Shor's Factoring Algorithm

Andreas Klappenecker

Texas A&M University

Create a uniform superposition of the n most significant bits by applying Hadarmard gates

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes |0\rangle.$$

Use modular exponentiation to create the state

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

Measure the second register to observe $a^b \bmod N$. Then we obtain the state

$$\frac{1}{\sqrt{m}} \sum_{z=0}^{m-1} |zr + b\rangle \otimes |a^b \bmod N\rangle$$

The sum extends over all $c = zr + b$ such that $a^c \equiv a^b \bmod N$.

Apply the inverse quantum Fourier transform $QFT_{2^n}^{-1}$

$$\frac{1}{\sqrt{m}} \sum_{z=0}^{m-1} \mathrm{QFT}_{2^n}^{-1} |zr + b\rangle \otimes |a^b \bmod N\rangle$$

$$= \frac{1}{\sqrt{2^n m}} \sum_{c=0}^{2^n-1} \sum_{z=0}^{m-1} \exp\left(-2\pi i (zr + b)c/2^n\right) |c\rangle \otimes |a^b \bmod N\rangle$$

$$= \frac{1}{\sqrt{2^n m}} \sum_{c=0}^{2^n-1} \exp\left(-2\pi i \frac{bc}{2^n}\right) \sum_{z=0}^{m-1} \exp\left(-2\pi i \frac{zrc}{2^n}\right) |c\rangle \otimes |a^b \bmod N\rangle$$

Order Finding

$$\frac{1}{\sqrt{2^n m}} \sum_{c=0}^{2^n-1} \exp\left(-2\pi i \frac{bc}{2^n}\right) \sum_{z=0}^{m-1} \exp\left(-2\pi i \frac{zrc}{2^n}\right) |c\rangle \otimes |a^b \bmod N\rangle$$

$$= \frac{1}{\sqrt{2^n m}} \sum_{c=0}^{2^n-1} \exp\left(-2\pi i \frac{bc}{2^n}\right) \sum_{z=0}^{m-1} \zeta^z |c\rangle \otimes |a^b \bmod N\rangle$$

where $\zeta = \exp(-2\pi i\, rc/2^n)$.

Order Finding

$$\frac{1}{\sqrt{2^n m}} \sum_{c=0}^{2^n-1} \exp\left(-2\pi i \frac{bc}{2^n}\right) \sum_{z=0}^{m-1} \zeta^z |c\rangle \otimes |a^b \bmod N\rangle$$

where $\zeta = \exp(-2\pi i\, rc/2^n)$.

Measure the first register. We observe c with probability

$$\Pr[\text{observe } c] = \frac{1}{2^n m} \left| \sum_{z=0}^{m} \zeta^z \right|^2 = \frac{1}{2^n m} \frac{|1-\zeta^m|^2}{|1-\zeta|^2}$$

$$\Pr[\text{observe } c] = \frac{1}{2^n m} \frac{|1-\zeta^m|^2}{|1-\zeta|^2} = \frac{1}{2^n m} \frac{|2\sin(m\alpha)|^2}{|2\sin(\alpha)|^2}$$

Plotting $\sin(mx)/\sin(x)$ reveals that small values are likely (so values rc mod N close to 0 are likely), and larger values unlikely.