

Phase Estimation

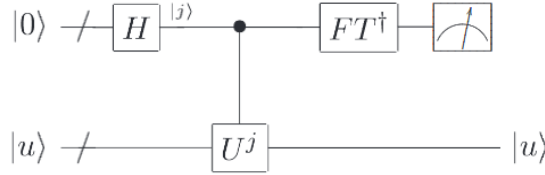
1 位相推定問題

$$U |u\rangle = e^{i2\pi\phi} |u\rangle \quad (1)$$

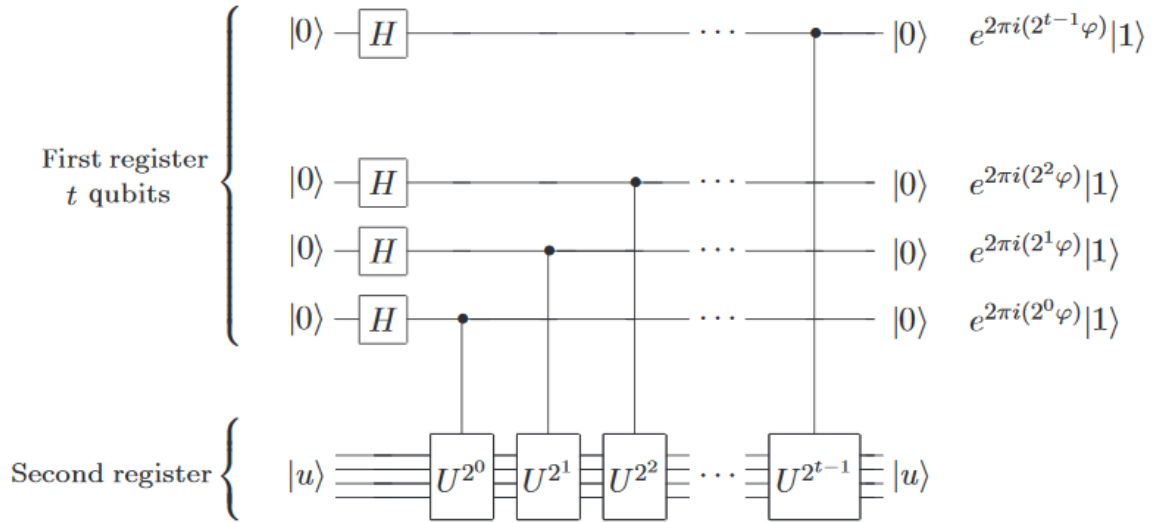
となる ϕ を求めたい.

ϕ は 2 進数表記で $\phi = 0.\phi_1\phi_2\phi_3\dots\phi_n$ の形とする.

位相推定問題を解く回路は



この回路の前半部分の詳しい図は下のようになっている.



1.1 回路の様子

初期状態は

$$|0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle \otimes |u\rangle \quad (2)$$

である. アダマールゲートを通過すると, 状態は

$$\frac{1}{\sqrt{2^n}} (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes \dots \otimes (|0\rangle + |1\rangle) \otimes |u\rangle \quad (3)$$

となり, また $U^{2^k} |u\rangle = UUU\dots U |u\rangle = e^{i2\pi 2^k \phi} |u\rangle$ であるから, 制御ゲート U^j を通過すると, 状態は

$$\frac{1}{\sqrt{2^n}} (|0\rangle + e^{i2\pi 2^{n-1}\phi} |1\rangle) \otimes (|0\rangle + e^{i2\pi 2^{n-2}\phi} |1\rangle) \otimes \dots \otimes (|0\rangle + e^{i2\pi 2^0\phi} |1\rangle) \otimes |u\rangle \quad (4)$$

$$= \frac{1}{\sqrt{2^n}} (|0\rangle + e^{i2\pi 0.\phi_n} |1\rangle) \otimes (|0\rangle + e^{i2\pi 0.\phi_{n-1}\phi_n} |1\rangle) \otimes \dots \otimes (|0\rangle + e^{i2\pi 0.\phi_1\phi_2\dots\phi_n} |1\rangle) \otimes |u\rangle \quad (5)$$

となる. これは ϕ を量子フーリエ変換した結果 (積表示) となっているので, 逆変換を施せば ϕ が得られる.

2 位数計算

互いに素な $N, x (x < N)$ に対して

$$x^r = 1 \bmod N \quad (6)$$

を満たす最小の自然数 r を位数という.

量子コンピュータでこれを解くには

$$U |y\rangle \equiv |xy \bmod N\rangle \quad (7)$$

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{-i2\pi j \frac{s}{r}} |x^j \bmod N\rangle \quad (8)$$

とおくと, 位相推定問題

$$U |u_s\rangle = e^{i2\pi \frac{s}{r}} |u_s\rangle \quad (s = 0, \dots, r-1) \quad (9)$$

を解けばよい.

位相推定問題の回路に, $|u_s\rangle = |1\rangle$ を入れる. 制御 U^k ゲートを通ると,

$$\frac{1}{\sqrt{2^n}} \sum_{k=0}^{N-1} |k\rangle \otimes U^k |1\rangle \quad (10)$$

$$= \frac{1}{\sqrt{2^n}} \sum_k |k\rangle \otimes U^k \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle \quad (11)$$

$$= \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \left(\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp(i2\pi k \frac{\tilde{s}}{r} / N) |k\rangle \right) \otimes |u_s\rangle \quad (12)$$

ここで $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle$, $U |u_s\rangle = e^{i2\pi \frac{s}{r}}$, $\frac{\tilde{s}}{r} = 2^n \frac{s}{r}$ を用いた. 上式のかっこ内は \tilde{s}/r を量子フーリエ変換したものであるから, 逆 QFT で s/r を得られる. 連分数アルゴリズムで $s/r \rightarrow r$ を得る.

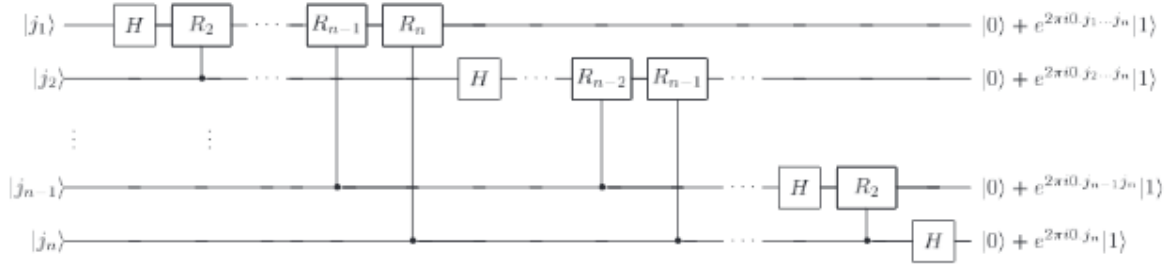
3 量子フーリエ変換の積表示

n ビットの計算基底 $|j\rangle = |j_1 j_2 \dots j_n\rangle$ (このとき $j = j_1 2^{n-1} + j_2 2^{n-2} + \dots + j_n 2^0$) に対する量子フーリエ変換は次のように表せる.

$$\begin{aligned} |j\rangle &\rightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i j k / 2^n} |k\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^1 \dots \sum_{k_n=0}^1 e^{2\pi i j (\sum_{l=1}^n k_l 2^{n-l})} |k_1 \dots k_n\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^1 \dots \sum_{k_n=0}^1 \otimes_{l=1}^n e^{2\pi i j k_l 2^{n-l}} |k_l\rangle \\ &= \frac{1}{\sqrt{2^n}} \otimes_{l=1}^n \left[\sum_{k_l=0}^1 e^{2\pi i j k_l 2^{n-l}} |k_l\rangle \right] \\ &= \frac{1}{\sqrt{2^n}} \otimes_{l=1}^n \left[|0\rangle + e^{2\pi i j 2^{n-l}} |1\rangle \right] \\ &= \frac{1}{\sqrt{2^n}} (|0\rangle + e^{2\pi i 0 \cdot j_n} |1\rangle) \otimes (|0\rangle + e^{2\pi i 0 \cdot j_{n-1} j_n} |1\rangle) \otimes \dots \otimes (|0\rangle + e^{2\pi i 0 \cdot j_1 \dots j_n} |1\rangle) \end{aligned}$$

この積表現から量子フーリエ変換の効率的回路が導ける. ここでゲート R_k は次のユニタリ変換を表す.

$$R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix} \quad (13)$$



- 2^n 要素の量子フーリエ変換は $O(n^2)$
- 最良の古典アルゴリズム (高速フーリエ変換) は $\Theta(n2^n)$

n ビットであらわされる N に対して $2n$ ビットの第一レジスタと n ビットの第二レジスタ