A theoretical approach to Shor's Algorithm and Quantum Bits

Francesco Stocco
March 26, 2021

Outline

1. Introduction to Qubits
2. Quantum Fourier Transform over $\mathbb{Z}/2^n\mathbb{Z}$
3. Shor's Algorithm
   - Hidden Subgroup Problem
   - Quantum Phase Estimation
4. Breaking RSA

1- Introduction to Qubits

1. A *hermitian space* is a finite dimensional vector space V over $\mathbb{C}$ equipped with a *hermitian form*

$$\langle\cdot,\cdot\rangle : V^2 \longrightarrow \mathbb{C},$$

that is

- sesquilinear:

$$\langle \lambda x + \mu x', y\rangle = \bar{\lambda}\langle x, y\rangle + \bar{\mu}\langle x', y\rangle$$
$$\langle x, \lambda y + \mu y'\rangle = \lambda\langle x, y\rangle + \mu\langle x, y'\rangle$$

- symmetric: $\langle x, y\rangle = \overline{\langle y, x\rangle}$
- positive: $\langle x, x\rangle > 0$ if $x \neq 0$.

2. We define also for $x \in V$ the norm $||x|| = \sqrt{\langle x, x\rangle}$.
3. Let V, W[1] be hermitian spaces, $f : V \to W$ is a *unitary morphism* if it is $\mathbb{C}$-linear and

$$\langle f(x), f(y)\rangle = \langle x, y\rangle \qquad \forall x, y \in V.$$

[1] actually we will consider always $V = W$ in this presentation.

Definition

An *n-qubit* is a vector of norm 1 in a hermitian space $V \cong \mathbb{C}^{2^n} = (\mathbb{C}^2)^{\otimes n}$. The set of n-qubits is denoted by Q_n.

In the case $n = 1, 2$:

- 1-qubits: $|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$;
- 2-qubits: $|00\rangle := \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$, $|01\rangle := \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$, $|10\rangle := \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$, $|11\rangle := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$.

- Let $x, n \in \mathbb{N}$ with $2^n > x$, then the x^{th} vector of the $n-$qubits basis is represented as

$$|x\rangle_n = |x_{n-1}x_{n-2}\dots x_0\rangle = |x_{n-1}\rangle \otimes |x_{n-2}\rangle \cdots \otimes |x_0\rangle\,,$$

where $x = \sum_{j=0}^{n-1} 2^j x_j$.

- A generic n-qubit is represented as a *superposition*

$$|\psi\rangle_n = \sum_{x=0}^{2^n-1} \alpha_x |x\rangle_n \text{ with } \sum_{x=0}^{2^n-1} |\alpha_x|^2 = 1.$$

Let n, m be positive integers, there's a bilinear map

$$\begin{aligned} Q_n \times Q_m &\longrightarrow Q_{n+m} \\ (\left|\psi\right\rangle_n, \left|\phi\right\rangle_m) &\longmapsto \left|\psi\right\rangle_n \otimes \left|\phi\right\rangle_m . \end{aligned}$$

As an example

$$\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} .$$

Notice that a 2-qubit is not always given by two 1-qubits. As an example

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \neq |\psi\rangle_1 \otimes |\phi\rangle_1 \qquad \forall\, |\psi\rangle_1, |\phi\rangle_1 \in Q_1.$$

However, we have clearly that Q_2 is spanned by 2-qubits that are given by two 1-qubits.

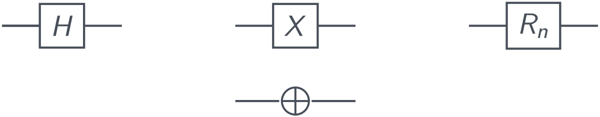
Gates acting on Q_1

Hadamard	$\mathbf{H} : \lvert x\rangle \mapsto \frac{1}{\sqrt{2}}(\lvert 0\rangle + (-1)^x \lvert 1\rangle)$
NOT	$\mathbf{X} : \lvert x\rangle \mapsto \lvert x \oplus 1\rangle$
Phase Shift	$\mathbf{R}_n : \lvert x\rangle \mapsto e^{\frac{2\pi i x}{2^n}} \lvert x\rangle$

Matrix representations

$$\mathbf{H} : \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \mathbf{X} : \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \mathbf{R}_n : \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i x}{2^n}} \end{pmatrix}$$

Circuit notation



Quantum gates

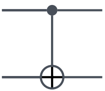
Gates acting on Q_2

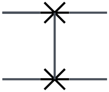
Controlled NOT	$\mathbf{CX} : \lvert xy\rangle \mapsto \lvert x, y \oplus x\rangle$
SWAP	$\mathbf{SWAP} : \lvert xy\rangle \mapsto \lvert yx\rangle$

Matrix representations

$$\mathbf{CX} : \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad \mathbf{SWAP} : \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Circuit notation





Let $f:\{0,1\}^n \to \{0,1\}^m$, up to special cases we cannot define a gate acting as

$$\begin{aligned}\mathbf{U}_f:\ Q_n &\longrightarrow Q_m\\ \left|x\right\rangle_n &\longmapsto \left|f(x)\right\rangle_m\end{aligned}$$

because is not generally a unitary transformation from a space to itself. Then we consider

$$\begin{aligned}\mathbf{U}_f:Q_{n+m} &\longrightarrow Q_{n+m}\\ \left|x\right\rangle_n \otimes \left|y\right\rangle_m &\mapsto \left|x\right\rangle_n \otimes \left|y \oplus f(x)\right\rangle_m .\end{aligned}$$

Measuring Qubits

Let $|\psi\rangle_n$ be a superposition of n-qubits. If we want to measure the k first qubits, we write

$$|\psi\rangle_n = \sum_{x=0}^{2^k-1} |x\rangle_k \otimes |\psi_x\rangle_{n-k}\,.$$

The outcome of the measure is x and the quantum state is left to

$$\frac{|x\rangle_k \otimes |\psi_x\rangle_{n-k}}{||\,|\psi_x\rangle_{n-k}\,||},$$

with probability

$$|||\psi_x\rangle_{n-k}||^2.$$

Circuit notation 

2- Quantum Fourier Transform over $\mathbb{Z}/2^n\mathbb{Z}$

Definition

Let x be a an integer in $\{0, \ldots, 2^n - 1\}$, we define the *Quantum Fourier Transform over* $\mathbb{Z}/2^n\mathbb{Z}$ of the n-qubit $|x\rangle_n$ as

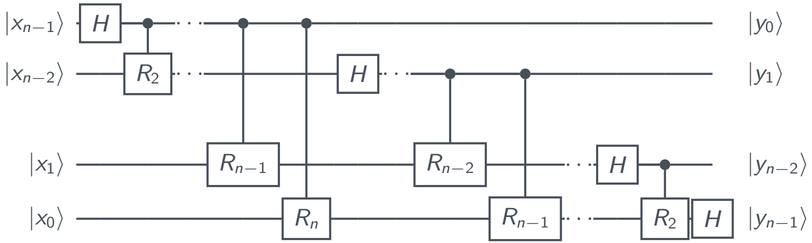
$$\mathbf{QFT}_n(|x\rangle_n) = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{\frac{2\pi xy}{2^n}} |y\rangle_n .$$

Let w_k be $e^{\frac{2\pi i}{2^k}}$, then we will need later also the equality:

$$\mathbf{QFT}_n(|x\rangle_n) = \frac{|0\rangle + w_1^x |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + w_2^x |1\rangle}{\sqrt{2}} \otimes \cdots \otimes \frac{|0\rangle + w_n^x |1\rangle}{\sqrt{2}}. \tag{1}$$

QFT_n circuit

The quantum circuit which performs the Quantum Fourier Transform is constructed out of Hadamard and Controlled Phase Shift gates.



3- Shor's Algorithm

Let N be a positive integer and a be an integer such that $\gcd(a, N) = 1$, then Shor's algorithm aim is to find the period of the function

$$f(x) = a^x \mod N,$$

with time complexity polynomial in $\log_2 N$.

The algorithm is divided in a main quantum part and a classical post processing. The interpretation of the quantum part is the subject of this presentation.

3.1- Hidden Subgroup Problem

Hidden Subgroup Problem

Problem

Let G be a finitely generated group and X be a set. Given a function $f : G \to X$ such that there exists a subgroup $H < G$ with the following property

$$f(g) = f(g') \Leftrightarrow g' = gh \; \exists h \in H,$$

find a generating set for H.

Let G be a group, a *character of G* is a group homomorphism $\chi : G \to \mathbb{C}^*$. The set $\hat{G}$ of characters of G is called the *dual group of G*.

Indeed, the set $\hat{G}$, equipped with

$$\begin{aligned} \hat{G} \times \hat{G} &\longrightarrow \hat{G} \\ (\chi_1, \chi_2) &\longmapsto \chi_1\chi_2 : g \mapsto \chi_1(g)\chi_2(g), \end{aligned}$$

is a group.

From now on, the group G will be a **finite abelian** group. In this particular case we have $\hat{G} \cong G$, however the isomorphism is not canonical.

Abelian Quantum Fourier Transform

Let $f : G \to X$, in this general context the *Quantum Fourier Transform* considered is a gate acting in the following way.

$$\mathbf{QFT}\left(\frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle\otimes\big|f(g)\big\rangle\right)=\frac{1}{\sqrt{|G|}}\sum_{\chi\in\hat{G}}|\chi\rangle\otimes\left|\hat{f}(\chi)\right\rangle,$$

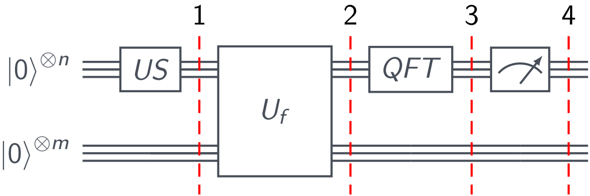
where

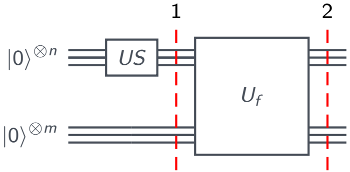
$$\left|\hat{f}(\chi)\right\rangle=\frac{1}{\sqrt{|G|}}\sum_{g\in G}\chi(g)\left|f(g)\right\rangle.$$

Of course, it can be proved that if $G = {}^{\mathbb{Z}}\!/_{2^n\mathbb{Z}}$ then applying $\mathbf{QFT}_n$ to the register $|g\rangle$ gives the same result.

HSP circuit

Given a function f with the assumptions of HSP, this quantum circuit returns a uniformly distributed $\chi \in \widehat{G/H}$, where $\widehat{G/H}$ is viewed as the subset of $\hat{G}$ acting trivial on H.



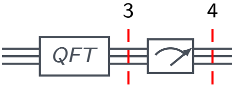


1. The gate **US** sends $|0\rangle^{\otimes n}$ to the uniform superposition

$$|0\rangle^{\otimes n} \longmapsto \frac{1}{\sqrt{|G|}} \sum_{x \in G} |g\rangle .$$

2. The gate $\mathbf{U}_f$ acts as defined before.

$$\frac{1}{\sqrt{|G|}} \sum_{x \in G} |g\rangle \otimes |0\rangle^{\otimes m} \longmapsto \frac{1}{\sqrt{|G|}} \sum_{x \in G} |g\rangle \otimes \left| f(g) \right\rangle$$



3. **QFT** gives

$$\frac{1}{\sqrt{|G|}}\sum_{x\in G}|g\rangle\otimes|f(g)\rangle\mapsto\frac{1}{|G|}\sum_{\chi\in\hat{G}}|\chi\rangle\otimes\Big(\sum_{g\in G}\chi(g)\,|f(g)\rangle\Big)$$

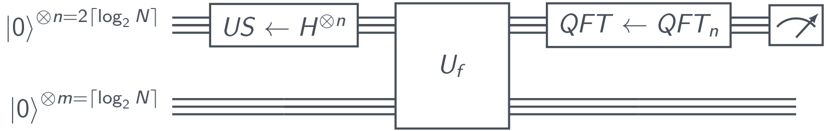
$$=\frac{1}{\left|{}^{G}\!/_{H}\right|}\sum_{\substack{\chi\in\hat{G}\\ \chi_{|H}=1}}|\chi\rangle\otimes\sum_{g\in {}^{G}\!/_{H}}\chi(g)\,|f(g)\rangle$$

4. The outcome of the measure is $\chi\in\widehat{{}^{G}\!/_{H}}$ with probability

$$\left\|\frac{1}{\left|{}^{G}\!/_{H}\right|}\sum_{g\in {}^{G}\!/_{H}}\chi(g)\,|f(g)\rangle\right\|^2=\frac{1}{\left|{}^{G}\!/_{H}\right|}.$$

Shor as HSP

Implementing Shor's algorithm, to find the order r of a modulo N, requires the following setting:



where

$$f : G \to \{0, \dots, N-1\}$$
$$x \longmapsto a^x \mod N,$$

with $G = {}^{\mathbb{Z}}\!/\!_{2^n\mathbb{Z}}$ and $H = \langle r \rangle \leq G$.

Shor as HSP

Observe that, from a theoretical point of view, the previous setting is well defined if the period r divides 2^n. Clearly, this is not always the case and a classical post processing is generally needed to recover r with good probability.

This is the main reason why Shor's algorithm is a probabilistic algorithm.

Shor DLP as HSP

Following the same line as factoring, Shor provides a solution to discrete logarithm problem (DLP) in a cyclic group $C = \langle g \rangle$ of order M. Let $x \in C$, the HSP setting to find $y \in \mathbb{Z}/M\mathbb{Z}$ such that $g^y = x$ is described below.

- The group is
$$G = \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/M\mathbb{Z}$$
- The function is
$$\begin{aligned} f:\ G &\longrightarrow C \\ (a,b) &\longmapsto g^a x^{-b} \end{aligned}$$
- The hidden subgroup is
$$H = \langle y, 1 \rangle \leq G$$

3.2- Quantum Phase Estimation

Quantum Phase Estimation

Problem

Let $\mathbf{U}$ *be a unitary transformation. Given an eigenstate* $|\psi\rangle$ *of* $\mathbf{U}$ *find the phase* $\theta \in [0,1)$ *describing its eigenvalue*

$$\mathbf{U}\,|\psi\rangle = e^{2\pi i\theta}\,|\psi\rangle\,.$$

Preliminary remark

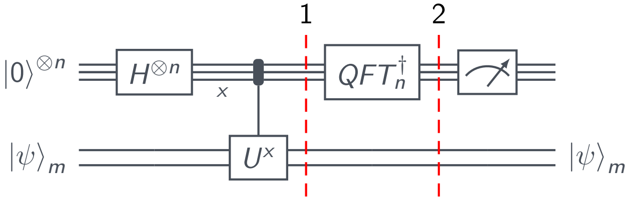
We point out the following main ingredient.

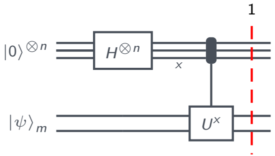
$$\mathbf{C\,U}\,\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |\psi\rangle = \frac{1}{\sqrt{2}}\Big(\,|0\rangle\,|\psi\rangle + e^{2\pi i\theta}\,|1\rangle\,|\psi\rangle\,\Big)$$
$$= \frac{|0\rangle + e^{2\pi i\theta}\,|1\rangle}{\sqrt{2}} \otimes |\psi\rangle$$

In this notation **C U** can be interpreted as a gate acting just on the first qubit since the last part $|\psi\rangle$ is fixed.

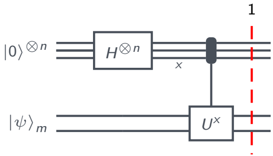
QPE circuit

Given a unitary transformation U acting on $m-$qubits and an its eigenstate $|\psi\rangle_m$, this quantum circuit computes $2^n\theta$ where θ is the phase of the corresponding eigenvalue.

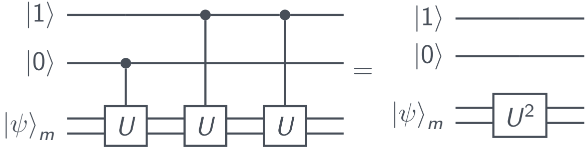




1. The gate in the middle sends $|x\rangle_n |\psi\rangle_m$ to $|x\rangle_n \mathbf{U}^x |\psi\rangle_m$. It is constructed out of 2^j gates $\mathbf{U}$ acting on the register $|\psi\rangle$ controlled by the j-th qubit for all j's.



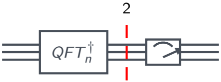
1 The gate in the middle sends $|x\rangle_n |\psi\rangle_m$ to $|x\rangle_n \mathbf{U}^x |\psi\rangle_m$. It is constructed out of 2^j gates $\mathbf{U}$ acting on the register $|\psi\rangle$ controlled by the j-th qubit for all j's. As an example, if $x = n = 2$



Hence, previous remark implies that the state in 1 is

$$\frac{1}{\sqrt{2^n}}(|0\rangle+|1\rangle)^{\otimes n}\otimes|\psi\rangle_m \mapsto \frac{|0\rangle + w_1^{2^n\theta}|1\rangle}{\sqrt{2}}\otimes\cdots\frac{|0\rangle + w_n^{2^n\theta}|1\rangle}{\sqrt{2}}\otimes|\psi\rangle_m .$$

The first register is exactly the Quantum Fourier Transform applied to $|x\rangle_n = |2^n\theta\rangle_n$, see (1).



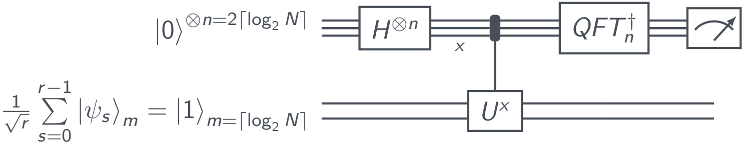
2 Applying the Inverse Quantum Fourier Transform over $\mathbb{Z}/2^n\mathbb{Z}$ to the first register gives

$$\frac{|0\rangle + w_1^{2^n\theta}|1\rangle}{\sqrt{2}} \otimes \cdots \frac{|0\rangle + w_n^{2^n\theta}|1\rangle}{\sqrt{2}} \mapsto |2^n\theta\rangle_n .$$

This works well if $2^n\theta$ is an integer, which is not always true. In the general case, the circuit returns an estimation of θ which allows us to recover it through a continued fraction argument with good probability.

Shor as QPE

Implementing Shor's algorithm, to find the order r of a modulo N, requires the following setting:



where

$$\mathbf{U} : |y\rangle_m \longmapsto |ay \mod N\rangle_m$$

and

$$|\psi_s\rangle_m = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-\frac{2\pi isk}{r}} \left|a^k \mod N\right\rangle_m \text{ s.t. } \mathbf{U}\,|\psi_s\rangle_m = e^{\frac{2\pi is}{r}}\,|\psi_s\rangle_m .$$

Shor as QPE

To avoid any inconvenience in producing $|\psi_s\rangle_m$ for some s, we observe

$$|1\rangle_m = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\psi_s\rangle_m \,.$$

Therefore, using $|1\rangle$ which is a uniform superposition of those eigenstates and reasoning by linearity, the final measure gives

$$\frac{2^n s}{r},$$

for s a random integer between 0 and $r-1$.

4- Breaking RSA

Direct attack to RSA

Given $N = pq$, Alice wants to send a message $b \in {\mathbb{Z}}/{N\mathbb{Z}}^*$ to Bob. Bob's public key is $c \in {\mathbb{Z}}/{(p-1)(q-1)\mathbb{Z}}^*$, then Alice sends him

$$a \equiv b^c \mod pq.$$

Assume Eve can detect the order r of a, $\gcd(r, c) = 1$ implies that r is also the order of b. Moreover, there exists d such that $cd \equiv 1 \mod r$.

$$a^d \equiv b^{cd} \equiv b^{1+mr} \equiv b \mod pq.$$

Factorization of $N = pq$

It can be proved that there's a good probability that the detected period r is even. If so, we have

$$a^r \equiv 1 \mod pq \qquad a^{\frac{r}{2}} \not\equiv 1 \mod pq.$$

Assume also that

$$a^{\frac{r}{2}} \not\equiv -1 \mod pq,$$

since

$$(a^{\frac{r}{2}} - 1)(a^{\frac{r}{2}} + 1) \equiv 0 \mod pq$$

we conclude

$$\{p, q\} = \{\gcd(a^{\frac{r}{2}} - 1, N), \gcd(a^{\frac{r}{2}} + 1, N)\}.$$

Bibliography

- Shor P. W., *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM J. Comp., **26**, 1484-1509, 1997.
- Beauregard S., *Circuit for Shor's algorithm using 2n+3 qubits*, Quantum Information and Computation, Vol. **3**, No. **2**, 175-185, 2003.
- Mermin D., *Quantum Computer Science: An Introduction.*, Cambridge: Cambridge University Press, 2007.
- Nielsen M., Chuang I., *Quantum Computation and Quantum Information: 10th Anniversary Edition.*, Cambridge: Cambridge University Press, 2010.

Q&A

francesco.stocco@telsy.it