

# 量子位相推定

9BSP1118 村岡海人

2022年6月22日

## 1 概要

量子位相推定アルゴリズムは、ユニタリ演算子  $U$  とその固有ベクトルの 1 つ  $|\psi\rangle$  が与えられた時、その固有値を求めるアルゴリズムである。このアルゴリズムは数多くの量子アルゴリズムの基礎として使われており、量子アルゴリズムの中で最も重要なものの 1 つである。

### 1.1 アダマールテストの改良

ユニタリ演算  $U$  の固有値  $e^{i\lambda}$  を求める問題を考える。アダマールテストでは、固有値の位相  $\lambda$  はテストの測定結果の確率分布に反映され、測定結果を沢山サンプルすることで  $\lambda$  を推定していた。これを工夫することにより、測定結果から位相の情報を直接取り出す。

アダマールテストを始める前に準備として、 $\lambda/2\pi$  を 2 進数に変換すると、

$$\frac{\lambda}{2\pi} = \frac{j_1}{2^1} + \frac{j_2}{2^2} + \cdots + \frac{j_k}{2^k} + \cdots$$

となる。 $j_k$  は 0 または 1 の値をとる古典ビットである。 $\lambda$  は  $e^{i\lambda}$  の形のみ出てくるので、 $0 \leq \lambda \leq 2\pi$  として一般性を失わない。この 2 進数展開を少数の表記にならって書くと、

$$\begin{aligned} \frac{\lambda}{2\pi} &= \frac{j_1}{2^1} + \frac{j_2}{2^2} + \cdots + \frac{j_k}{2^k} + \cdots \\ \Leftrightarrow \lambda &= (2\pi)0.j_1j_2\cdots j_k\cdots \end{aligned}$$

以下、簡単のため、 $\lambda/2\pi$  は小数点以下  $n$  桁で書けるものとする。

$$\lambda = (2\pi)0.j_1j_2j_3\cdots j_n$$

アダマールテストでは制御ユニタリ演算として  $\Lambda(U)$  を用いたが、今回はそれを変えた  $\Lambda(U^{2^k})$  とする。ユニタリ演算  $U$  の固有状態  $|\psi\rangle$  とすると、制御ユニタリ演算を作成させた後の状態は、

$$\frac{1}{\sqrt{2}} \left( |0\rangle + e^{i2^k\lambda} |1\rangle \right) \otimes |\psi\rangle$$

上記の 2 進数展開を使うと、

$$2^k\lambda = 2^k \cdot (2\pi)0.j_1j_2j_3\cdots j_r = (2\pi)j_1j_2\cdots j_k \cdot j_{k+1}\cdots j_n$$

$e^{i(2\pi)j_1 \dots j_k} = 1$  なので、

$$\frac{1}{\sqrt{2}} \left( |0\rangle + e^{i(2\pi)0.j_{k+1} \dots j_n} |1\rangle \right) \otimes |\psi\rangle \quad (1)$$

となる。

次に、固有値の位相を 1 桁ずつ確定した量子ビットの状態として取り出す。 $k = n - 1$  のとき、

$$\frac{1}{\sqrt{2}} \left( |0\rangle + e^{i(2\pi)0.j_n} |1\rangle \right)$$

となり ( $|\psi\rangle$  は省略)、アダマールゲートを作用させると、

$$\frac{1}{\sqrt{2}} \left( |0\rangle + e^{i(2\pi)0.j_n} |1\rangle \right) \rightarrow |j_n\rangle$$

となる。 $\lambda$  の 2 進小数表示の  $n$  番目のビット  $j_n = \pm 1$  に対応した状態に変換できる。この状態を測定すれば、100% の確率で  $j_n$  が観測されるので、1 回の測定で  $\lambda$  の  $n$  桁目を決定することができる。次に  $k = n - 2$  の時を考えると、状態は

$$\frac{1}{\sqrt{2}} \left( |0\rangle + e^{i(2\pi)0.j_{n-1}j_n} |1\rangle \right)$$

である。 $j_n$  は先ほど調べてあるので、 $j_n = 0$  の時は何もせず、 $j_n = 1$  の時は一般位相ゲート、

$$R_l^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\frac{2\pi}{2^l}} \end{pmatrix}$$

より、 $R_2^\dagger$  を作用させれば、

$$\frac{1}{\sqrt{2}} \left( |0\rangle + e^{i(2\pi)0.j_{n-1}j_n} |1\rangle \right) \rightarrow \frac{1}{\sqrt{2}} \left( |0\rangle + e^{i(2\pi)0.j_{n-1}} |1\rangle \right)$$

と変換できる。そして、アダマールゲートを作用させれば、

$$\frac{1}{\sqrt{2}} \left( |0\rangle + e^{i(2\pi)0.j_{n-1}} |1\rangle \right) \rightarrow |j_{n-1}\rangle$$

となるから、 $j_{n-1}$  もこの状態を 1 回測定するだけで決定できる。

以降、同様に  $k = n - 3, n - 4, \dots, 0$  とすれば下の方の桁から  $j_{k+1}$  を決定していくことができる。

このようにして、アダマールテストを変形することにより、固有値の位相を 1 桁ずつ確定した量子ビットの状態として取り出すことができる。この手続きを量子回路で一度に行うのが量子位相推定アルゴリズムである。

## 1.2 量子位相推定アルゴリズムの概要

量子位相推定アルゴリズムは、上記のアルゴリズムの測定側の量子ビットを拡張し、量子 Fourier 変換を組み合わせたものである。

$U$  を量子回路として構成できる一般的なユニタリ行列とする。 $U$  の固有ベクトルを  $|eigen_l\rangle$  とし、対応する固有値を  $e^{i\lambda_l}$  とする。ある一般的な量子状態  $|\psi\rangle$  が与えられたとする。これは必ず固有ベクトルで展開できるので、

$$|\psi\rangle = \sum_l c_l |eigen_l\rangle$$

となる。具体的に係数  $c_l$  がどのような値になるかはまだわからない。このとき、量子位相推定アルゴリズムは、 $n$  個の補助量子ビットを用いて、入力状態

$$|00\cdots 0\rangle |\psi\rangle$$

を、

$$\sum_l c_l |\lambda_l\rangle |eigen_l\rangle$$

へと変換するアルゴリズムのことである。ここで、 $|\lambda_l\rangle$  は固有値の位相  $\lambda_l$  の 2 進小数表示  $\lambda_l = (2\pi)0.j_1^{(l)}\cdots j_n^{(l)}$  に対応する量子状態  $|j_1^{(l)}\cdots j_n^{(l)}\rangle$  である。

つまり、量子位相推定アルゴリズムは、 $|\psi\rangle$  の重ね合わせの中にあるそれぞれの固有ベクトルに対応した固有値を  $n$  個の補助量子ビットへと取り出すアルゴリズムになっている。この状態に対して補助量子ビットの測定をすると、確率、

$$p_l = |c_l|^2$$

で、どれか 1 つの固有ベクトル  $|eigen_l\rangle$  とその固有値  $\lambda_l$  が乱択される。

このアルゴリズムは、素因数分解や量子化学アルゴリズムなど、多くのアルゴリズムのサブルーチンとして利用されており、量子コンピュータが従来のコンピュータよりも指数的に高速に解を得られると期待される最も重要な例である。

## 2 量子位相推定アルゴリズムの回路

以下、量子状態  $|\psi\rangle$  を固有状態  $|eigen\rangle$  とその固有値  $\lambda$  に限定する。アダマールテストでは 1 つしか測定用の量子ビットを使わなかったが、量子位相推定では、測定用の補助量子ビットとして  $n$  個の量子ビットを確保する。量子位相推定を行う量子回路は図 1 である。

まず初めに、 $|0\rangle$  に初期化された  $n$  個の量子ビットのそれぞれに、アダマールテストと同様にアダマールゲートと制御ユニタリー演算を作用させる。ただし、 $k$  番目 ( $k = 1, \dots, n$ ) の補助量子ビットには制御  $U^{2^{k-1}}$  演算をすることにする。 $U|eigen\rangle = e^{i2\pi\lambda} |eigen\rangle$  だから、 $k$  番目の補助量子ビットには  $e^{i\lambda 2^k}$  の位相が獲得されるので、

$$\left( \frac{|0\rangle + e^{i(2\pi)0.j_1\cdots j_n}|1\rangle}{\sqrt{2}} \right) \otimes \left( \frac{|0\rangle + e^{i(2\pi)0.j_2\cdots j_n}|1\rangle}{\sqrt{2}} \right) \otimes \cdots \otimes \left( \frac{|0\rangle + e^{i(2\pi)0.j_n}|1\rangle}{\sqrt{2}} \right) \otimes |eigen\rangle$$

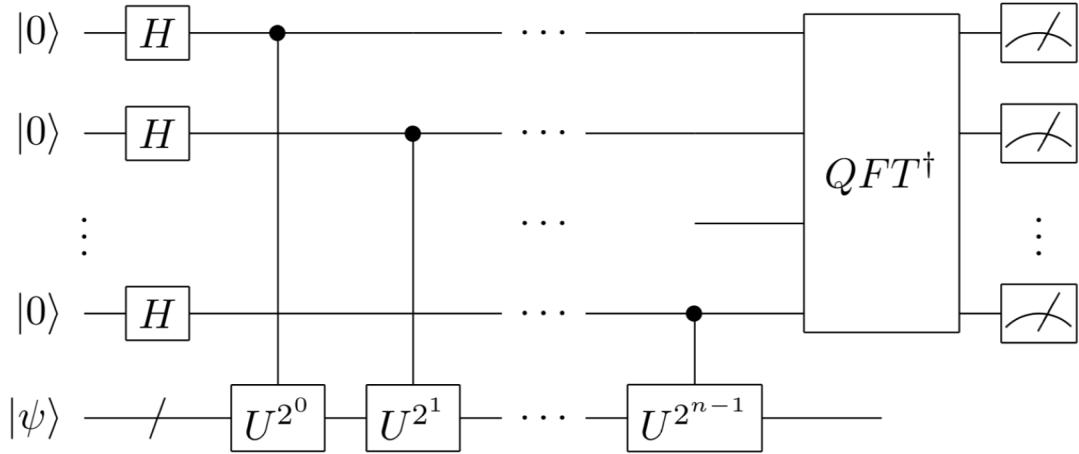


図 1 量子位相推定の量子回路

という状態になる。つまり、固有値の位相を 2 進少数表示で 1 ビットずつシフトしたものが各補助量子ビットの位相に格納されることになる。

次に、 $n$  個の補助量子ビットの状態は、量子フーリエ変換の結果の式と同じ形をしている。よって、逆量子フーリエ変換(図の  $QFT^\dagger$ )をこれらの補助量子ビットに作用させると、

$$\left(\frac{|0\rangle + e^{i(2\pi)0.j_1 \dots j_n}|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + e^{i(2\pi)0.j_2 \dots j_n}|1\rangle}{\sqrt{2}}\right) \otimes \dots \otimes \left(\frac{|0\rangle + e^{i(2\pi)0.j_n}|1\rangle}{\sqrt{2}}\right) \otimes |eigen\rangle \rightarrow |j_1 \dots j_n\rangle$$

となる。よって、この段階で補助量子ビットの測定を行えば、100% の確率で  $j_1, j_2, \dots, j_n$  を得ることができ、 $U$  の固有値の位相  $\lambda$  が求められる。

まとめると、測定用の各量子ビットを制御ビットとする制御  $U^{2^k}$  演算を行い、固有値の位相の情報を補助量子ビットに移した後、逆フーリエ変換で位相の値を取り出すのが、量子位相推定アルゴリズムである。