわかる。その事と定理７から、S は $\Omega(|V|^{\frac{1}{4}}) \times \Omega(|V|^{\frac{1}{4}})$ のグリッドをマイナーとして含むグラフ G を考えた時、$G \times K_2$ を含む事がわかる。そのグラフで図２で表されている領域 P, Q, R とその中からサブグリッドとして Box(p),Box(q),Box(r) を考える。するとそれぞれの Box 同士で点素なパスがたくさんある事から、頂点 p, q, r を通る偶数長さのサイクルで尚且つそれぞれの頂点から近いところの出力にしか影響を及ぼさないものが少なくとも一つ取る事ができる事がわかる。そしてそのサイクルはまさに定理８の量子非局所性が起き古典回路が上手く正しい出力を返せない。つまり $\rho(S)$ を解くにはより深い古典回路 $\rho(S)$ が必要

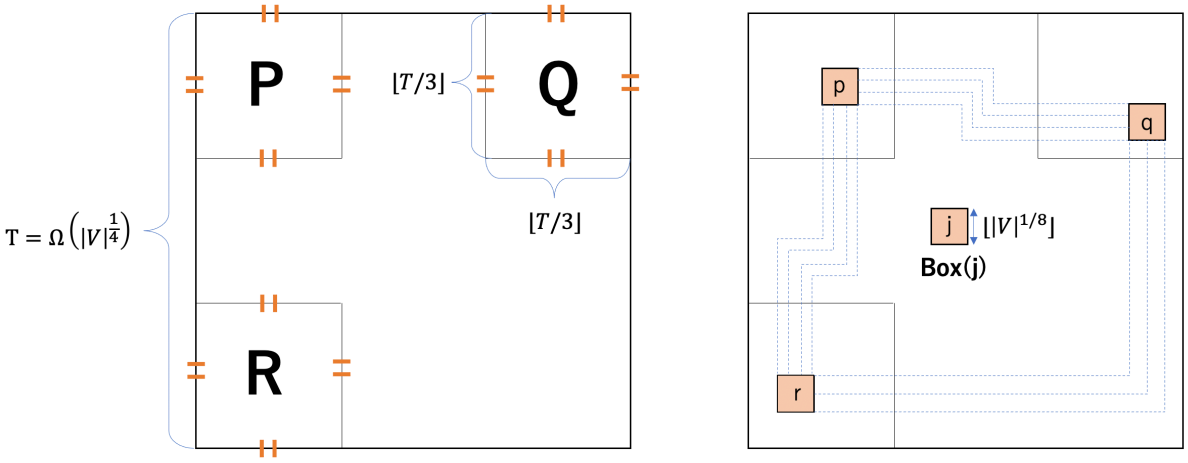

図 2　グラフ $G' \times K_2$ の領域 P,Q,R と三つの Box の図

になる事がわかる。

5　まとめ

定理 9 の結果について部分グラフに含めない頂点を量子キュービットのノイズとして解釈する。そうすると小さい一定割合のキュービットを使わなくても定数深さの量子回路で解けるある計算問題を古典回路で解こうとすると入力サイズに対して対数深さが必要になってしまうというものである。さらに使わないキュービットに関しては任意に取る事ができる。この点が Bravyi らの結果 [5] との大きな違いである。さらに私たちの結果ではノイズの形としてどんなものでも許容できる。これらをまとめたものが表 1 である。

	Computational Problem	Type of Noise	Locality of Noise	Locality of Quantum Circuits	Required Depth of Classical Circuits	Error Correction
Our Result	Graph State Sampling	Any Type	Global	Expander Graph	$\Omega(\log(n))$	✕
Quantum Advantage with Noisy Shallow Circuits[12]	Generalized Magic Square	Pauli X, Y or Z gates	Local	3D Grid	$\Omega\left(\frac{\log(n)}{\log(\log(n))}\right)$	○

表 1　Bravyi らの結果 [5] と私たちの結果の比較

参考文献

[1] Scott Aaronson and Alex Arkhipov. The computational complexity of linear optics. In *Proceedings of the forty-third annual ACM symposium on Theory of computing*, pages 333–342, 2011.

[2] Andris Ambainis. Understanding quantum algorithms via query complexity. *arXiv preprint arXiv:1712.06349*, 244, 2017.

[3] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A Buell, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.

[4] Sergey Bravyi, David Gosset, and Robert König. Quantum advantage with shallow circuits. *Science*, 362(6412):308–311, Oct 2018.

[5] Sergey Bravyi, David Gosset, Robert Koenig, and Marco Tomamichel. Quantum advantage with noisy shallow circuits. *Nature Physics*, 16(10):1040–1045, 2020.

[6] Ronald De Wolf. Quantum communication and complexity. *Theoretical Computer Science*, 287(1):337–353, 2002.

[7] Reinhard Diestel. *Graph theory*, volume 173 of *Graduate texts in mathematics*. Springer, 2000.

[8] Emmanuel Kowalski. *An introduction to expander graphs*. Société Mathématique de France, 2019.

[9] Michael Krivelevich. Expanders — how to find them, and what to find in them. *Surveys in Combinatorics*, pages 115–142, 2019.

[10] Hoi-Kwong Lo. Classical-communication cost in distributed quantum-information processing: a generalization of quantum-communication complexity. *Physical Review A*, 62(1):012313, 2000.

[11] Michael A Nielsen and Isaac Chuang. *Quantum computation and quantum information*. American Association of Physics Teachers, 2002.

[12] John Preskill. Quantum computing and the entanglement frontier. *arXiv preprint arXiv:1203.5813*, 2012.

[13] Peter W Shor. Polynomial time algorithms for discrete logarithms and factoring on a quantum computer. In *International Algorithmic Number Theory Symposium*, pages 289–289. Springer, 1994.