Shor's Algorithm

Xabier LEGASPI JUANATEY
Clément LOUIS

M1 Mathématiques de l'information, cryptographie

Université de Rennes 1

Introduction

Let $N = pq \in \mathbb{N}_{\geq 2}$ with p and q two prime numbers.

Introduction

Let $N = pq \in \mathbb{N}_{\geq 2}$ with p and q two prime numbers.

Lemma 3.1.1

Suppose that $x \in [\![1, N-1]\!]$ is a solution $\neq \pm 1 \mod N$ to the equation $x^2 \equiv 1 \pmod{N}$. Then $gcd(x-1, N)$ and $gcd(x+1, N)$ are the non-trivial factors of N.

Introduction

Let $N = pq \in \mathbb{N}_{\geq 2}$ with p and q two prime numbers.

Lemma 3.1.1

Suppose that $x \in [\![1, N-1]\!]$ is a solution $\neq \pm 1 \mod N$ to the equation $x^2 \equiv 1 \pmod N$. Then $gcd(x-1, N)$ and $gcd(x+1, N)$ are the non-trivial factors of N.

Lemma 3.1.2

Let $x \in [\![1, N-1]\!]$ be a uniformly chosen random integer such that $gcd(x, N) = 1$. Define the sets:

$$A := \{x \in [\![1, N-1]\!] : 2 | ord(x, N)\}$$

$$B := \{x \in [\![1, N-1]\!] : x^{\frac{ord(x,N)}{2}} \not\equiv -1 \pmod N\}$$

Then,

$$\mathbb{P}(A \cap B) \geq 1 - \frac{1}{4}$$

Introduction

Shor's algorithm is a quantum algorithm that takes as input a composite integer N and returns a prime factor.

Algorithm 3.1.4 (Idea)

(1) Pick a random number $x \in [\![1, N-1]\!]$ and compute $gcd(x, N)$. If $gcd(x, N) \neq 1$, we have the factorization. Else $gcd(x, N) = 1$ and we jump to step (2).

(2) Find $r = ord(x, N)$.

(3) If (r is odd or $x^r \equiv -1 \pmod{N}$) go to the first step, else $x^{\frac{r}{2}} - 1$ and $x^{\frac{r}{2}} + 1$ are the non-trivial factors of N.

Introduction

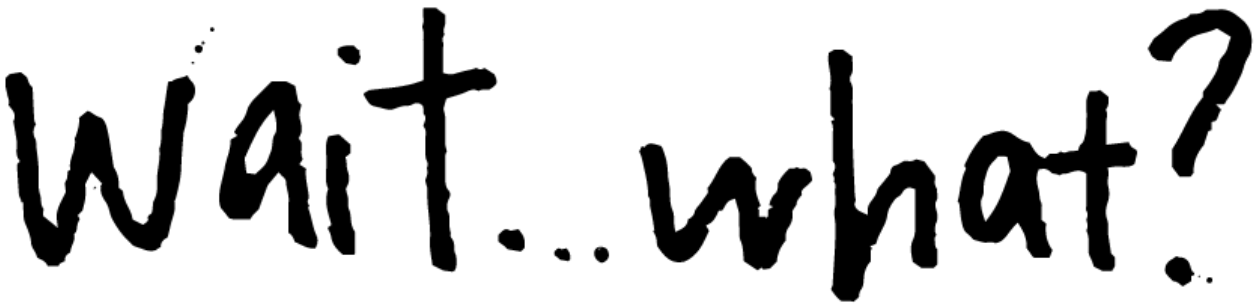
Shor's algorithm is a quantum algorithm that takes as input a composite integer N and returns a prime factor.

Algorithm 3.1.4 (Idea)

(1) Pick a random number $x \in [\![1, N-1]\!]$ and compute $gcd(x, N)$. If $gcd(x, N) \neq 1$, we have the factorization. Else $gcd(x, N) = 1$ and we jump to step (2).

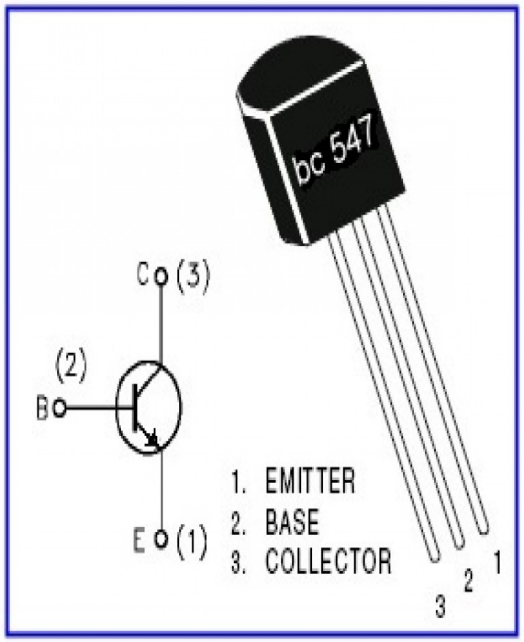
(2) Find $r = ord(x, N)$.

(3) If (r is odd or $x^r \equiv -1 \pmod{N}$) go to the first step, else $x^{\frac{r}{2}} - 1$ and $x^{\frac{r}{2}} + 1$ are the non-trivial factors of N.

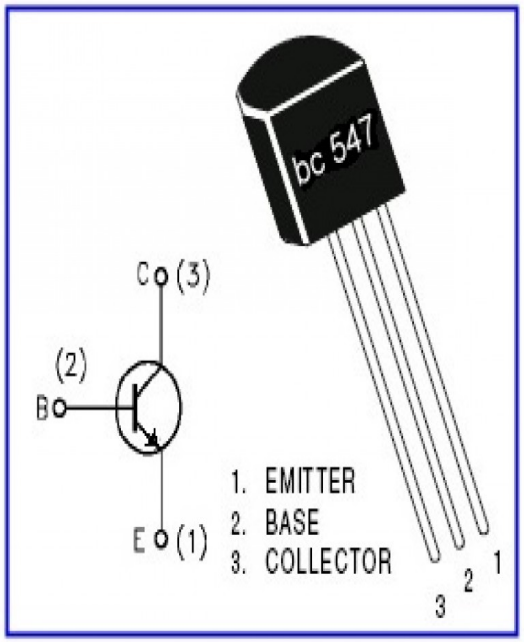


Transistors

- Transistor, 1947 (Bardeen, Brattain, Shocklay).

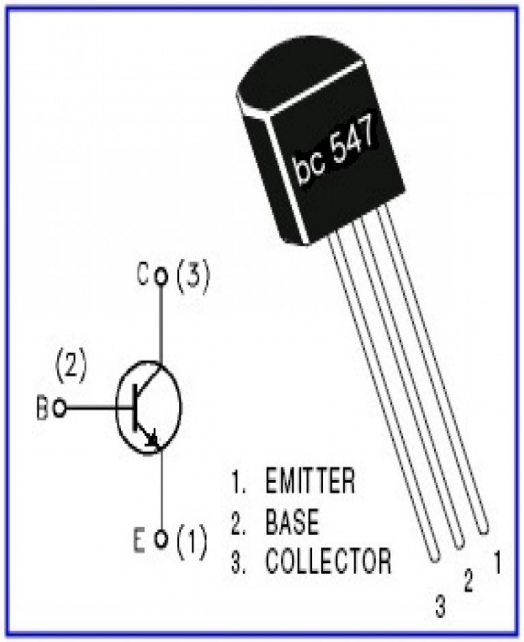


Transistors



- Transistor, 1947 (Bardeen, Brattain, Shocklay).
- Moore's law, 1965:
  - (1) Every 18 months, the number of transistors per square inch on integrated circuits (chips) is multiplied by a factor of 2.
  - (2) The capital cost of every new generation of integrated circuits is also multiplied by a factor of 2.

Transistors

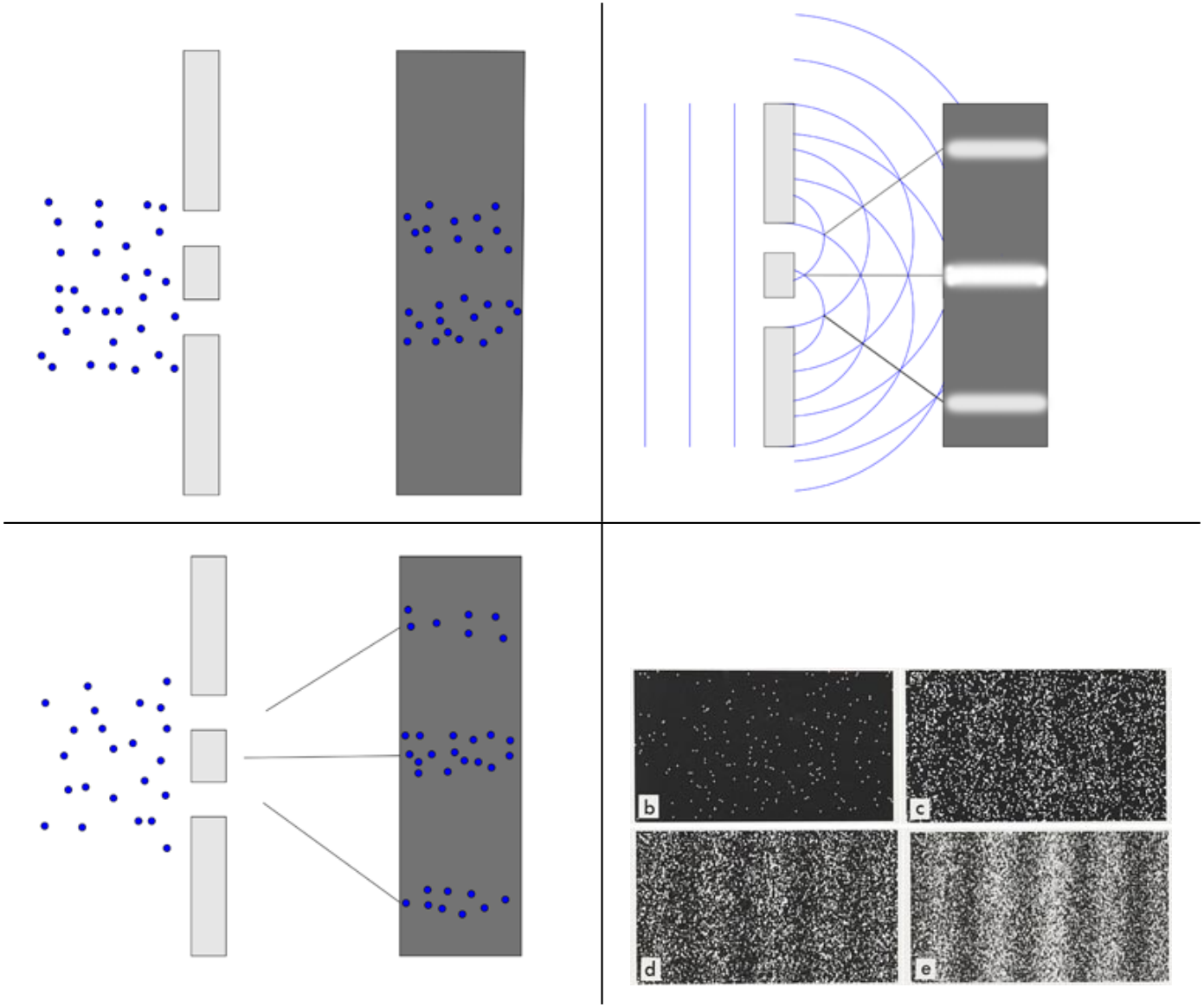


- Transistor, 1947 (Bardeen, Brattain, Shocklay).
- Moore's law, 1965:
  - (1) Every 18 months, the number of transistors per square inch on integrated circuits (chips) is multiplied by a factor of 2.
  - (2) The capital cost of every new generation of integrated circuits is also multiplied by a factor of 2.
- Quantum effects: ≤ 100 *nm* ($nm = 10^{-9}m$) or very low temperature.
- Size of smallest transistor: 5 *nm*, commerciable in 2020.

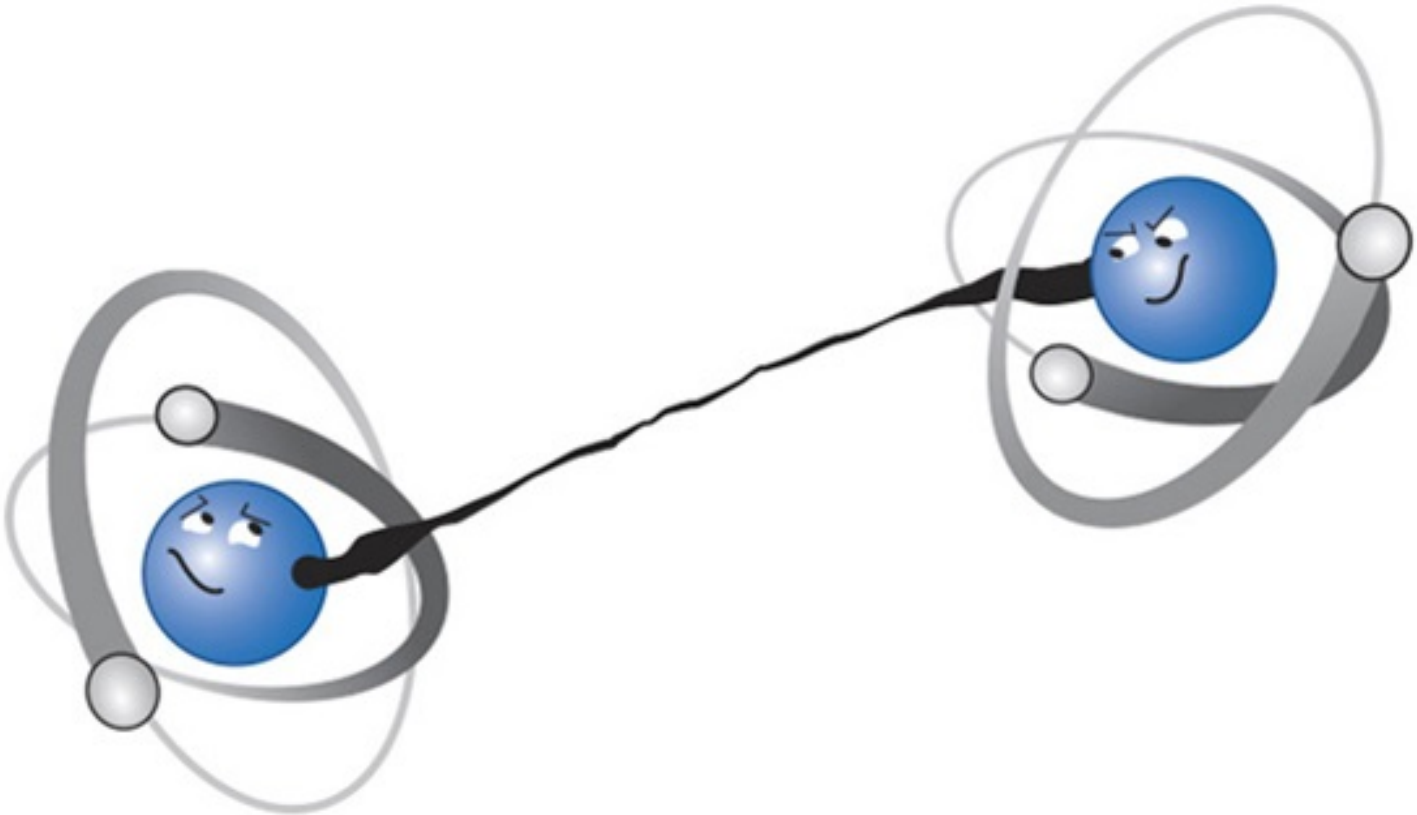
Index

Quantum Effects

Quantum Effects: Superposition



Quantum Effects: Entanglement



Qubits

Qubits

Obtaining information of a physical system.

Postulate	**Classical**	**Quantum**
States	$\rho\colon (\Omega, \mathcal{F}) \to [0,1]$	$\lvert\psi\rangle \in \mathcal{H}$, $\langle\psi\vert\psi\rangle = 1$
Questions	$X\colon (\Omega, \mathcal{F}) \to (\mathbb{X}, \mathcal{X})$, $\mathbb{X} \subset \mathbb{R}$	$A\colon \mathcal{H} \to \mathcal{H}$ self-adjoint
Measurement	$\mathbb{P}_\rho(x) := \rho(X^{-1}(x))$, $x \in \mathbb{X}$	$\mathbb{P}_\psi(\psi_j) := \lVert E_j \lvert\psi\rangle \rVert^2$ $\{\lvert\psi_j\rangle\} \subset H$
Dynamics	$T\colon (\Omega, \mathcal{F}) \to (\Omega, \mathcal{F})$	$U\colon \mathcal{H} \to \mathcal{H}$ unitary
Composition	$(\Omega_1 \times \Omega_2, \mathcal{P}(\Omega_1 \times \Omega_2))$ Conj. prob. measure of ρ_1, ρ_2	$\mathcal{H}_1 \otimes \mathcal{H}_2$ $\lvert\psi\rangle_1 \otimes \lvert\psi\rangle_2$

Qubits

Definition

A *qubit* is a state of the quantum system defined by the Hilbert space $\mathcal{H} = \mathbb{C}^2$ with inner product $\langle \psi | \varphi \rangle = \psi_{(1)} \overline{\varphi}_{(1)} + \psi_{(2)} \overline{\varphi}_{(2)}$. A *n−qubit register* of $|\psi_1\rangle, \ldots, |\psi_n\rangle \in \mathbb{C}^2$ is the state $|\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$ of the composite quantum system $\mathcal{H}^{\otimes n} = (\mathbb{C}^2)^{\otimes n}$.

- Electron, photon.
- $|0\rangle, |1\rangle$ canonical basis.
- Superposition: $\alpha |0\rangle + \beta |1\rangle$.
- *Unentanglement* $\equiv \otimes \equiv$ "*Concatenation*".

Elements of Computing

Definition 2.1.1

(I) A *Boolean function* is a function $f : \{0,1\}^m \to \{0,1\}^n$ from some number m of input bits to some number n of output bits.

(II) Let f be a Boolean function and $\mathbb{B}$ be a fixed set of Boolean functions. We call *Boolean circuit* of f in terms of the basis $\mathbb{B}$ a representation of f in terms of functions from $\mathbb{B}$.

Definition 2.1.1

(I) A *Boolean function* is a function $f : \{0,1\}^m \to \{0,1\}^n$ from some number m of input bits to some number n of output bits.

(II) Let f be a Boolean function and $\mathbb{B}$ be a fixed set of Boolean functions. We call *Boolean circuit* of f in terms of the basis $\mathbb{B}$ a representation of f in terms of functions from $\mathbb{B}$.

Elementary classical gates.

NOT($\neg$)	
Input	Output
0	1
1	0

AND($\wedge$)		
Input		Output
0	0	0
0	1	0
1	0	0
1	1	1

OR($\vee$)		
Input		Output
0	0	0
0	1	1
1	0	1
1	1	1

XOR($\oplus$)		
Input		Output
0	0	0
0	1	1
1	0	1
1	1	0

Elements of Computing

- A quantum circuit implements a unitary operator $U\colon \mathbb{C}^2 \to \mathbb{C}^2$ using quantum gates, which are also unitary operators.

Elements of Computing

- A quantum circuit implements a unitary operator $U\colon \mathbb{C}^2 \to \mathbb{C}^2$ using quantum gates, which are also unitary operators.

Elementary quantum gates.

Hadamard (H)
$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
$H\left\|j\right\rangle = \frac{1}{\sqrt{2}}((-1)^j \left\|j\right\rangle + \left\|1-j\right\rangle)\,\forall j \in \{0,1\}$

$\phi-$**phase** $(\Phi(\phi))$
$\begin{pmatrix} 1 & 0 \\ 0 & exp(2i\phi) \end{pmatrix}$
$\Phi(\phi)\left\|j\right\rangle = exp(2ij\phi)\,\forall j \in \{0,1\}$

NOT (N)
$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
$N\left\|j\right\rangle = \left\|1-j\right\rangle\ \forall j \in \{0,1\}$

Quantum Fourier Transform

Quantum Fourier Transform

Definition 3.2.1

(I) The *Discrete Fourier Transform* is the complex map

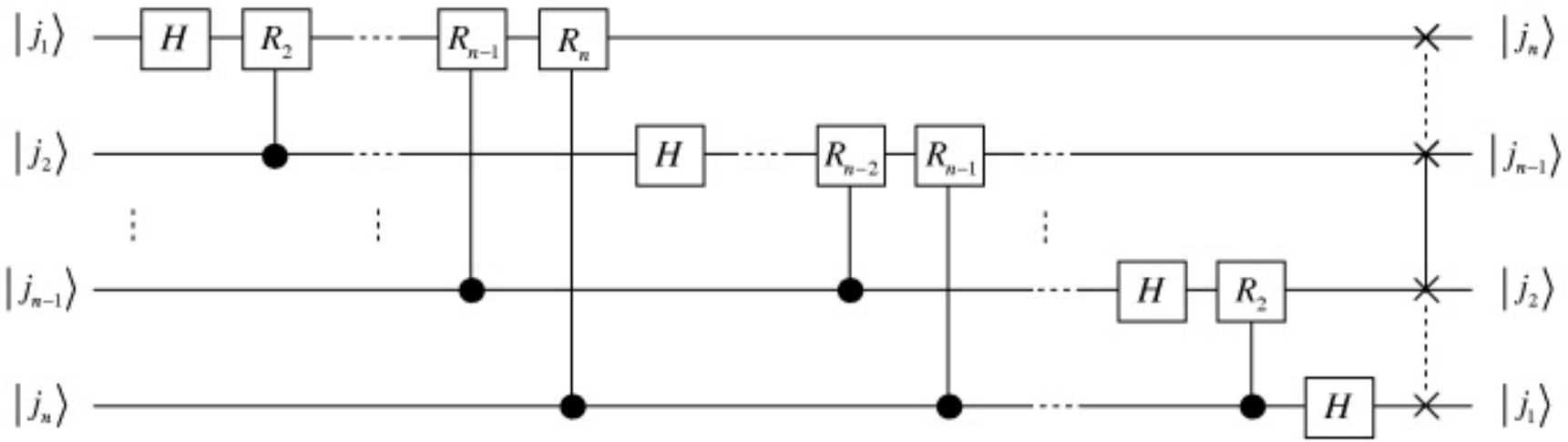
$$F : \mathbb{C}^n \to \mathbb{C}^n, x = (x_j)_{j=0}^{n-1} \mapsto F(x) = \left(\frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} exp\left(\frac{2\pi ik}{n} j\right)\right)_{j=0}^{n-1}$$

(II) The *Quantum Fourier Transform* is the operator defined by

$$\mathcal{F} : \mathbb{C}^n \to \mathbb{C}^n, |j\rangle \mapsto \mathcal{F}|j\rangle = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} exp\left(\frac{2\pi ik}{n} j\right) |k\rangle$$

$\forall j \in \{0, \ldots, n-1\}$

Quantum Fourier Transform



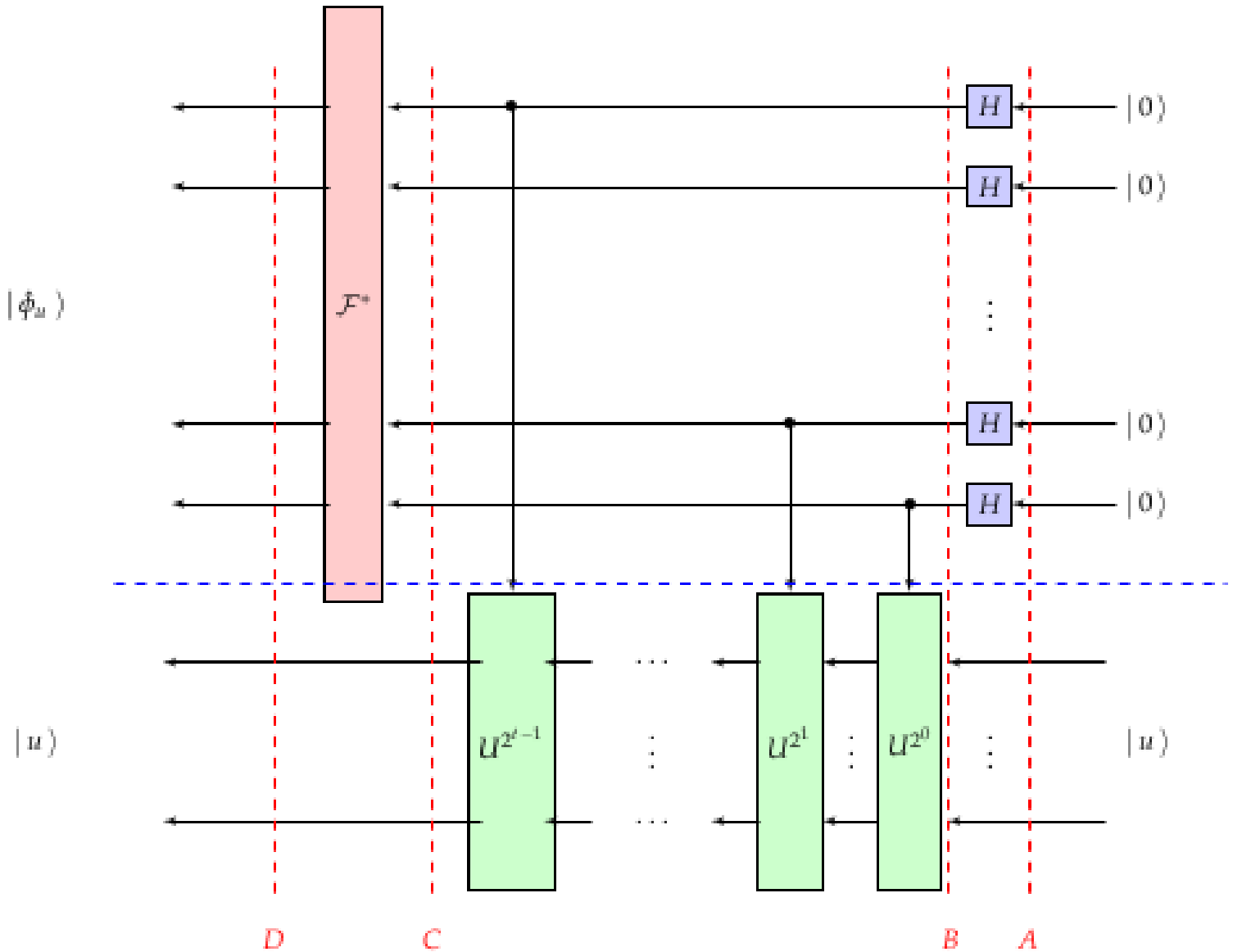
Quantum Phase Estimation

Quantum Phase Estimation

Let $n \in \mathbb{N}_{\geq 1}$ be arbitrary fixed. Let $U\colon (\mathbb{C}^2)^{\otimes n} \to (\mathbb{C}^2)^{\otimes n}$ be a unitary operator and $|u\rangle \in (\mathbb{C}^2)^{\otimes n}$ an eigenvector of U. The *quantum phase estimation problem* consists in determine $\phi_u \in [0, 1]$ such that

$$U|u\rangle = exp(2\pi i \phi_u)|u\rangle$$

Quantum Phase Estimation



Quantum Phase Estimation

- The input of the circuit is composed by a 1^{st} $t-$qubit register $|0\rangle^{\otimes t} \in (\mathbb{C}^2)^{\otimes t}$ tensored with a 2^{nd} $n-$qubit register $|u\rangle \in (\mathbb{C}^2)^{\otimes n}$ (the eigenvector of U).
- Can we obtain ϕ_u accurate to some $\nu \in \mathbb{N}$ bits with large probability?

Order Finding Algorithm

Order Finding Algorithm

Two ingredients.

Order Finding Algorithm

Two ingredients.

Definition 3.4.1

Let $x, N \in \mathbb{Z}_{\geq 2}$ such that $pgcd(x, N) = 1$ and let $n = \lceil logN \rceil$. We define the *order finding operator* of x modulo N to be the mapping

$$OF_{x,N} \colon (\mathbb{C}^2)^{\otimes n} \to (C^2)^{\otimes n}, |y\rangle \mapsto OF_{x,N}\,|y\rangle := \begin{cases} |xy \mod N\rangle & y \in [\![0, N-1]\!] \\ |y\rangle & y \in [\![N, 2^n - 1]\!] \end{cases}$$

Order Finding Algorithm

Two ingredients.

Definition 3.4.1

Let $x, N \in \mathbb{Z}_{\geq 2}$ such that $pgcd(x, N) = 1$ and let $n = \lceil logN \rceil$. We define the *order finding operator* of x modulo N to be the mapping

$$OF_{x,N} \colon (\mathbb{C}^2)^{\otimes n} \to (C^2)^{\otimes n}, |y\rangle \mapsto OF_{x,N}|y\rangle := \begin{cases} |xy \mod N\rangle & y \in [\![0, N-1]\!] \\ |y\rangle & y \in [\![N, 2^n - 1]\!] \end{cases}$$

Proposition 3.4.3

Let $r = ord(x, N)$, $n = \lceil logN \rceil$ and define

$$|u_s\rangle := \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} exp(-\frac{2\pi iks}{r}) \left| x^k \mod N \right\rangle \in (\mathbb{C}^2)^{\otimes n} \qquad \forall s \in [\![0, r-1]\!]$$

Then

(i) $OF_{x,N}|u_s\rangle = exp(\frac{2\pi is}{r})|u_s\rangle$

(ii) $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle$

Order Finding Algorithm

Continued Fraction Expansion (**CFE**)

Require: $\alpha \in \mathbb{R}_{>0}$, $M \in \mathbb{Z}_{>0}$

Ensure: $a_0, \ldots, a_M$ such that $[a_0; a_1, \ldots, a_m] = \frac{p_m(\alpha)}{q_m(\alpha)}$

$m \leftarrow 0$

while $m \leq M$ **do**

$a_m \leftarrow \lfloor \alpha \rfloor$

$\beta \leftarrow \alpha - \lfloor \alpha \rfloor$

$m \leftarrow m + 1$

if $\beta \neq 0$ **then**

$\alpha \leftarrow \frac{1}{\beta}$

else

$\alpha \leftarrow 0$

end if

end while

Order Finding Algorithm

Algorithm (**OF**)

Require: $x, N \in \mathbb{Z}_{\geq 2}$ such that $pgcd(x, N) = 1$
Ensure: $ord(x, N)$ with probability $1 - \varepsilon$
Set up the $QPE_{x,N}$ circuit
$\theta \leftarrow QPE_{x,N}$ (a $(2n+1)-$bit approximation of a $\frac{s}{r}$)
$\alpha := [a_0; a_1, \ldots, a_m] \leftarrow CFE(\theta)$
$\frac{s}{r} \leftarrow \frac{p_m(\alpha)}{q_m(\alpha)}$
if $x^r \equiv 1 \pmod{N}$ **then**
  return r
else
  return "The algorithm fails"
end if

Proposition 3.4.12

The probability that r is the correct order is $\geq \frac{1}{4}$ and can be arbitrarily improved at the expense of several independent repetitions of the $QPE_{x,N}$ circuit.

Summary

Algorithm (**SHOR**)

Require: $N \in \mathbb{Z}_{>0}$ of n bits such that $N = pq$ with p, q primes, $\varepsilon \in]0, 1[$.
Ensure: p, q with probability $1 - \varepsilon$.

Set up the $QPE_{x,N}$ circuit with the given ε.
$x, r \leftarrow 1$
while r is odd **or** $x^r \equiv -1 \pmod{N}$ **do**
  $x \leftarrow (\llbracket 1, N-1 \rrbracket).\text{random\_element}()$
  $r \leftarrow OF(x, N)$
end while
if $r ==$"The algorithm fails" **then**
  return r
else
  $p \leftarrow x^{\frac{r}{2}} - 1$
  $q \leftarrow x^{\frac{r}{2}} + 1$
  return p, q
end if

Bibliography

- R. Coolman, *What Is Quantum Mechanics?*. Article, Live Science, 2014. Available at: `https://www.livescience.com/33816-quantum-mechanics-explanation.html`
- R.P. Feynman, *Simulating Physics with Computers*, International Journal of Theoretical Physics, vol. 21, no. 6/7, pp. 467–488, 1982.
- S. Lang, *Introduction to Diphantine Approximations*, chap. 1. Springer-Verlag, New York, 2nd edition, 1995.
- F. Xi Lin, *Shor's Algorithm and the Quantum Fourier Transform*. McGill University, 2013.
- J. von Neumann, *Mathematical Foundations of Quantum Mechanics*, 1932.
- M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.
- D. Petritis, *Quantum Mechanics: Foundations and Applications*. Lecture Notes, Université de Rennes 1, 2018. Available at: `https://perso.`

Thanks!