Mathematical aspects of Shor's algorithm

Christophe Pittet

MATHEMATICAL ASPECTS OF SHOR'S ALGORITHM

CHRISTOPHE PITTET

ABSTRACT. Given a large n-bits integer $N < 2^n$, Shor's algorithm finds with positive probability a factor of N after

$$O(n^2 \log n \log\log n)$$

quantum steps. We describe some of the mathematical aspects of Shor's algorithm. We mainly follow a description due to M. Batty, S.L. Braunstein, A. J. Duncan and S. Rees.

1. INTRODUCTION

There exist (determistic) algorithms, based on the Agrawal-Kayal-Saxena primality test, which *decide* wether a large n-bits integer N is prime or not in $O(n^6)$ classical steps (see [5] and [3]). But the best known algorithms (including probabilistic ones) which *deliver* a factor of N, all require a superpolynomial number of classical steps in n. For example, the Schnorr-Seysen-Lenstra probabilistic algorithm factorizes $N < 2^n$ in

$$\exp(O((n \log n)^{\frac{1}{2}}))$$

classical steps [4]. In constrast, Shor's algorithm [7] delivers (with positive probability) a factor of $N < 2^n$ in $O(n^2 \log n \log\log n)$ quantum steps.

Implementing efficiently a quantum algorithm on a quantum computer is a major goal in today's science and technology. It involves stability issues in quantum technology. But the mathematical aspects of Shor's algorithm are elementary: the algorithm relies on the structure of cyclic groups, on Fourier transform on cyclic groups, on orthogonal projections in finite dimensional Hilbert spaces, on continued fraction, on properties of the Euler function, and on the Euclidean algorithm.

Date: February 26, 2014.

2010 *Mathematics Subject Classification.* Primary: 68Q12, 20K01; Secondary: 11A41,

Key words and phrases. Shor's algorithm, quantum factorization prime numbers, quantum algorithms, fast Fourier transform.

Ch. Pittet is partially supported by the CNRS.

The goal of this note is to explain how those tools beautifully combine in Shor's algorithm. We mainly follow [2] where the interested reader will find more details. It is obvious from our exposition that $O(n^4)$ bounds the complexity of the algorithm. Shor's tight bound $O(n^2 \log n \log\log n))$ is more technical and we do not attempt to explain it.

2. Reducing the factorization problem to a period finding problem

2.1. **The Euclidean algorithm is efficient.** Let $a, b \in \mathbb{N}$, $b \neq 0$, $a \geq b$. It is convenient to define $r_{-1} = a$ and $r_0 = b$. For $i \geq 0$, the Euclidian division

$$r_{i-1} = q_{i+1} r_i + r_{i+1},$$

with $q_{i+1} \in \mathbb{N}$ and $0 \leq r_{i+1} < r_i$, defines the Euclidean algorithm: the smallest $n \in \mathbb{N}$ with $r_n = 0$ is such that the greatest common divisor of a and b is

$$GCD(a, b) = r_{n-1}.$$

It also defines the continuous fraction

$$\frac{a}{b} = q_1 + \frac{1}{q_2 + \frac{1}{\cdots + \frac{1}{q_n}}}.$$

Any truncation of it is called a convergent of the continuous fraction. It is easy to check that $r_{i+2} < r_i$ hence the algorithm finds $GDC(a, b)$ after $O(\log a)$ divisions.

2.2. **The first steps in Shor's algorithm are classical and they involve the structure of the unit group $(\mathbb{Z}/N\mathbb{Z})^*$.** We are given a large integer $N < 2^n$ and the goal is to find a factor of N. We choose an integer

$$1 < y < N$$

at random. We compute $GCD(y, N)$ (on a classical computer) with the Euclidean algorithm. As explained above it requires at most $O(n)$ divisions. If it turns out that $GCD(y, N) \neq 1$ then we have found a factor of N and the algorithm stops. In the case $GCD(y, N) = 1$, that is if y has an inverse modulo N, then we consider y as an element of the multiplicative group of units $(\mathbb{Z}/N\mathbb{Z})^*$ of the ring $\mathbb{Z}/N\mathbb{Z}$. Let r be the order of y in $(\mathbb{Z}/N\mathbb{Z})^*$.

Assume we are lucky in the sense that r is even. We have:

$$(y^{r/2} - 1)(y^{r/2} + 1) = y^r - 1 = 0[N].$$

That is N divides $(y^{r/2}-1)(y^{r/2}+1)$. So at least one of the prime factors of N must divide $y^{r/2}+1$ (otherwise N would divide $y^{r/2}-1$ and this would contradict the definition of r). This implies

$$1 < GCD(y^{r/2}+1, N).$$

Assume we are super lucky in the sense that r is even and

$$y^{r/2}+1 \neq 0[N]$$

(see the proposition below for a lower bound on the probabiliy of being super lucky in the above sense). In this case,

$$1 < GCD(y^{r/2}+1, N) < N$$

is a non trivial factor of N and we can efficiently compute it with the Euclidian algorithm, provided we know r.

If E is a finite set, let $|E|$ denotes its cardinal.

Proposition 2.1. *(A lower bound on the probability of picking y with good properties.) Assume N is odd. Let m be the number of distinct prime factors of N. The set*

$$\{y \in (\mathbb{Z}/N\mathbb{Z})^* : \textit{the order } r \textit{ of } y \textit{ is even and } y^{r/2}+1 \neq 0[N]\}$$

contains at least

$$\varphi(N)\left(1-\frac{1}{2^{m-1}}\right)$$

elements, where $\varphi(N) = |\,(\mathbb{Z}/N\mathbb{Z})^*\,|$ is the Euler function.

(The proof is based on the fact that if p is an odd prime and $m \in \mathbb{N}$ then $(\mathbb{Z}/p^m\mathbb{Z})^*$ is cyclic.)

As it is obvious to find a factor in the case N is even and as it is easy to find a factor if N is a power of a single prime (compute the d-root of N for $d \leq \log N/\log 3$ and check if it is a factor of N), we may apply the above proposition, with $m \geq 2$. In this case, we see that we are super lucky in the above sense more than half of the time. So if we have a device which efficiently compute the order r of y, then the strategy is straightforward: first we efficiently compute a candidate for a factor of N as explained above. Then we check if the candidate is indeed a factor. If not, we pick another y and try again. The chance we don't get a factor after 10 tries for example, is less than $\frac{1}{2^{10}} = \frac{1}{1024}$.

3. Mathematical concepts for classical/quantum computations

3.1. **Classical bits versus quantum bits.** A (classical) *bit* is the field $\mathbb{Z}/2\mathbb{Z}$ with two elements. It has two *states* **0** and **1**.

A *quantum bit*, (a *q-bit*), is the group algebra over the field of complex numbers of the group with two elements:

$$\mathbb{C}[\mathbb{Z}/2\mathbb{Z}] \cong \mathbb{C}^2 \cong \{\alpha\mathbf{0} + \beta\mathbf{1} : \alpha, \beta \in \mathbb{C}\}.$$

It has two *fundamental states* $\mathbf{0}$ and $\mathbf{1}$. A *state* of a q-bit is a unit vector in $\mathbb{C}^2$ for the standard hermitian product on $\mathbb{C}^2$ which makes $\mathbf{0}$ and $\mathbf{1}$ an orthonormal basis. Hence any state v of the q-bit $\mathbb{C}[\mathbb{Z}/2\mathbb{Z}]$ is a complex superposition

$$v = \alpha\mathbf{0} + \beta\mathbf{1}$$

of the fundamental states with the condition

$$|\alpha|^2 + |\beta|^2 = 1.$$

We will view $\mathbb{C}[\mathbb{Z}/2\mathbb{Z}]$ as a Hilbert space with two distinguished elements $\mathbf{0}$ and $\mathbf{1}$.

3.2. **Classical memory versus quantum memory.** An *n-bit register (or memory)* is the $\mathbb{Z}/2\mathbb{Z}$-vector space $(\mathbb{Z}/2\mathbb{Z})^n$. It has dimension n over $\mathbb{Z}/2\mathbb{Z}$. A *state* of it is any of its 2^n elements.

An *n-q-bit register (or memory)* V_n is the Hilbert tensor product of n copies of the q-bit $\mathbb{C}[\mathbb{Z}/2\mathbb{Z}]$:

$$V_n = \mathbb{C}[\mathbb{Z}/2\mathbb{Z}]^{\otimes n} \cong \left(\mathbb{C}^2\right)^{\otimes n}.$$

The Hilbert product of two pure tensors is

$$(v_1 \otimes \cdots \otimes v_n, w_1 \otimes \cdots \otimes w_n) = \prod_{i=1}^{n} (v_i, w_i).$$

Hence if we denote

$$e_0 = \mathbf{0},\ e_1 = \mathbf{1},$$

then the 2^n *fundamental states*

$$\{e_{i_1} \otimes \cdots \otimes e_{i_n}\}_{(i_1,\ldots,i_n)\in(\mathbb{Z}/2\mathbb{Z})^n},$$

form an orthonormal basis of V_n. A *state* of V_n is any of its unit vector. Hence any state v is a complex superposition

$$v = \sum_{I\in(\mathbb{Z}/2\mathbb{Z})^n} \alpha_I e_I$$

of the fundamental states with the condition

$$\sum_{I\in(\mathbb{Z}/2\mathbb{Z})^n} |\alpha_I|^2 = 1.$$

We may view a quantum n-register as an enhancement of a classical n-register: not only it contains the 2^n fundamental states but it

contains also any of their complex superposition (of unit norm). This makes possible to consider the *homogeneous state*

$$\frac{1}{2^n}\sum_{I\in(\mathbb{Z}/2\mathbb{Z})^n} e_I$$

of the quantum register V_n which entangles all fundamental states in a single quantum state. This entanglement of information is a common feature in quantum algorithms and as we will see, it is the first step in the period finding part of Shor's algorithm.

We will use the following identifications:

$$\mathbb{C}[\mathbb{Z}/2\mathbb{Z}]^{\otimes n} \to \mathbb{C}[(\mathbb{Z}/2\mathbb{Z})^n] \to \mathbb{C}[\mathbb{Z}/2^n\mathbb{Z}],$$

$$e_{i_1}\otimes\cdots\otimes e_{i_n} \mapsto (i_1,\ldots,i_n) \mapsto \sum_{k=1}^{n} i_k 2^{k-1}.$$

The two maps are isomorphisms of Hilbert spaces: each of the above three families of elements, on which we have specified the maps, forms an orthonormal basis with respect to the chosen Hermitian product on the complex vector space it belongs to. In any of the three models of V_n, we will refer to the above orthonormal basis as the set of fundamental states.

3.3. **Classical computation versus quantum computation.** A *computation* is a map

$$f : (\mathbb{Z}/2\mathbb{Z})^m \to (\mathbb{Z}/2\mathbb{Z})^n$$

from the m-register to the n-register. A *quantum computation* is a unitary transformation

$$U : V_n \to V_n$$

from the quantum n-register V_n to itself.

Notice that a classical computation may not be reversible (for example if $m > n$), whereas a quantum computation always is, by definition of a unitary transformation. Nevertheless any (classical) computation can be handled with a quantum computation. Indeed, if f is as above, we define

$$U_f : V_m \otimes V_n \to V_m \otimes V_n,$$

$$x\otimes y \mapsto x\otimes(f(x)+y).$$

Some caution about notation is in order here. The element x varies among the 2^m fundamental states of V_m and y varies among the 2^n

fundamental states of V_n. Hence $x \otimes y$ varies among the 2^{n+m} fundamental states of $V_{m+n} = V_m \otimes V_n$ which form an orthonormal basis. The right hand side of the tensor

$$x \otimes (f(x) + y) \in V_m \otimes V_n$$

is best described in the model

$$V_n = \mathbb{C}[(\mathbb{Z}/2\mathbb{Z})^n]$$

where the sum $f(x) + y$ makes sense (because $f(x) \in (\mathbb{Z}/2\mathbb{Z})^n$ and we may see $y \in \mathbb{C}[(\mathbb{Z}/2\mathbb{Z})^n]$) and is by definition a fundamental state.

Obviously $f(x) + f(x) = 0$ in $(\mathbb{Z}/2\mathbb{Z})^n$. Hence U_f is a well defined unitary involution. We can recover f from U_f by choosing $y = \mathbf{0} \otimes \cdots \otimes \mathbf{0}$ and projecting

$$U_f(x \otimes \mathbf{0} \otimes \cdots \otimes \mathbf{0}) = x \otimes f(x),$$

to the second register.

The *Walsh-Hadamard* transform

$$W_1 : V_1 \to V_1$$

is defined as the unitary transformation of the q-bit $V_1 = \mathbb{C}[\mathbb{Z}/2\mathbb{Z}]$ into itself whose matrix in the basis of the fundamental states $\mathbf{0}, \mathbf{1}$ is

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

(It is the complexification of the orthogonal reflexion in the real plane generated by $\mathbf{0}$ and $\mathbf{1}$ whose axis forms an angle with $\mathbb{R}\mathbf{0}$ of measure $\pi/8$.) The *Walsh-Hadamard* transform

$$W_n : V_n \to V_n$$

is defined as

$$W_n = W_1 \otimes \cdots W_1.$$

It is obviously a unitary transformation because W_1 is a unitary transformation. For example, if we allow ourself to denote also by W_1 the matrix of the unitary transformation W_1 in the orthonormal basis of the fundamental states, then the matrix of W_2 in the orthonormal basis of the fundamental states is

$$\frac{1}{\sqrt{2}} \begin{pmatrix} W_1 & W_1 \\ W_1 & -W_1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

It is easy to check that

$$W_n(\mathbf{0}\otimes\cdots\otimes\mathbf{0}) = \frac{1}{2^{n/2}}\sum_{I\in(\mathbb{Z}/2\mathbb{Z})^n} e_I$$

is the homogeneous state.

3.4. **Measurements on a quantum register.** Let V be a finite dimensional Hilbert space over $\mathbb{C}$. A *measurement* on V is a finite collection of orthogonal projections

$$P_1,\ldots,P_k : V\to V,$$

(hence $P_i^2 = P_i$ and $P_i^* = P_i$) such that

(1) $P_iP_j = 0$ if $i\neq j$,
(2) $id_V = \sum_{i=1}^k P_i$.

If V is a quantum register in a state $v\in V$, $\|v\| = 1$, and if the measurement

$$(P_1,\cdots,P_k)$$

is applied, the result of the measurement is the integer

$$1\leq i\leq k$$

with probability

$$\mathcal{P}(i) = \|P_i(v)\|^2.$$

Notice that according to Pythagoras

$$\sum_{i=1}^k \mathcal{P}(i) = \sum_{i=1}^k \|P_i(v)\|^2 = \|\sum_{i=1}^k P_i(v)\|^2 = \|v\|^2 = 1.$$

If the measurement $(P_1,\cdots,P_k)$ is applied to a register V in the state $v\in V$ and if the integer i is observed, then the register after measurement is in the state

$$\frac{P_i(v)}{\|P_i(v)\|}.$$

(Notice that if i is observed then $P_i(v)\neq 0$ because obviously $\mathcal{P}(i)\neq 0$.)

4. The Fourier transform on finite cyclic groups

Let n be an integer. Let $\mathbb{C}[\mathbb{Z}/n\mathbb{Z}]$ be the complex group algebra of the cyclic group $\mathbb{Z}/n\mathbb{Z}$ and let $L^2(\mathbb{Z}/n\mathbb{Z})$ be the Hilbert space of complex valued functions on $\mathbb{Z}/n\mathbb{Z}$. We perform the natural identification

$$\mathbb{C}[\mathbb{Z}/n\mathbb{Z}]\to L^2(\mathbb{Z}/n\mathbb{Z}),$$
$$\sum_{x\in\mathbb{Z}/n\mathbb{Z}} a_x x \mapsto \sum_{x\in\mathbb{Z}/n\mathbb{Z}} a_x\delta_x,$$

where $a_x \in \mathbb{C}$ and $\delta_x(y) = 0$ if $x \neq y$ and $\delta_x(x) = 1$. The basis $\{\delta_x\}_{x\in\mathbb{Z}/n\mathbb{Z}}$ is an orthonormal basis of $L^2(\mathbb{Z}/n\mathbb{Z})$ for the scalar product

$$(\phi, \psi) = \sum_{x\in\mathbb{Z}/n\mathbb{Z}} \phi(x)\overline{\psi(x)}.$$

It is easy to check that the characters

$$\chi^c : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*$$
$$x \mapsto \exp(2i\pi cx/n),$$

when normalized as

$$\left\{\frac{\chi^c}{\sqrt{n}}\right\}_{c\in\mathbb{Z}/n\mathbb{Z}}$$

also form an orthonormal basis of $L^2(\mathbb{Z}/n\mathbb{Z})$. We define the Fourier transform $\mathcal{F}$ as the unique unitary transformation which extends

$$L^2(\mathbb{Z}/n\mathbb{Z}) \to L^2(\mathbb{Z}/n\mathbb{Z})$$
$$\frac{\chi^c}{\sqrt{n}} \mapsto \delta_c.$$

That is

$$\mathcal{F}\left(\sum_{x\in\mathbb{Z}/n\mathbb{Z}} f(x)\delta_x\right) = \sum_{c\in\mathbb{Z}/n\mathbb{Z}} \hat{f}(c)\delta_c,$$

where

$$\hat{f}(c) = (f, \frac{\chi^c}{\sqrt{n}}).$$

Although the following proposition is not needed in building Shor's algorithm (a more elaborated version of it is needed; see Proposition 8.1 below), it is helpful to have it in mind.

Proposition 4.1. *Assume r is a factor of n. Let*

$$f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$$

be a function of period r. Then

$$\hat{f}(c) = 0$$

excepted if

$$c \in \{0; \frac{n}{r}; \cdots; (r-1)\frac{n}{r}\}$$

Proof. The subspace of periodic functions of period r has dimension r. It is generated by

$$\chi^{n/r}, \ldots, \chi^{(r-1)n/r}, \chi^n = 1_{\mathbb{Z}/n\mathbb{Z}}.$$

□

5. Construction of the double quantum register in Shor's algorithm

As explained in the first section, the factorization problem is reduced to a finding period problem. We explain how a double quantum register encodes the relevant periodic function. Let N be the large integer we want a factor of. Let n be the unique integer such that

$$2^{n-1} < N^2 \leq 2^n.$$

Let

$$L = \lceil \log_2 N \rceil.$$

Let $1 < y < N$ such that $GCD(y, N) = 1$. Let

$$f : \mathbb{Z}/2^n\mathbb{Z} \to \mathbb{Z}/2^L\mathbb{Z}$$

$$x \mapsto y^x \mathrm{mod}[N].$$

In the definition of f it is understood that

$$y^x \in \{0; 1; \ldots; N-1\} \subset \mathbb{Z}/2^L\mathbb{Z}.$$

(Notice that there is no reason for the order r of y in $(\mathbb{Z}/N\mathbb{Z})^*$ to divide 2^n, hence strictly speaking, the function f is not necessary periodic. But as we will see, f captures enough of the periodicity of

$$\mathbb{Z} \to (\mathbb{Z}/N\mathbb{Z})^*$$

$$x \mapsto y^x$$

so that the order r of y can be extracted from it.)

Let $V_n \otimes V_L$ be a double quantum register. Let it be in the state

$$(\mathbf{0} \otimes \cdots \otimes \mathbf{0}) \otimes (\mathbf{0} \otimes \cdots \otimes \mathbf{0}) \in V_n \otimes V_L.$$

We have:

$$\begin{aligned} & U_f(W_n \otimes id_{V_L})(\mathbf{0} \otimes \cdots \otimes \mathbf{0}) \otimes (\mathbf{0} \otimes \cdots \otimes \mathbf{0}) \\ &= U_f \left(\frac{1}{2^{n/2}} \sum_{x \in \mathbb{Z}/2^n\mathbb{Z}} x \otimes (\mathbf{0} \otimes \cdots \otimes \mathbf{0}) \right) \\ &= \frac{1}{2^{n/2}} \sum_{x \in \mathbb{Z}/2^n\mathbb{Z}} U_f(x \otimes (\mathbf{0} \otimes \cdots \otimes \mathbf{0})) \\ &= \frac{1}{2^{n/2}} \sum_{x \in \mathbb{Z}/2^n\mathbb{Z}} x \otimes f(x). \end{aligned}$$

The unitary operator U_f can be theoretically implemented on a quantum computer as the composition of $O(n^3 \log n \log\log n)$ elementary quantum gates because the classical modular exponentiation $y^x \mathrm{mod}[N]$,

with $N \leq 2^n$, needs less than $O(n^3 \log n \log\log n)$ classical gates: exponentiation by squaring needs $O(n^2)$ multiplications between n-bits numbers, and multiplication of two n-bits number needs less than $O(n \log n \log\log n)$ classical gates. On the other hand W_n needs $O(n)$ elementary quantum gates.

At this point, it may seem that the goal is reached: it is possible to entangle all the values of the function $f(x) = y^x \mathrm{mod}[N]$ in a single state of a quantum register which is the tensor product of $O(\log N)$ quantum bits, using $O(n^2 \log n \log\log n)$ elementary quantum gates, where $N < N^2 \leq 2^n$. In fact there are two obstacles left. First, as mentioned above, the function f is not really periodic. A well-known rigidity feature from number theory handles this issue (see Proposition 9.1 below). The second obstacle is the measurement problem: extracting information from a quantum register perturbs its state. So it is not obvious to extract a period from it. This problem is solved by first measuring the second register V_L, then applying a Fourier transform, then measuring the first register V_n. We explain these points in what follows.

6. Measurement on the second register

Let $L = \lceil \log_2 N \rceil$, as in the previous section. Let

$$V_L = \mathbb{C}[\mathbb{Z}/2^L\mathbb{Z}].$$

Let $b \in \mathbb{Z}/2^L\mathbb{Z} \subset C[\mathbb{Z}/2^L\mathbb{Z}]$ be a fundamental state. Let

$$P_b : V_L \to V_L$$

be the orthogonal projection onto the complex line $\mathbb{C}b$. The family of projectors

$$\{id_{V_n} \otimes P_b\}_{b \in \mathbb{Z}/2^L\mathbb{Z}}$$

obviously forms a measurement on $V_n \otimes V_L$. If this measurement is applied to the state

$$\frac{1}{2^{n/2}} \sum_{x \in \mathbb{Z}/2^n\mathbb{Z}} x \otimes f(x),$$

then $b \in \mathbb{Z}/2^L\mathbb{Z}$ is observed with probability

$$\begin{aligned}
&\|(id_{V_n} \otimes P_b)\left(\frac{1}{2^{n/2}} \sum_{x \in \mathbb{Z}/2^n\mathbb{Z}} x \otimes f(x)\right)\|^2 \\
&= \|\frac{1}{2^{n/2}} \sum_{x \in f^{-1}(b)} x \otimes b\|^2 \\
&= \frac{|f^{-1}(b)|}{2^n}.
\end{aligned}$$

Notice that if b is observed, then after measurement the double register is in the state

$$\left(\frac{1}{\sqrt{|f^{-1}(b)|}} \sum_{x \in f^{-1}(b)} x\right) \otimes b.$$

Notice also that if b is observed then the above formula for the probability of observing b implies that $f^{-1}(b)$ is nonempty. Let us denote

$$\psi_b : \mathbb{Z}/2^n\mathbb{Z} \to \mathbb{C},$$

the normalized characteristic function of the set $f^{-1}(b)$:

$$\psi_b = \frac{1_{f^{-1}(b)}}{\sqrt{|f^{-1}(b)|}}.$$

With this notation, the state of the double register can be written as

$$\left(\sum_{x \in \mathbb{Z}/2^n\mathbb{Z}} \psi_b(x)x\right) \otimes b.$$

7. Applying the Fourier transform

As explained above the Fourier transform $\mathcal{F}$ on the group $\mathbb{Z}/2^n\mathbb{Z}$ is a unitary transformation of $V_n = \mathbb{C}[\mathbb{Z}/2^n\mathbb{Z}]$. We have

$$\begin{aligned}
&(\mathcal{F} \otimes id_V)\left(\sum_{x \in \mathbb{Z}/2^n\mathbb{Z}} \psi_b(x)x\right) \otimes b \\
&= \left(\sum_{c \in \mathbb{Z}/2^n\mathbb{Z}} \hat{\psi_b}(c)c\right) \otimes b.
\end{aligned}$$

It can be performed by running $O(n^2)$ elementary quantum gates.

8. Measurement on the first register

Let $c \in \mathbb{Z}/2^n\mathbb{Z}$. Let

$$P_c : V_n \to V_n$$

be the orthogonal projection onto the complex line $\mathbb{C}c$. The family of projectors

$$\{P_c \otimes id_{V_L}\}_{c\in\mathbb{Z}/2^n\mathbb{Z}}$$

obviously forms a measurement on $V_n \otimes V_L$. If this measurement is applied to the state

$$\left(\sum_{c\in\mathbb{Z}/2^n\mathbb{Z}} \hat{\psi}_b(c)c\right) \otimes b,$$

then $c \in \mathbb{Z}/2^n\mathbb{Z}$ is observed with probability

$$\|\hat{\psi}_b(c)c \otimes b\|^2 = |\hat{\psi}_b(c)|^2.$$

Recall that the order r of $y \in (\mathbb{Z}/N\mathbb{Z})^*$ satisfies $r^2 < N^2 \leq 2^n$.

Proposition 8.1. *The probability of observing $0 \leq c < 2^n$ with the property that there exists an integer s such that $0 \leq s < r$ with $GCD(s, r) = 1$ and*

$$\left|\frac{c}{2^n} - \frac{s}{r}\right| < \frac{1}{2r^2},$$

is greater or equal to

$$\frac{4}{\pi^2}\frac{\varphi(r)}{r}\left(1 - \frac{1}{N}\right),$$

where φ denotes the Euler function.

Notice that the inequality in the above proposition can be rewritten as

$$\left|c - s\frac{2^n}{r}\right| < \frac{1}{2}\frac{2^n}{r^2}.$$

As $r^2 < 2^n$, the above inequality imposes a weaker constrain on c than the inequality

$$\left|c - s\frac{2^n}{r}\right| \leq \frac{1}{2}.$$

But in the special case of periodic functions we have seen that there exists an integer s such that the left hand side of the above inequality vanishes. Hence, it is expected that the almost periodic distribution of the set $f^{-1}(b)$ implies the existence of an s satisfying the above inequality. Technically, notice that there exists $0 \leq a < r$, where r is the order of y in $(\mathbb{Z}/N\mathbb{Z}))^*$, such that

$$f^{-1}(b) = \{a + kr : k = 0, \ldots, K_a - 1\}$$

where K_a is the largest integer such that $a + (K_a - 1)r < 2^n$. Hence by definition $|f^{-1}(b)| = K_a$ and the probability of observing c is

$$\begin{aligned}|\hat{\psi}_b(c)|^2 &= |(\psi_b, \frac{\chi^c}{2^{n/2}})|^2 \\ &= \frac{1}{K_a 2^n} \left| \sum_{k=0}^{K_a-1} \exp\left(-\frac{2i\pi c(a+kr)}{2^n}\right)\right|^2 .\end{aligned}$$

The above formula enables one to prove the proposition.

9. End of the algorithm: recovering the period through the convergents of a continuous fraction

The final step of Shor's algorithm is based on the following well-known number theoretical property of continued fractions.

Proposition 9.1. *Let $x \in \mathbb{Q}$. Let $s, r \neq 0$ be two integers. Assume*

$$\left|x - \frac{s}{r}\right| < \frac{1}{2r^2}.$$

Then s/r is a convergent of x.

The quantum computer provides us with the integer c. According to Proposition 8.1, with positive probability, the integer c satisfies

$$\left|\frac{c}{2^n} - \frac{s}{r}\right| < \frac{1}{2r^2},$$

for some integer s such that $0 \leq s < r$ and $GCD(s, r) = 1$. So with positive probability, Proposition 9.1 applies with $x = \frac{c}{2^n}$, $r = \text{order}(y)$ in $(\mathbb{Z}/N\mathbb{Z})^*$, and some s such that $0 \leq s < r$ and $GCD(s, r) = 1$. Therefore with positive probability, the order r is a denominator of the reduced form of one of the convergents of $\frac{c}{2^n}$. The Euclidean algorithm computes efficiently the convergents in reduced form of $\frac{c}{2^n}$. So it is possible to efficiently list their denominators.

10. A lower bound on the Euler function

The efficiency of the algorithm depends on the lower bound

$$\frac{4}{\pi^2}\frac{\varphi(r)}{r}\left(1 - \frac{1}{N}\right)$$

from Proposition 8.1. When N goes to infinity the period r, which is by definition the order of a random element in $(\mathbb{Z}/N\mathbb{Z})^*$, may also go to infinity. The bad new is that for infinitely many integers m,

$$\frac{\varphi(m)}{m} < \frac{1}{\exp(\gamma)\log\log m},$$

where $\gamma = 0,57\ldots$ denotes Euler's constant (see for example [1, Theorem 13.14 (b)]). The good new is that the quotient admits a lower bound which goes to zero extremely slowly: for $m > 2$,

$$\frac{\varphi(m)}{m} > \frac{1}{\exp(\gamma)\ \log\log m + \frac{2.50637}{\log\log m}},$$

(see [6]).

11. Acknowledgments

We are indebted to Andrew Duncan for giving us a preprint version of [2] when quantum algorithms were still considered as science fiction. Most of the note is based on it and most of the proofs can be found in it. We have been supported by the CNRS and the Poncelet Laboratory in Moscow when giving a course on Shor's algorithm at the Independent University of Moscow. We are very grateful to Tatiana Smirnova Nagnibeda and Stanislav Smirnov who invited us to give a talk at the Chebyshev Laboratory in St-Petersburg (May 18, 2011). The video of the talk is available on the net under the name: Shor's algorithm. A link is: http://www.lektorium.tv/lecture/?id=13296. The present note is an isomorphic written version of the video and of talks we gave at the CIMPA-UNESCO School on Fourier Analysis on groups and combinatorics, November 18-30, 2013, Shillong (India). We are very grateful to the organizers Gautami Bhowmik and Himadri Mukherjee for inviting us to their School.

References

[1] Tom M. Apostol, *Introduction to analytic number theory*, Springer-Verlag, New York, 1976. Undergraduate Texts in Mathematics. MR0434929 (55 #7892)

[2] Michael Batty, Samuel L. Braunstein, Andrew J. Duncan, and Sarah Rees, *Quantum algorithms in group theory*, Computational and experimental group theory, Contemp. Math., vol. 349, Amer. Math. Soc., Providence, RI, 2004, pp. 1–62, DOI 10.1090/conm/349/06356.

[3] H. W. Lenstra Jr. and Carl Pomerance, *Primality Testing with Gaussian Periods*, In proceeding of: FST TCS 2002: Foundations of Software Technology and Theoretical Computer Science, 22nd Conference Kanpur, India, December 12-14, posted on 2002, DOI 10.1007/3-540-36206-1-1.

[4] ———, *A rigorous time bound for factoring integers*, J. Amer. Math. Soc. **5** (1992), no. 3, 483–516, DOI 10.2307/2152702. MR1137100 (92m:11145)

[5] Carl Pomerance, *Primality testing: variations on a theme of Lucas*, Congr. Numer. **201** (2010), 301–312. MR2598366 (2010k:11191)

[6] J. Barkley Rosser and Lowell Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94. MR0137689 (25 #1139)

[7] Peter Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM J.Sci.Statist.Comput. **26** (1997).

I2M, Aix-Marseille Université
E-mail address: pittet@math.cnrs.fr