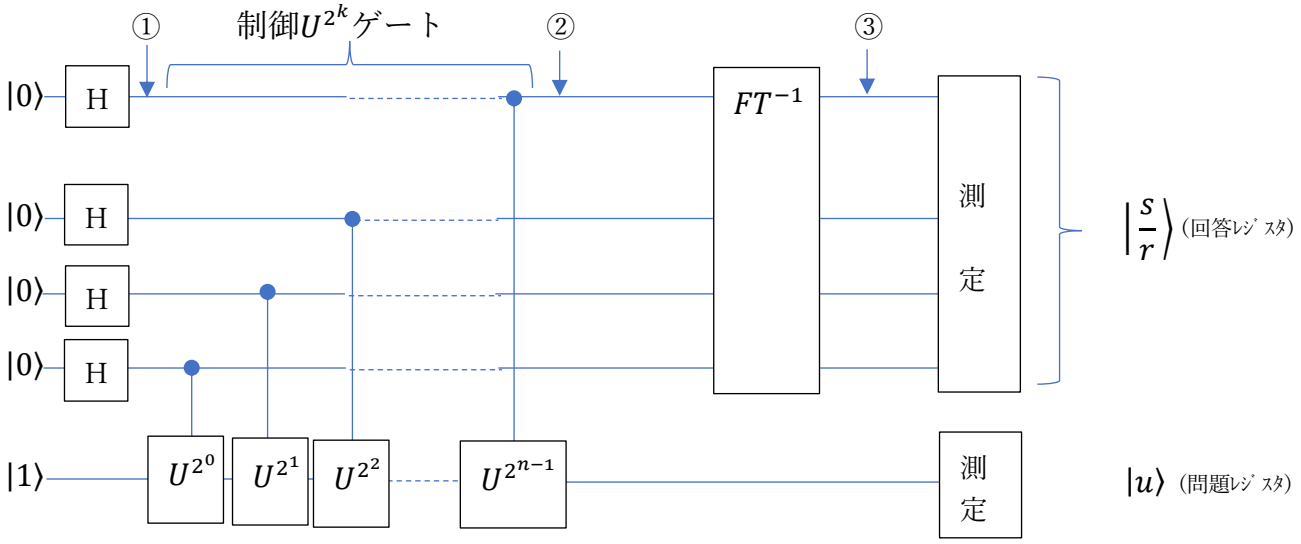
位数計算と素因数分解

$$\frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}|k\rangle \otimes U^k|1\rangle = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}|k\rangle \otimes |x^k \bmod M\rangle$$

ただし　$U|y\rangle = |xy \bmod M\rangle$

上式により、制御U^{2^k}ゲート通過直後の状態（②の状態）は、0 から N-1 までのkによる、$|k\rangle \otimes |x^k$を M で割った余り$\rangle$　の計算結果を重ね合わせた状態になっていることがわかる。



M =15、x = 7　の場合の位数 r を求める。

$$\frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}|k\rangle \otimes |x^k \bmod \mathrm{M}\rangle$$

$$= \frac{1}{\sqrt{2^4}}\sum_{k=0}^{2^4-1}|k\rangle \otimes |7^k \bmod 15\rangle$$

$$= \frac{1}{4}(\,|0\rangle \otimes |7^0 \bmod 15\rangle + |1\rangle \otimes |7^1 \bmod 15\rangle + |2\rangle \otimes |7^2 \bmod 15\rangle + \cdots$$

$$+ |15\rangle \otimes |7^{15} \bmod 15\rangle)$$

$$= \frac{1}{4}(\,|0\rangle \otimes |1\rangle + |1\rangle \otimes |7\rangle + |2\rangle \otimes |4\rangle \; + \; |3\rangle \otimes |13\rangle +$$

$$|4\rangle \otimes |1\rangle + |5\rangle \otimes |7\rangle + |6\rangle \otimes |4\rangle) + |7\rangle \otimes |13\rangle \; + \; \cdots\cdots + |15\rangle \otimes |13\rangle$$

上式では問題レジスターは１、７、４、１３の値が周期的に繰り返されるが、この周期が位数となり、量子計算上では後に続くフーリエ逆変換によりこの周期を求めている。

ショアのアルゴリズムにより、実際に位数計算と素因数分解を行ってみる。

但し、位数計算の部分では、$\sum_{k=0}^{2^n-1}|k\rangle \otimes |x^k \bmod \mathrm{M}\rangle$において、$|x^k \bmod \mathrm{M}\rangle$の周期から位数を求める。

＜ショアのアルゴリズム＞

① Mが偶数なら素因数 2 を出力。

② M=$b^a(a\geqq 1, b\geqq 1)$なら素因数aを出力。

③ 1 から M-1 の間で任意にxを選ぶ。このとき xと M の最大公約数が 1 より大きいなら、その最大公約数を出力。

④ x、M$(x > \mathrm{M})$の位数rを計算する（$x^r \bmod \mathrm{M} = 1$）。
もしrが偶数であり$x^{\frac{r}{2}} \bmod \mathrm{M} \neq -1$ならば、$\gcd(x^{\frac{r}{2}} - 1, \mathrm{M})$と $\gcd(x^{\frac{r}{2}} + 1, \mathrm{M})$を計算し、内 1 つが M の因数ならそれを出力。

⑤　③に戻る。