Shor's Algo

- Factoring reduces to order finding
- Order finding algo (quantum)
- Analysis intuition
- Postprocessing
- QFT implementation
- Approx QFT

Given integer N (composite)
Return a nontrivial factor of N, i.e., m s.t. $1 < m < N$ and $m \mid N$.

1. If N is even, then return 2 and quit
2. If N is a power of a prime p, then output $\sqrt[k]{N}$ integer
   [$N = p^k$, then $k \le \log_2 N$
   compute $\lfloor \sqrt[2]{N} \rfloor, \lfloor \sqrt[3]{N} \rfloor, \lfloor \sqrt[4]{N} \rfloor, \dots$
   $\dots, \lfloor \sqrt[\log_2 N]{N} \rfloor$ or until
   find that $\sqrt[k]{N}$ is an integer.
   If so, then return $\sqrt[k]{N}$]
3. $N = pq$ for some $p, q > 1$ & coprime.
4. Choose a value $x \in \mathbb{Z}_N$ with $1 < x < N-1$ [uniformly at random]
5. If $\gcd(N, x) > 1$, then output $\gcd(N, x)$ & quit.
6. $x \in \mathbb{Z}_N^*$. Let $\boxed{r := \mathrm{ord}_N(x)}$ Shor's algo
   [$x^r \equiv_N 1$, & $x^s \not\equiv_N 1$ for all $1 \le s < r$]
7. If r is odd, then give up [failure] or go back to Step 4.
8. Compute $y := x^{r/2} \bmod N$
9. If $y \equiv_N \pm 1$, then go to Step 4
10. [$y^2 \equiv_N (x^{r/2})^2 \equiv_N x^r \equiv_N 1$]
    [but $y \not\equiv_N \pm 1$]
    [$\therefore N \mid y^2 - 1 = (y+1)(y-1)$]
    Output $\gcd(N, y-1)$. Success!

Orderfinding algo. | Input: N, $a \in \mathbb{Z}_N^*$ hard-coded into the circuit

1. Initialize two quantum registers in state $\underbrace{|0\rangle}_{\substack{n \text{ qubits} \\ \# \text{ in } \mathbb{Z}_{2^n}}} \otimes \underbrace{|0\rangle}_{\substack{m \text{ qubits} \\ \# \text{ in } \mathbb{Z}_{2^m}}} = |0^n\rangle|0^m\rangle$

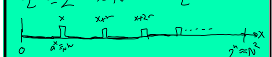
   $m := \lceil \log_2 N \rceil$
   $n := 2m$

2. Apply H gates to all qubits in the 1st register. Get the state
   $$\frac{1}{2^{n/2}} \sum_{x \in \mathbb{Z}_{2^n}} |x\rangle|0\rangle$$
3. Apply classical circuit that computes
   $$(*) \quad |x\rangle|0\rangle \longmapsto |x\rangle|a^x \bmod N\rangle$$
   [modular exponentiation can be computed efficiently by a classical algo
   $\therefore \exists$ quantum circuit that implements $(*)$ efficiently.]
   Get the state
   $$|\varphi\rangle := \frac{1}{2^{n/2}} \sum_{x \in \mathbb{Z}_{2^n}} |x\rangle \otimes |a^x \bmod N\rangle$$
4. (Optional) Measure the 2nd register, obtaining some value $w \in \mathbb{Z}_{2^m}$ that we ignore.
   $|\varphi\rangle$ collapses to
   $$C \sum_{\substack{x \in \mathbb{Z}_{2^n}: \\ a^x \equiv_N w}} |x\rangle \overbrace{|w\rangle}^{\text{don't care}}$$
   [$C > 0$ is a normalization factor]
5. Apply QFT_n to the first register
6. Measure the 1'st register in the computational basis, obtaining some value $y \in \mathbb{Z}_{2^n}$ [done with the quantum circuit]
7. Classically compute the smallest coprime integers $k, r > 0$ such that
   $$\left| \frac{y}{2^n} - \frac{k}{r} \right| \le 2^{-n-1}$$
9. Classically compute $a^r \bmod N$
   If result is 1 then output r and quit. Else give up [fail]

$N \lessapprox 2^m$

$2^n = 2^{2m} \approx N^2$

[$r = \mathrm{ord}(a)$
$r < N$]

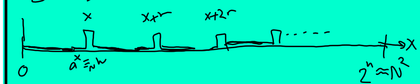


plotting amplitude of $|x\rangle|w\rangle$ (a^x) in $|\varphi\rangle$

QFT_n picks out the fundamental period of a periodic signal

$N \lesssim 2^m$ $\left[\begin{array}{l} r = \mathrm{ord}(a) \\ r < N \end{array}\right.$

$2^n = 2^{2m} \approx N^2$



plotting amplitude of $|x\rangle|\underset{a^x}{w}\rangle$ in $|\varphi\rangle$

QFT_n picks out the fundamental period of a periodic signal

$\Downarrow QFT_n$

Measure — get something close to $\frac{k}{r}$ some k. This is $\frac{y}{2^n}$

$\frac{k'}{r'}$ // $\left[\begin{array}{l} k' < k \\ r' < r \end{array}\right]$

if $\frac{k}{r}$ not in lowest terms

(happens with reasonably low prob)

Finding $\frac{k}{r}$ classically:

SRI(a, b) — "simplest rational interpolant"

$0 < a < b$

returns a rational number (num, denom)

such that $\frac{num}{denom} \in [a, b]$

& num & denom are as small as possible.

To find k, r such that

$$\left|\frac{y}{2^n} - \frac{k}{r}\right| \leq 2^{-n-1}$$

apply $SRI\left(\frac{y}{2^n} - 2^{-n-2}, \frac{y}{2^n} + 2^{-n-2}\right)$

SRI(a,b):

If $1 \in [a,b]$, then return $\frac{1}{1}$

else if $a > 1$ then

let $q \in \mathbb{Z}$ s.t. $q < a$ and $q+1 \geq a$

return $(SRI(a-q, b-q))$

else // $b < 1$

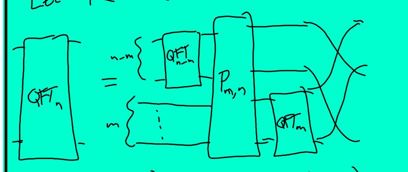
let $z := SRI\left(\frac{1}{b}, \frac{1}{a}\right)$

return $\frac{1}{z}$.

Implementing QFT_n

(induction on n) — Base case: $QFT_1 = H$ (Hadamard gate)

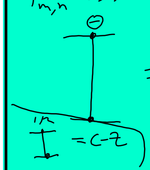
Let $1 \leq m < n$



$P_{m,n}|x, y\rangle = \underbrace{e_n(xy)}_{= e^{\frac{2i\pi xy}{2^n}}}|x, y\rangle$

$x \in \mathbb{Z}_{2^{n-m}}$ $y \in \mathbb{Z}_{2^m}$

$P_{m,n}$ uses 2-qubit controlled phase gates



$$= \begin{bmatrix} 1 & & & 0 \\ & 1 & & \\ & & 1 & \\ 0 & & & e^{2i\pi\theta} \end{bmatrix}$$