

ランダム確率測度と量子超越の実証

間野 修平 数理・推論研究系 教授

1 量子計算とは

古典ゲート(XORとAND):

A	B	$A \oplus B$	A	B	$A \wedge B$
0	0	0	0	0	0
0	1	1	0	1	0
1	0	1	1	0	0
1	1	0	1	1	1

縦ベクトルを $|\cdot\rangle$, 横ベクトルを $\langle\cdot|$ で表す. N 次元ヒルベルト空間 $\mathbb{H}^N \simeq \mathbb{C}^N$ を状態空間とする任意の量子状態 $|\nu\rangle$ は, 正規直交基底

$$|b_1\rangle, \dots, |b_N\rangle, \quad \langle b_j | b_k \rangle = \delta_{jk}, \quad j, k \in [N] := \{1, 2, \dots, N\}$$

に対し, $|\nu\rangle = \langle b_1 | \nu \rangle |b_1\rangle + \dots + \langle b_N | \nu \rangle |b_N\rangle$ と表せる. この基底に対して測定すると, 古典状態 j を $\langle b_j | \nu \rangle$ の確率で得る. つまり, 可能な測定結果は $N-1$ 次元標準単体に属する $\{\|b_j\|^2 : j \in [N]\}$ により特定される. 以降, これを確率ベクトルと呼び, \mathbb{H}^2 をqubitと呼ぶ. 量子ゲートの作用はユニタリ変換で,

1qubit量子ゲート(Y):

$$Y|0\rangle = Y\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = i \begin{pmatrix} 0 \\ 1 \end{pmatrix} = i|1\rangle, \quad i \equiv \sqrt{-1}.$$

$$Y\left\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right\} = \frac{i}{\sqrt{2}}(|1\rangle - |0\rangle).$$

2qubit量子ゲート(CNOT):

A	B	A	B'
00\rangle = 0\rangle 0\rangle	0\rangle 0\rangle	0\rangle 0\rangle	
01\rangle = 0\rangle 1\rangle	0\rangle 1\rangle	0\rangle 1\rangle	
10\rangle = 1\rangle 0\rangle	1\rangle 0\rangle	1\rangle 1\rangle	
11\rangle = 1\rangle 1\rangle	1\rangle 1\rangle	1\rangle 0\rangle	

$$\text{CNOT}\left\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle\right\} = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle).$$

量子状態は測定以外でも意図せず古典状態になるので, 量子状態の維持が技術的挑戦である. 量子状態を維持して測定できたことを, 以降, 成功と呼び, そうでないことを失敗と呼ぶ. 成功の確率を忠実度と呼ぶ.

2 ランダム量子回路による量子超越の実証

量子計算が古典計算を何らかのタスクにおいて何らかの意味で優越することを量子超越という. 古典アルゴリズムを計算複雑性の意味で優越する有用な量子アルゴリズムは存在するが, それらによる実証には技術的, 計算複雑性理論上の困難がある. そこで, 全く有用ではないが, ランダムに生成した量子回路の測定で得られる出力をタスクとし, 古典計算機はそれをシミュレートすることとし, 挑戦されるようになった. 測定における確率ベクトルの古典計算複雑性が確立して, それを多項式時間で計算する古典アルゴリズムが存在すれば, 計算複雑性理論において正しくない信じられている結果(多項式階層の崩壊)を導くからである.

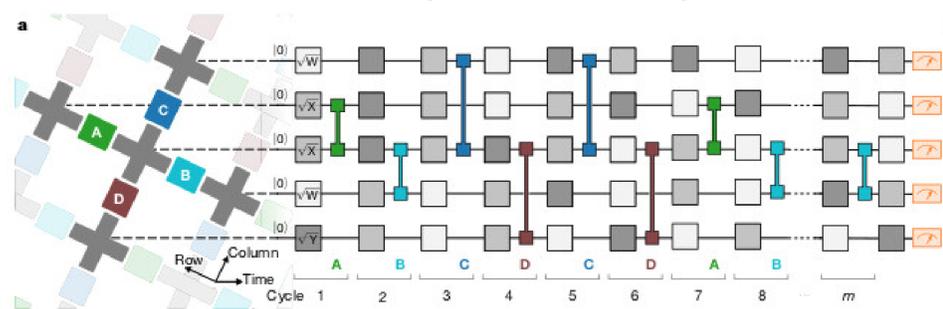


図1: (左) プロセッサの一部. +はqubit (53のうち5), A,B,C,Dはカプラ. (右) 量子回路の表現. 四角は1 qubitゲート, 縦棒は2 qubitゲートで, 決められたゲートの集合から無作為に選んだ. (Arute et al. Nature 2019)

Googleによる量子超越の主張(Arute et al. 2019)の根拠:

量子計算 53 qubit, $m = 20$, $n = 10^6$ の出力(53桁の2進数の長さ 10^6 の列)を200秒で得た.

古典計算 量子回路の実現に対し確率ベクトル π が定まる. 出力はiid列で, 成功すると π によるsize-biased sampling, 失敗すると一様分布に従うとした.

$$\mathbb{P}(X = b_j | \pi) = \phi \pi_{b_j} + (1 - \phi) \frac{1}{N}, \quad \pi = (\pi_1, \dots, \pi_N), \quad j \in [N], \quad N = 2^{53}.$$

忠実度 ϕ は推定する. π は古典計算で求める必要があり, 単純化した回路に対する結果の外挿によれば, 10^6 コアを用いても1万年かかる.

3 ランダム確率測度によるモデル

ランダム量子回路の出力を交換可能列とみなす.

$$\mathbb{P}(X_1, X_2, \dots, X_n) \stackrel{d}{=} \mathbb{P}(X_{\sigma(1)}, X_{\sigma(2)}, \dots, X_{\sigma(n)}).$$

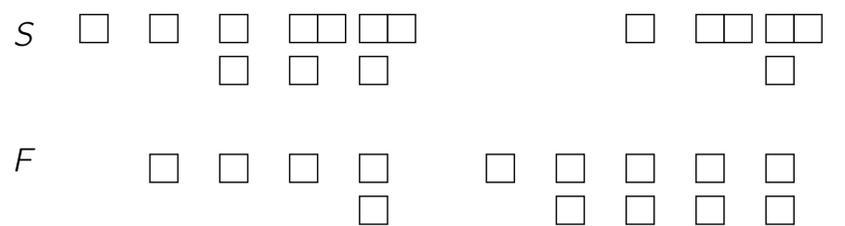
ただし σ は $[n]$, $n \in \mathbb{N}$ の任意の置換. De Finettiの表現定理によれば, 交換可能な確率変数列は何らかのランダム確率測度(de Finetti測度)に従うiid列の混合として表せる. π に対して事前過程 P_θ を用いれば, π の計算は避けられる. 出力の周辺尤度は

$$\mathbb{P}_{\theta, \phi}(X_1 = x_1, \dots, X_n = x_n) = \int \prod_{k=1}^n \left\{ \phi \pi_{x_k} + (1 - \phi) \frac{1}{N} \right\} P_\theta(d\pi)$$

となり, de Finetti測度は P_θ と一様分布の混合で表せる. 母数 (ϕ, θ) は周辺尤度最大化により推定する. P_θ としてDirichlet過程を用いるとき, 以下のアルゴリズムにより出力をシミュレートできる.

アルゴリズム 1. 無数のテーブルがある中華料理店 S と, カウンターのみ 2人の店員 F がある. 客が1人ずつ現れて, S を ϕ , F を $1 - \phi$ で選ぶ.

- S を選んだとき, テーブルに着いている人数に比例するレートで人が座っているテーブルに, レート θ で誰も座っていないテーブルに着く.
- F を選んだときは常に1人.



$$\phi(1 - \phi) \frac{\phi \theta}{1 + \theta + \theta} (1 - \phi) = (1 - \phi)(1 - \phi) \phi \frac{\phi}{1 + \theta + \theta} = \frac{\phi^3 \theta^2 (1 - \phi)^2}{(\theta)_3}$$

図2: 成功3回(2数は同じ), 失敗2回の2通りの出力. 確かに交換可能.

Intel i5 (Let's note CF-S10, 2011) 1コアの結果を外挿すると, 10^6 コアを用いて1.2年かかる.

4 まとめ

ランダムな出力のシミュレートと確率ベクトルの計算は異なる. 交換可能列においてde Finetti測度を混合とするモデルにより, 確率ベクトルを計算することなくランダム量子回路の出力をシミュレートできる. 古典計算の時間を大幅に短縮できるが, 量子計算には敵わないようである.