Shor's algorithm

Course at IUM Ch. Pittet

Continued fractions

Let $a, b \in \mathbb{N}$, $b \neq 0$ $a \geq b$.

Recall the Euclidean algorithm

$a = r_{-1}$, $b = r_0$

for $i \geq 0$, let $r_{i-1} = q_{i+1} r_i + r_{i+1}$

where $q_{i+1} \in \mathbb{N}$, $0 \leq r_{i+1} < r_i$.

The smallest $n \in \mathbb{N}$ such that

$r_n = 0$ gives $r_{n-1} = GCD(a, b)$.

It gives the continued fraction

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

Notice that $r_{n-2} = q_n \cdot r_{n-1} + 0$

hence $q_n > 1$.

We conclude that any positive rational $\frac{a}{b}$, $a, b \in \mathbb{N}$ $b \neq 0$ has a finite continued fraction

$$\frac{a}{b} = [q_1, q_2, \cdots, q_n] \quad \text{with } q_n > 1$$

(with $q_1 = 0$ if $a < b$).

Any truncation $[q_1, \cdots, q_i]$, $i \leq n$, is called a convergent of $\frac{a}{b}$.

Theorem Let $x \in \mathbb{Q}$. If $\frac{s}{r} \in \mathbb{Q}$ s.t.

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

then $\frac{s}{r}$ is a convergent of the continued fraction of x.

(Hardy Wright Th 184)

Description of the algorithm.

1) $N > 1$ is given (N is a big integer and the goal is to find a factor.) Let n be the unique integer such that $N^2 \leq 2^n < 2N^2$. Let $L := \lceil \log_2 N \rceil$. We identify $\mathbb{Z}/N\mathbb{Z}$ with:

$$\{0; 1; \cdots; N-1\} \longrightarrow \mathbb{Z}/2^L\mathbb{Z}.$$

2) We form the Hilbert tensor product of the n q-bit register and the L q-bit register

$$\mathbb{C}\left[\mathbb{Z}/2\mathbb{Z}\right]^{\otimes n} \otimes \mathbb{C}\left[\mathbb{Z}/2\mathbb{Z}\right]^{\otimes L}.$$

3) For $m \in \{n; L\}$ we identify the Hilbert space defined as the group algebra over $\mathbb{C}$ of the cyclic group $\mathbb{Z}/2^m\mathbb{Z}$ with the m q-bit register:

$$\mathbb{C}\left[\mathbb{Z}/2^m\mathbb{Z}\right] \longrightarrow \mathbb{C}\left[\mathbb{Z}/2\mathbb{Z}\right]^{\otimes m}$$

$$\sum_{k=0}^{m} i_k \cdot 2^k \longmapsto e_{i_0} \otimes \cdots \otimes e_{i_{m-1}}$$

(the elements $0, 1, \ldots, 2^m - 1 \in \mathbb{C}\left[\mathbb{Z}/2^m\mathbb{Z}\right]$ form an orthonormal basis by definition.)

Let V_m denote this Hilbert space.

4) We start with the state

$0 \otimes 0 \in V_n \otimes V_L$

[N.B.: the first 0 in $0 \otimes 0$ denotes the unit vector

$0 \in \mathbb{Z}/2^n\mathbb{Z} \subset \mathbb{C}[\mathbb{Z}/2^n\mathbb{Z}]$

same remark for the second 0 in $0 \otimes 0$.]

We apply $W_n \otimes id$ and we get

$$\left(\frac{1}{2^{n/2}} \sum_{x \in \mathbb{Z}/2^n\mathbb{Z}} x \right) \otimes 0$$

↑ homogeneous superpos. of all states.

5) Let $f : \mathbb{Z}/2^n\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z} \subset \mathbb{Z}/2^L\mathbb{Z}$

$f = f_{y_0}$, $f_{y_0}(x) \doteq y_0^x \ [N]$ where $1 < y_0 < N$ is fixed and choosen at random (see Prop. p. 11 and Lemma p. 14 of Lecture I).

Let $U_f : V_n \otimes V_L \to V_n \otimes V_L$

$$x \otimes y \longmapsto x \otimes \lambda(f(x))y .$$

$$U_f \left(\frac{1}{2^{n/2}} \sum_{x \in \mathbb{Z}/2^n\mathbb{Z}} x \otimes 0 \right)$$

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

- This is the heart of the algorithm:

the state of the first register

$\frac{1}{2^{n/2}} \sum_{x \in \mathbb{Z}/2^n\mathbb{Z}} x$ is the homogeneous

superposition of all the fundamental states $x \in \mathbb{Z}/2^n\mathbb{Z}$, but it is a single state.

- The unitary operator U_f can be theoretically implemented on a quantum computer as the composition of $O(n^3)$ (or even $O(n^2 \log n \log\log n)$) elementary quantum gates.
This is because the classical modular exponentiation $\exp_{y_0}(x) = y_0^x = f(x)\ [N]$ $N \leq 2^n$ can be performed with $O(n^3)$ (or even $O(n^2 \log n \log\log n)$) classical gates. (The NAND and COPY classical gates generate all classical gates)
(see Führer for recent results).
- The point is that the linearity of U_f gives the state:

$$U_f\left(\frac{1}{2^{n/2}} \sum_{x \in \mathbb{Z}/2^n\mathbb{Z}} x \otimes 0\right) =$$

$$\frac{1}{2^{n/2}} \sum_{x \in \mathbb{Z}/2^n\mathbb{Z}} U_f(x \otimes 0) = \frac{1}{2^{n/2}} \sum_{x \in \mathbb{Z}/2^n\mathbb{Z}} x \otimes f(x),$$

which encyphers <u>all</u> the values of f!
But we can't "see" them, we can only apply a measurement and get <u>one</u> of them.

6) Apply the measurement $\{id \otimes P_y\}_{y \in \mathbb{Z}/2^L\mathbb{Z}}$ of $V_n \otimes V_L$ to the state $\frac{1}{2^{n/2}} \sum_{x \in \mathbb{Z}/2^n\mathbb{Z}} x \otimes f(x)$,

where P_y is the orthonormal projection on the complex line (y) in V_L.

We observe $y \in \mathbb{Z}/2^L\mathbb{Z}$ with probability

$$\left\| \frac{1}{2^{n/2}} \sum_{x \in \mathbb{Z}/2^n\mathbb{Z}} x \otimes P_y(f(x)) \right\|^2$$

$$= \frac{1}{2^n} \left\| \sum_{x \in f^{-1}(y)} x \otimes y \right\|^2 = \frac{1}{2^n} \sum_{x \in f^{-1}(y)} \|x \otimes y\|^2$$

$$= \frac{1}{2^n} \# f^{-1}(y) .$$

After this measurement the state projects to:

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

Let $b \in \mathbb{Z}/2^n\mathbb{Z}$ s.t. the probability of observing b is non-zero. Hence $f^{-1}(b)$ is non-empty (and $0 \leq b \leq N-1$) and if r denotes the order of γ_0 in $(\mathbb{Z}/N\mathbb{Z})^*$ (that is if r is the smallest non-zero integer s.t. $f(r) \equiv 1 \,[N]$), then there exists $0 \leq a < r$ s.t.

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

where

$$K_a := \max\{ m \in \mathbb{N} \,:\, a + (m-1)\cdot r < 2^n \}.$$

Let $\psi : \mathbb{Z}/2^n\mathbb{Z} \to \mathbb{C}$:

$$\psi(x) = \begin{cases} 1/\sqrt{K_a} & \text{if } r \mid x-a \\ 0 & \text{if not.} \end{cases}$$

Hence

$$\frac{1}{\sqrt{\#f^{-1}(b)}} \sum_{x \in f^{-1}(b)} x = \frac{1}{\sqrt{K_a}} \sum_{k=0}^{K_a - 1} a + kr$$

$$= \sum_{x \in \mathbb{Z}/2^n\mathbb{Z}} \psi(x) \cdot x \in \mathbb{C}\left[\mathbb{Z}/2^n\mathbb{Z}\right].$$

7) Identifying $L^2(\mathbb{Z}/2^n\mathbb{Z})$ with $\mathbb{C}[\mathbb{Z}/2^n\mathbb{Z}]$, we apply the Fourier transform to the first register:

$$F \otimes id_{V_L}\left(\frac{1}{\sqrt{\#f^{-1}(b)}} \sum_{x \in f^{-1}(b)} x\right) \otimes b$$

$$= F \otimes id_{V_L}(\psi \otimes b)$$

$$= F(\psi) \otimes b,$$

where

$$F(\psi) = \sum_{c=0}^{2^n-1} \hat{\psi}(c) \cdot c \in \mathbb{C}[\mathbb{Z}/2^n\mathbb{Z}],$$

and

$$\hat{\psi}(c) = \langle \psi, \frac{\chi^c}{2^{n/2}} \rangle =$$

$$= \frac{1}{\sqrt{K_a \cdot 2^n}} \sum_{k=0}^{K_a-1} e^{-\left[\frac{2i\pi c(a+kr)}{2^n}\right]}.$$

This can be done with $O(n^2)$ elem. quantum gates.

8) Apply the measurement

$$\{ P_x \otimes id \}_{x \in \mathbb{Z}/2^n\mathbb{Z}} \quad \text{of} \quad V_n \otimes V_L$$

to the state

$$\sum_{c=0}^{2^n-1} \hat{\varphi}(c) \cdot c \otimes b$$

where P_x is the orth. proj. of V_n to the line $\langle x \rangle$.

We observe $c \in \mathbb{Z}/2^n\mathbb{Z}$ with probability

$$\| \hat{\varphi}(c) \cdot c \otimes b \|^2 = |\hat{\varphi}(c)|^2$$

$$= \frac{1}{K_a 2^n} \left(\sum_{k=0}^{K_a-1} e^{-\left[\frac{2\pi i c(a+kr)}{2^n}\right]} \right)^2 .$$

<u>Proposition</u>: The probability of observing $0 \le c < 2^n$ such that $\exists\, s \in \mathbb{N}$ with $\left| \frac{c}{2^n} - \frac{s}{r} \right| < \frac{1}{2r^2}$ and $\gcd(s,r) = 1$ is at least

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

Proof of Proposition p. 43.

For $0 \leq s \leq r-1$ integer, consider the following r reals of $s \cdot \frac{2^n}{r} < 2^n$. We expect the observed value of the measurement $\{P_x \otimes Id\}_{x \in \mathbb{Z}/2^n\mathbb{Z}}$ to be close to one of this real (see p. 34 remarks about r periodic functions and their Fourier transform). Let $\delta_s \in \left[-\frac{1}{2}, \frac{1}{2}\right]$ s.t.

$$c_s \doteq s \cdot \frac{2^n}{r} + \delta_s \quad \text{is an integer.}$$

Notice that δ_s obviously exists for each s because any real, in particular $s \cdot \frac{2^n}{r}$ is at distance at most $\frac{1}{2}$ from an integer.

Notice that $0 \leq c_s < 2^n$ because $s \cdot \frac{2^n}{r} \geq 0$ and $d\left(\frac{r-1}{r} \cdot 2^n, 2^n\right) > \frac{1}{2}$.

Notice that the y_s are r distinct integers because $d(c_s, c_t) > 1$ if $s \neq t$, $(r < 2^n)$.

The probability of observing y_s is

$$\mathcal{P}(c_s) = \frac{1}{K_a \cdot 2^n} \left| \sum_{k=0}^{K-1} e^{\frac{2i\pi c_s k r}{2^n}} \right|^2 .$$

We compute: $(c_s \doteq c \quad K_a \doteq K)$ [if $\delta_s = 0$ we get $\frac{1}{K \cdot 2^n} \cdot K^2 = \frac{K}{2^n} \geq$

$$\frac{1}{r} - \frac{a}{r 2^n} = \frac{1}{r}\left(1 - \frac{a}{2^n}\right) \geq_{*} \frac{1}{r}\left(1 - \frac{1}{N}\right) \quad \left[* \ \frac{a}{2^n} < \frac{N}{2^n} \leq \frac{N}{N^2} \leq \frac{1}{N}\right]$$

$$\sum_{k=0}^{K_a-1} e^{\frac{2\pi i c k r}{2^n}} = \frac{1 - e^{\frac{2\pi i c K_a r}{2^n}}}{1 - e^{\frac{2\pi i c r}{2^n}}} =$$

$$= e^{\frac{i\pi c (K_a - 1) r}{2^n}} \cdot \frac{\sin\left(\frac{\pi c K_a r}{2^n}\right)}{\sin\left(\frac{\pi c r}{2^n}\right)} \quad /$$

$$\left(\text{because } \frac{1 - e^{in\theta}}{1 - e^{i\theta}} = e^{i\frac{\theta}{2}(n-1)} \frac{\sin\left(\frac{n\theta}{2}\right)}{\sin\left(\frac{\theta}{2}\right)} \right).$$

Hence, for any $0 \le s \le r-1$

$$\mathcal{P}(c_s) = \frac{1}{2^n K} \cdot \frac{\sin^2\left(\frac{\pi \delta_s K r}{2^n}\right)}{\sin^2\left(\frac{\pi \delta_s r}{2^n}\right)} \cdot$$

As $\frac{2}{\pi} x \le \sin x \le x$, if $0 \le x \le \frac{\pi}{2}$, and as

$0 \le \frac{\pi |\delta_s| K r}{2^n} \le \frac{\pi}{2}$ (by def. $K_a = \max \{ m : a + (m-1) r < 2^n \}$, hence $\boxed{\frac{Kr}{2^n} < \frac{r-a}{2^n} < \frac{r}{2^n} < 1}$)

and as $0 \le \frac{\pi |\delta_s| r}{2^n} \le \frac{\pi}{2}$, we obtain:

$$\mathcal{P}(c_s) \ge \frac{1}{2^n K} \cdot \frac{\left(\frac{2}{\pi} \frac{\pi |\delta_s| K r}{2^n}\right)^2}{\left(\frac{\pi |\delta_s| r}{2^n}\right)^2} = \frac{4}{\pi^2} \frac{K}{2^n} \ge \frac{4}{\pi^2} \frac{1}{r} \left(1 - \frac{1}{N}\right)$$

Taking the measure of the y_s such that s is prime to r, we get $\varphi(r)$ possibilities (the case $s=r$ is excluded because $s<r$ by def. but $(r,r) \neq 1$) each with measure at least $\frac{4}{N^2}\frac{1}{r}\left(1-\frac{1}{N}\right)$. This proves the proposition. ∎

Theorem: (see Rosser and Schoenfeld 1962)

If $r \geq 3$

$$\frac{\varphi(r)}{r} > \frac{1}{e^{\gamma}\log\log r + \frac{2{,}50637}{\log\log r}}$$

where

$$\gamma = \lim_{n\to\infty}\left(1+\frac{1}{2}+\cdots+\frac{1}{n}-\log n\right)$$

$\simeq 0{,}58$ is Euler's c.t.

9) Compute the convergents of $\frac{c}{2^n}$ with the Euclidean algorithm, and check their denominators.

[This requires $O(n^3)$ classical gates. ($O(n^3)$: ↑ Eucl. alg. (include a test of divisib. $O(n^2)$ when running Euclidean alg.).]

According to Theorem p. 36, if c is as in Proposition p. 43 (and this happens with a positive probability) one of the denominators is t.

End of the algorithm.