Shor's Algorithm

September 3, 2023

Table of Contents

Table of Contents

Periodic functions

$$f(x+p) = f(x) \text{ for fixed non zero p and all x}$$

r is said to be the period of the function f.

Periodic functions

$$f(x+p) = f(x) \text{ for fixed non zero p and all x}$$

r is said to be the period of the function f.

$$f(x) \equiv a^x \mod N \text{ where gcd(a,N)} = 1$$

$f(x)$ forms a group under multiplication modulo N.
Let the order of this group be r thus $a^r \equiv 1 \mod N$ where r is smallest positive number where this holds

Periodic functions

$$f(x+p) = f(x) \text{ for fixed non zero p and all x}$$

r is said to be the period of the function f.

$$f(x) \equiv a^x \mod N \text{ where gcd(a,N)} = 1$$

$f(x)$ forms a group under multiplication modulo N.
Let the order of this group be r thus $a^r \equiv 1 \mod N$ where r is smallest positive number where this holds

Observe $p = r$ due to $f(x+r) \equiv a^{x+r} \equiv a^x \times a^r \equiv a^x \equiv f(x)$

Table of Contents

Period to factoring

Let $N = pq$ where p and q are old primes
Let $x^r \equiv 1 \mod N$ where r is even and $x^{r/2} \not\equiv \pm 1 \mod N$

Period to factoring

Let $N = pq$ where p and q are old primes
Let $x^r \equiv 1 \mod N$ where r is even and $x^{r/2} \neq \pm 1 \mod N$

$x^r - 1 \equiv 0 \therefore (x^{r/2} - 1)(x^{r/2} + 1) \equiv 0 \therefore (x^{r/2} - 1)(x^{r/2} + 1) = mN$
Observe that $(x^{r/2} - 1)$ and $(x^{r/2} + 1)$ must contain factors of m

Period to factoring

Let $N = pq$ where p and q are old primes
Let $x^r \equiv 1 \mod N$ where r is even and $x^{r/2} \not\equiv \pm 1 \mod N$

$x^r - 1 \equiv 0 \therefore (x^{r/2} - 1)(x^{r/2} + 1) \equiv 0 \therefore (x^{r/2} - 1)(x^{r/2} + 1) = mN$
Observe that $(x^{r/2} - 1)$ and $(x^{r/2} + 1)$ must contain factors of m

Thus $(x^{r/2} - 1)$ and $(x^{r/2} + 1)$ and be written has ca and $c'b$ respectability where $m = c \times c'$.

Period to factoring

Let $N = pq$ where p and q are old primes
Let $x^r \equiv 1 \mod N$ where r is even and $x^{r/2} \neq \pm 1 \mod N$

$x^r - 1 \equiv 0 \therefore (x^{r/2} - 1)(x^{r/2} + 1) \equiv 0 \therefore (x^{r/2} - 1)(x^{r/2} + 1) = mN$
Observe that $(x^{r/2} - 1)$ and $(x^{r/2} + 1)$ must contain factors of m

Thus $(x^{r/2} - 1)$ and $(x^{r/2} + 1)$ and be written has ca and $c'b$ respectability where $m = c \times c'$.

Thus $ca \times c'b = cc'pq \therefore a = pq/b$
Has p and q are prime and a is integer then b must be equal to p or q

Period to factoring

Let $N = pq$ where p and q are old primes
Let $x^r \equiv 1 \mod N$ where r is even and $x^{r/2} \neq \pm 1 \mod N$

$x^r - 1 \equiv 0 \therefore (x^{r/2} - 1)(x^{r/2} + 1) \equiv 0 \therefore (x^{r/2} - 1)(x^{r/2} + 1) = mN$
Observe that $(x^{r/2} - 1)$ and $(x^{r/2} + 1)$ must contain factors of m

Thus $(x^{r/2} - 1)$ and $(x^{r/2} + 1)$ and be written has ca and $c'b$ respectability where $m = c \times c'$.

Thus $ca \times c'b = cc'pq \therefore a = pq/b$
Has p and q are prime and a is integer then b must be equal to p or q

So gcd(ca, N) and gcd(c'b, N) to equal p and q or q and p respectability
gcd$((x^{r/2} - 1), N)$ and gcd$((x^{r/2} + 1), N)$ can be used to find p and q $\square$

Table of Contents

Probability of conditions on r holding

1. $x^{r/2} \neq 1 \mod N$
2. $x^{r/2} \neq -1 \mod N$
3. r is even

1. Holds due to r being the smallest for $x^r \equiv 1 \therefore$ if it didn't hold then r wouldn't be the smallest thus contradiction

2. and 3. are proved to hold at least $\frac{1}{2}$ time for a random x, Appendix M [Mermin, 2007].

Table of Contents

Shor Algorithm Overview

- The first part of this presentation was the classical part of Shor Algorithm, which allows for factoring if you have the period of a periodic function.
- The quantum part of the algorithm acquire this period. It does this by using Quantum Parallelism with Quantum Fourier Transform throw in.
- Fourier Transform decomposes a function into frequency components

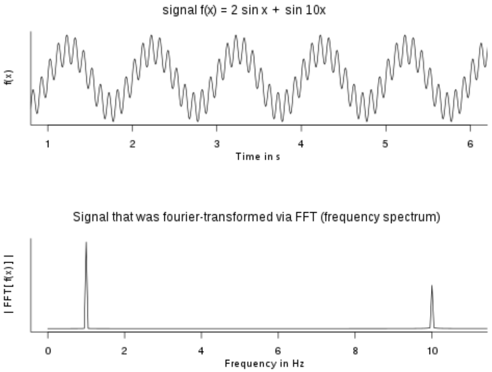
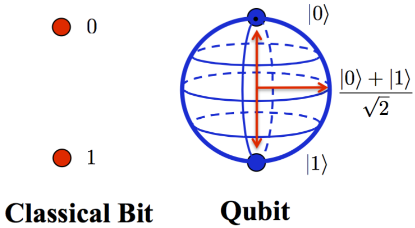


Table of Contents

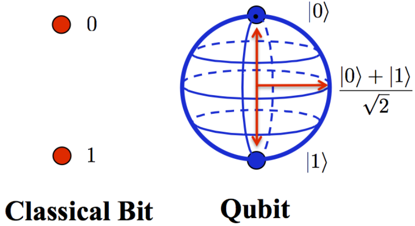
Hadamard gate



$$H^{\otimes n} |x\rangle = \frac{\sum_z (-1)^{X \cdot Z} |z\rangle}{2^{n/2}}$$
$$H^{\otimes n} |000\rangle = \frac{1}{\sqrt{8}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle)$$

$$\sum_{i=0}^{2^n-1} | \alpha_i |^2 = 1$$

Hadamard gate

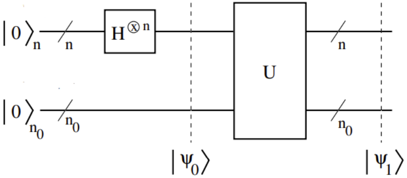


$$H^{\otimes n} |x\rangle = \frac{\sum_z (-1)^{X \cdot Z} |z\rangle}{2^{n/2}} H^{\otimes n} |000\rangle = \frac{1}{\sqrt{8}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |10$$

Using the above the probability of measuring 001 (the first qubit being zero, second zero, third one) is $\frac{(\frac{1}{\sqrt{8}})^2}{\sum_{i=0}^{2^n-1} |\alpha_i|^2} = \frac{1}{8}$

Table of Contents

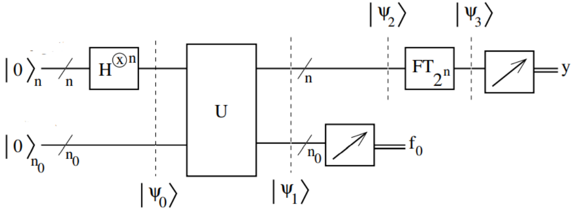
Superpositioned input



We assume $2^n > N^2$ where n is the number of qubits in the first register and $n_0 = \frac{n}{2}$ in second.
[Young, 2022] The state entering U is $|\psi_0\rangle = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n |0\rangle_{n_0}$ and the state exiting from U is $|\psi_1\rangle = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n |f(x)\rangle_{n_0}$ where $f(x) = a^x$ mod N.

U is treated has a black box however under the hood it could use modular exponentiation (same has square and multiple) to achieve this.

Table of Contents

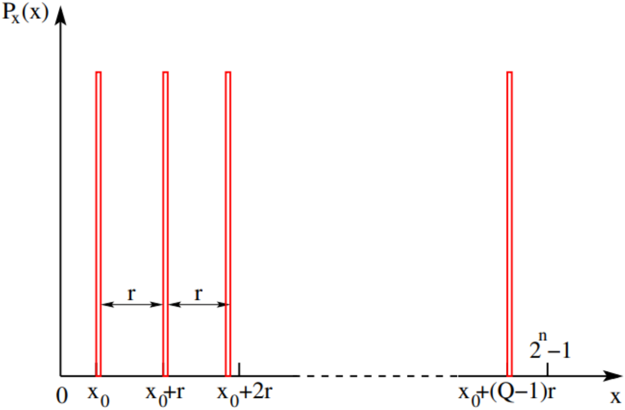


We take a measurement on the lower register which fields f_0 by the extended Born hypothesis the ψ_2 contains a superposition of x where $f(x) = f_0$ i.e $f(x_0 + kr) = f_0$ where $Q = \lfloor \frac{2^n}{r} \rfloor$

$$|\psi_2\rangle = \frac{1}{\sqrt{Q}} \sum_{k=0}^{Q-1} |x_0 + kr\rangle_n$$

FT_{2^n} perform a quantum Fourier transform on ψ_2

$$|\psi_3\rangle = \sum_{p=0}^{2^n-1} \left(\frac{1}{\sqrt{2^n Q}} \sum_{k=0}^{Q-1} e^{2\pi i (x_0+kr)p/2^n} |p\rangle_n \right)$$



The above shows the probability of getting a certain value when we take a measurement on $|\psi_2\rangle = \frac{1}{\sqrt{Q}} \sum_{k=0}^{Q-1} |x_0 + kr\rangle_n$

$$P(y) = \frac{1}{2^n Q} \left| \sum_{k=0}^{Q-1} e^{2\pi i k r y / 2^n} \right|^2$$

let y $= m\frac{2^n}{r} + \delta$, we assume 2^n,r and m is large (this comes from assuming there are at least N periods in the data x thus $2^n > N^2$ [Mermin, 2007])

$$\begin{aligned}
\sum_{k=0}^{Q-1} e^{2\pi i k r y} &= \sum_{k=0}^{Q-1} e^{2\pi i k m} e^{2\pi i k r \delta / 2^n} \\
&= \sum_{k=0}^{Q-1} (-1)^{2km} e^{2\pi i k r \delta / 2^n} \\
&= \sum_{k=0}^{Q-1} e^{2\pi i Q r \delta / 2^n} \\
&= \frac{1 - e^{2\pi i Q r \delta / 2^n}}{1 - e^{2\pi i k m r \delta / 2^n}} \\
&= \frac{e^{\pi i Q r \delta / 2^n} sin(\pi Q r \delta / 2^n)}{e^{\pi i r \delta / 2^n} sin(\pi r \delta / 2^n)}
\end{aligned}$$

$$\sum_{k=0}^{Q-1} e^{2\pi ikry} = \frac{(-1)^{Qr\delta/2^n} sin(\pi Qr\delta/2^n)}{(-1)^{r\delta/2^n} sin(\pi r\delta/2^n)}$$
$$= \frac{sin(\pi Qr\delta/2^n)}{sin(\pi r\delta/2^n)}$$

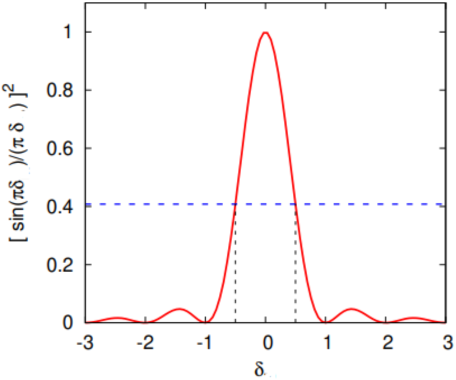
$\therefore$

$$P(y) = \frac{1}{2^n Q} \left| \frac{sin(\pi Qr\delta/2^n)}{sin(\pi r\delta/2^n)} \right|^2$$

Recall that $Q = \lfloor \frac{2^n}{r} \rfloor$ thus Q is at most a one integer away from $\frac{2^n}{r}$ and Q is large $\therefore$ $\frac{Qr}{2^n}$ being 1 is a good approximation.

$\frac{r}{2^n}$ goes small when n is large, since we take n that there are at least N periods and $2^n > N^2$ thus the argument in the sin() is small allowing to us to use the sin() approximation

$$P(y) = \frac{1}{r}\left(\frac{sin(\pi\delta)}{\pi\delta}\right)^2$$



Thus at least 40% of the time δ is within $-\frac{1}{2}$ and $\frac{1}{2}$
Thus y is at most $\frac{1}{2}$ away from $\frac{2^n m}{r}$ 40% of the time. We now assume we have this y.

$$\therefore |y - 2^n \frac{m}{r}| < \frac{1}{2}$$

$$\therefore |\frac{y}{2^n} - \frac{m}{r}| < \frac{1}{2^{n+1}}$$

$$x = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{c_3 + \cdots}}}$$

if $|\frac{y}{2^n} - \frac{m}{r}| < \frac{1}{2r^2}$ then $\frac{m}{r}$ is one of the partial sums in in the continued fraction representation of $\frac{y}{2^2}$, A4.16 in Appendix 4 [Nielsen and Chuang, 2010] Using this you can get the value of $\frac{m}{r}$ if m and r have no common factors then you can get r which happen $\frac{1}{2}$ of the time Appendix J [Mermin, 2007] if not you can do some tricks to get r.

Table of Contents

Summary

- Shor algorithm can find factors of N in polynomial time
- Its probabilistic at two stages in the algorithm meaning you may need to run shor algorithm multiple times on different values of x
- The algorithm is hard to implement, however it was implement on a quantum computer which was able to factor 15

References

Mermin, N. D. (2007).
Quantum Computer Science: An Introduction.
Cambridge University Press, Cambridge.

Nielsen, M. A. and Chuang, I. L. (2010).
Quantum Computation and Quantum Information: 10th Anniversary Edition.
Cambridge University Press.

Young, P. (2022).
An Undergraduate Course on Quantum Computing.
University of California Santa Cruz, California.