Montangero's lectures

Notes taken by Jacopo Tissino

June 2019

1 Shor's algorithm

We want to factor a product of large numbers.

Bob and Alice want to communicate, Bob generates a public key K_{Pu} and a private key K_{Pr}, he sends K_{Pu} to Alice, who encodes the message C, sends it to Bob, who uses K_{Pr} to decode it.

Given a message P, we encode it as

$$C = E_{K_{\mathrm{Pu}}}(P) = P^e \mod n \tag{1}$$

where n is chosen such that $n = pq$, with $p, q \in \mathbb{Z}_{\mathrm{prime}}$, $\Phi = (p-1)(q-1)$, $1 < e < \Phi$ and Φ, e are coprime.

d is chosen such that $de = 1 \mod \Phi$. The message is decoded as

$$D_{K_{\mathrm{Pr}}} C^d \mod P(d, n) \tag{2}$$

Factoring n is equivalent to finding the period of a function: the *order* r is the number such that $x^r = 1 \mod N$, $f(r) = x^r \mod N$.

If r is even, then $y = x^{r/2}$, so $y^2 = 1 \mod N$ therefore $(y+1)(y-1) = 0 \mod N$.

(The new variable N is actually n, to fix later).

Therefore $(y+1)(y-1) = kN$ for some $k \in \mathbb{N}$, so we have found the factors.

The algorithm Given $N = pq$, we have the following steps:

1. Choose $x < N$. If it divides N, we are done;
2. Find the order r such that $f(r) = x^r \mod N$;
3. If r is even, we have the factors. If it is not, start over.

The quantum step is in step 2.

Step 1

Hypotheses These are not actually needed but they make treating the problem much simpler. $N = 2^n$, $N/r = m \in \mathbb{N}$.

we encode the function like

$$U : |x\rangle |0\rangle \longmapsto |x\rangle \left|f(x)\right\rangle \tag{3}$$

We start from $|0\rangle^n$, apply many Hadamards and get $|x\rangle$ = superposition of all possible states, and with this we prepare

$$\left|\psi\right\rangle = \frac{1}{\sqrt{2^n}} \sum |x\rangle \left|f(x)\right\rangle \tag{4}$$

Step 2 We measure the second registry, and obtain $\left|\overline{f}\right\rangle$. Then the first registry must contain all the combinations which generate that state: so:

$$\begin{aligned}\left|\psi_2\right\rangle &= \frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} \left|x_0 + jr\right\rangle \left|\overline{f(x_0)}\right\rangle & (5)\\ &= \left[\frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} \left|x_0 + jr\right\rangle\right] \otimes \left|\overline{f(x_0)}\right\rangle & (6)\end{aligned}$$

Step 3 We want to find r, so we can do a quantum Fourier transform. It can be slow for generic functions but in our case the transform is applied to a function which is actually periodic

$$\left|\psi_3\right\rangle = \mathrm{QFT}\left\{\left|\psi_2\right\rangle\right\} = \frac{1}{\sqrt{mN}} \sum_{y=0}^{N-1} \sum_{j=0}^{m-1} \exp\bigl(2\pi i (x_0 + jr) y/N\bigr) \left|y\right\rangle \tag{7}$$

Step 4

$$\begin{aligned}P(\overline{y}) &= \frac{1}{Nm} \left| \sum_{j=0}^{m-1} \exp\bigl(2\pi i (x_0 + jr)\overline{y}/N\bigr) \right| & (8)\\ &= \frac{1}{r} \left| \frac{1}{m} \sum_j \exp\bigl(2\pi i j \overline{y}/m\bigr) \right| & (9)\end{aligned}$$

Claim: the states with nonzero probability to be found are those with $\overline{y} = km$, where $k \in 0, \dots, r$.

Example $P(\overline{y}=0) = 1/r\left|1/m\sum_j 1\right| = 1/r$. Our function is periodic with period

So all the states we get are in the form $\overline{y} = km = kN/r$. We know N, we measured $\overline{y}$, so:

- if $k=0$, we failed;
- if $k \neq 0$, we set $\overline{y}/N = \overline{k}/r$ and find the solution in polynomial time.

$P(\text{success}) \sim 1$ dopo $O(\log(\log(r)))$.

Detto $n = \log N$, Shor scala come $O(n^2 \log n \log\log n)$, l'algoritmo classico scala come $\exp\left(O(\sqrt[3]{n \log n})\right)$.

Example

$$f(x) = \frac{1}{2}(\cos \pi x + 1) \tag{10}$$

$$f : \left| \begin{array}{ccc} \{0,1\}^3 & \longrightarrow & \{0,1\} \\ 0,2,4,6 & \longmapsto & 1 \\ 1,3,5,7 & \longmapsto & 0 \end{array} \right.$$

So $N = 2^3 = 8$. $r = 2$, $m = N/r = 4$.

Step 1

$$|\psi_1\rangle = \frac{1}{\sqrt{8}} \sum_{m=0}^{7} |x\rangle_1 |f(x)\rangle_2 \tag{11}$$

Step 2

$$|\psi_2\rangle = \frac{1}{2}(|1\rangle + |3\rangle + |5\rangle + |7\rangle)_1 \otimes |0\rangle_2 \tag{12}$$

Step 3 We map $j \to \frac{1}{\sqrt{8}} \sum_k \exp(2\pi ijk/8) |k\rangle$

$$|\psi_3\rangle = \frac{1}{2\sqrt{8}}(|0\rangle + e^{i\pi/4}|1\rangle \tag{13}$$

$$+ \cdots + |0\rangle + e^{3i\pi/4}|1\rangle)_1 \otimes |0\rangle_2 \tag{14}$$

$$= \frac{1}{\sqrt{2}}(|0\rangle + |4\rangle) \tag{15}$$

We either measure 0 or 4. So, if it is 0 we have failed, if it is 4 we have $\overline{y} = 4$, therefore $k = 1$ works and $r = 2$.