Shor's algorithm (on an ideal quantum computer)

(*"Only" the mathematical part*)

Assis Azevedo

Centro de Matemática e Departamento de Matemática da Universidade do Minho

11 de Abril de 2019

Algorithms for Quantum computation: discrete logarithms and factoring -P. W. Shor

In *35th Annual Symposium on Foundations of Computer Science - FOCS* 1994, pages 124 - 134. IEEE, 1994

Discrete logarithms and integer factoring are two number-theory problems which have been studied extensively but for which no polynomial-time algorithms are known. In fact, these problems are so widely believed to be hard that cryptosystems based on their hardness have been proposed, and the RSA public key cryptosystem, based on the hardness of factoring, is in use. We show that these problems can be solved in BQP (bounded-error quantum polynomial time).

Notation

$\mathbb{Z}_{\mathrm{N}}^{*} = \{a \in \mathbb{N} : 1 \leq a \leq \mathrm{N},\ (a, \mathrm{N}) = 1\}.$

1. Examples:
   - $\mathbb{Z}_{27}^{*}$=$\{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26\}$;
   - $\mathbb{Z}_{21}^{*} = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$;
   - $\mathbb{Z}_{p^m}^{*} = \{1, 2, \ldots, p^m\} \setminus \{p, 2p, \ldots, p^{m-1}p\}$;
   - $\mathbb{Z}_{pq}^{*} = \{1, 2, \ldots, pq\} \setminus \{p, 2p, \ldots, (q-1)p, q, 2q, \ldots, (p-1)q\}$;

$$\left|\mathbb{Z}_{p^m}^{*}\right| = p^{m-1}(p-1), \quad \left|\mathbb{Z}_{p\,q}^{*}\right| = (p-1)(q-1).$$

Euler function.

Definition

$\varphi(\mathrm{N}) = |\mathbb{Z}_{\mathrm{N}}^*|$.

$$\mathrm{N} = \prod_{i=1}^{k} p_i^{n_i} \quad \Longrightarrow \quad \varphi(\mathrm{N}) = \prod_{i=1}^{k} p_i^{n_i - 1}(p_i - 1).$$

From now on N is odd and $k \geq 2$.

A key result about the Euler function - difficult!

Theorem 1

$$\frac{\varphi(m)}{m} \geq \frac{1}{4\log(\log(m))}, \quad for\ m \geq m_0.$$

Notice that $\frac{\varphi(m)}{m} = \prod_{p|m} \frac{p-1}{p}$.

We only need

$$r|\varphi(\mathrm{N}) \Rightarrow \frac{\varphi(r)}{r} \geq \frac{1}{4\log(\log(\mathrm{N}))}.$$

Order modulo N

Definition

If $y \in \mathbb{Z}_N^*$, then the order of y modulo N ($\mathrm{ord}_N y$) is the smallest natural r such that $y^r = 1$, modulo N.

1. Example. $N = 21$. Notice that $\varphi(N) = 12$.
   $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 11$, $\boxed{2^6 = 1}$,
   $2^7 = 2$, $2^8 = 2^2$, $2^9 = 2^3$, $2^{10} = 2^4$, $2^{11} = 2^5$, $2^{12} = 1$,....

   $\therefore \mathrm{ord}_{21} 2 = 6$.

y	1	2	4	5	8	10	11	13	16	17	19	20
$\mathrm{ord}_{21} y$	1	6	3	6	2	6	6	2	3	6	6	2

2. Em $\mathbb{Z}_N^*$, $y^s = y^t$ if and only if $\mathrm{ord}_N y$ divides $s - t$.

3. If $y \in \mathbb{Z}_N^*$ then $\mathrm{ord}_N y$ divides $\varphi(N)$ (Euler's Theorem).

Another key result!

Recall that $\mathrm{N} = \prod_{i=1}^{k} p_i^{n_i}$, $k \geq 2$ and p_i odd prime number.

Theorem 2

If $\mathrm{N} \in \mathbb{N}$ *and* $y \in \mathbb{Z}_{\mathrm{N}}^*$ *then:*

$$\mathrm{Prob}\left(\mathrm{ord}_{\mathrm{N}} y \text{ even and } \mathrm{N} \not| (y^{\frac{r}{2}} + 1)\right) \geq 1 - \frac{1}{2^{k-1}} \geq \frac{1}{2}.$$

It is a good exercise for students of Teoria de Números.

Shor's algorithm. Reduction to "order finding" in $\mathbb{Z}_N^*$

Steps:

- Choose randomly $1 < y < \mathrm{N}$ and evaluates $d = \gcd(y, \mathrm{N})$;
- If $d \neq 1$ then d is a nontrivial divisor of N;
- If $d = 1$ then, with probability greater or equal to $\frac{1}{2}$, $\mathrm{ord}_{\mathrm{N}} y = r$ is even and $\mathrm{N} \not| (y^{\frac{r}{2}} + 1)$;
- $\mathrm{N} \Big| (y^r - 1) = \left(y^{\frac{r}{2}} + 1\right)\left(y^{\frac{r}{2}} - 1\right)$;
- $\mathrm{N} \not| \left(y^{\frac{r}{2}} + 1\right)$ and $\mathrm{N} \not| \left(y^{\frac{r}{2}} - 1\right)$;
- $\gcd(\mathrm{N}, y^{\frac{r}{2}} + 1)$, $\gcd(\mathrm{N}, y^{\frac{r}{2}} - 1)$ are nontrivial divisors of N;
- Everything works $\boxed{\text{if we know } r}$.

$$\frac{7225}{972} = 7 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{5 + \cfrac{1}{6}}}}}.$$

Notation: $\frac{7225}{972} = [7; 2, 3, 4, 5, 6]$

Convergents:

$$\begin{aligned} [7] &= 7 \\ [7;2] &= \tfrac{15}{2} \\ [7;2,3] &= \tfrac{52}{7} \end{aligned} \quad \Bigg\| \quad \begin{aligned} [7;2,3,4] &= \tfrac{223}{30} \\ [7;2,3,4,5] &= \tfrac{1167}{157} \\ [7;2,3,4,5,6] &= \tfrac{7225}{972} \end{aligned}$$

Theorem 3

If $\left|x - \frac{p}{q}\right| < \frac{1}{2q^2}$ *then* $\frac{p}{q}$ *is a convergent of* x.

A trigonometric inequality

$$f(\alpha) \quad = \quad \left| \sum_{k=0}^{M-1} e^{-i\alpha k} \right|^2 = \frac{\operatorname{sen}^2\left(\frac{\alpha M}{2}\right)}{\operatorname{sen}^2\left(\frac{\alpha}{2}\right)}$$

- f decrescente em $\left[0, \dfrac{\pi}{M-1}\right]$;
- $f(\alpha) \geq \left(1 - \left(\dfrac{\alpha}{2}\right)^2\right)\left(\dfrac{2}{\alpha}\right)^2$ if $\alpha \geq \frac{\pi}{M+1}$.

Quantum - notation

$\mathbb{C}X$ is the complex vector space with basis the elements of X.

- $\mathbb{C}\mathbb{Z}_2 = \left\{\alpha\,|0\rangle + \beta\,|1\rangle : \alpha, \beta \in \mathbb{C}\right\}$.
- $\mathbb{C}\mathbb{Z}_2^{\otimes n} = \mathbb{C}\mathbb{Z}_2 \otimes \cdots \otimes \mathbb{C}\mathbb{Z}_2$.
- $\left\{\, |a_0\rangle \otimes \cdots \otimes |a_{n-1}\rangle : a_i \in \mathbb{Z}_2 \right\}$ forms a basis for $\mathbb{C}\mathbb{Z}_2^{\otimes n}$.
- $\mathbb{C}\mathbb{Z}_2^{\otimes n} \sim \mathbb{C}\mathbb{Z}_2^{n} \sim \mathbb{C}\mathbb{Z}_{2^n}$, as vectorial spaces, which leads us to identify $|a_{n-1}\rangle \otimes \cdots \otimes |a_0\rangle$ with $|a_{n-1} \cdots a_0\rangle$ and $\left|2^{n-1}a_{n-1} + \cdots + 2^0 a_0\right\rangle$.

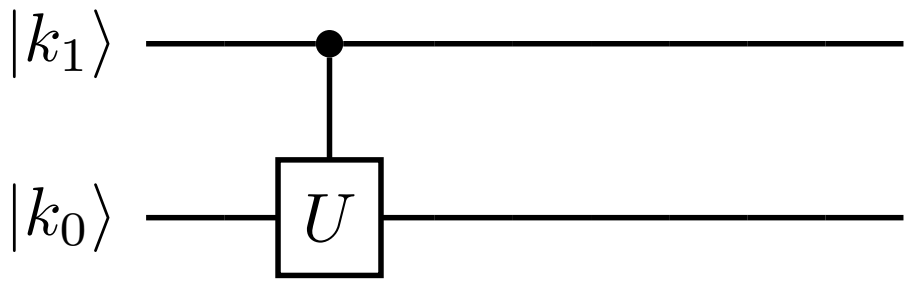
The unitary transformations $T : \mathbb{C}\mathbb{Z}_2^{\otimes n} \to \mathbb{C}\mathbb{Z}_2^{\otimes n}$ will be defined on the elements of the referred basis.

Gates we will use!

- Walsh-Hadamard: $H\left|x\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle + e^{-i\,\pi\,x}\left|1\right\rangle\right)$;
- $H^{\otimes n}\left|0\right\rangle = \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}\left|k\right\rangle$

Gates we will use! (2)

- Phase shift. $R_s\,|0\rangle = |0\rangle\,; \quad R_s\,|1\rangle = e^{-\frac{i\,\pi}{2^s}}\,|1\rangle, \;\; s \in \mathbb{N};$
- Given U, $\quad \mathrm{ctr}(U)\,|1b\rangle = |1\rangle\,U(|b\rangle); \quad \mathrm{ctr}(U)\,|0b\rangle = |0b\rangle\,;$



Example: $\mathrm{ctr}(R_s)\,|ab\rangle = e^{\frac{-\pi\,i\,ab}{2^s}}\,|ab\rangle.$

- Simulation of $f : \mathbb{Z}_{2^m} \to \mathbb{Z}_{2^k}$,
  $U_f : \mathbb{C}\mathbb{Z}_{2^m} \otimes \mathbb{C}\mathbb{Z}_{2^k} \to \mathbb{C}\mathbb{Z}_{2^m} \otimes \mathbb{C}\mathbb{Z}_{2^k}$

$$U_f := |x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |y + f(x)\rangle\,.$$

$\mathcal{Q}_{2^n}$ - quantum Fourier transform

$$\mathcal{Q}_{2^n}\,|k\rangle \;=\; \frac{1}{\sqrt{2^n}}\sum_{b=0}^{2^n-1} e^{-\frac{2\,i\,\pi\,k\,b}{2^n}}\,|b\rangle\,, \qquad \text{for} \quad |k\rangle = |k_{n-1}\cdots k_1 k_0\rangle\,.$$

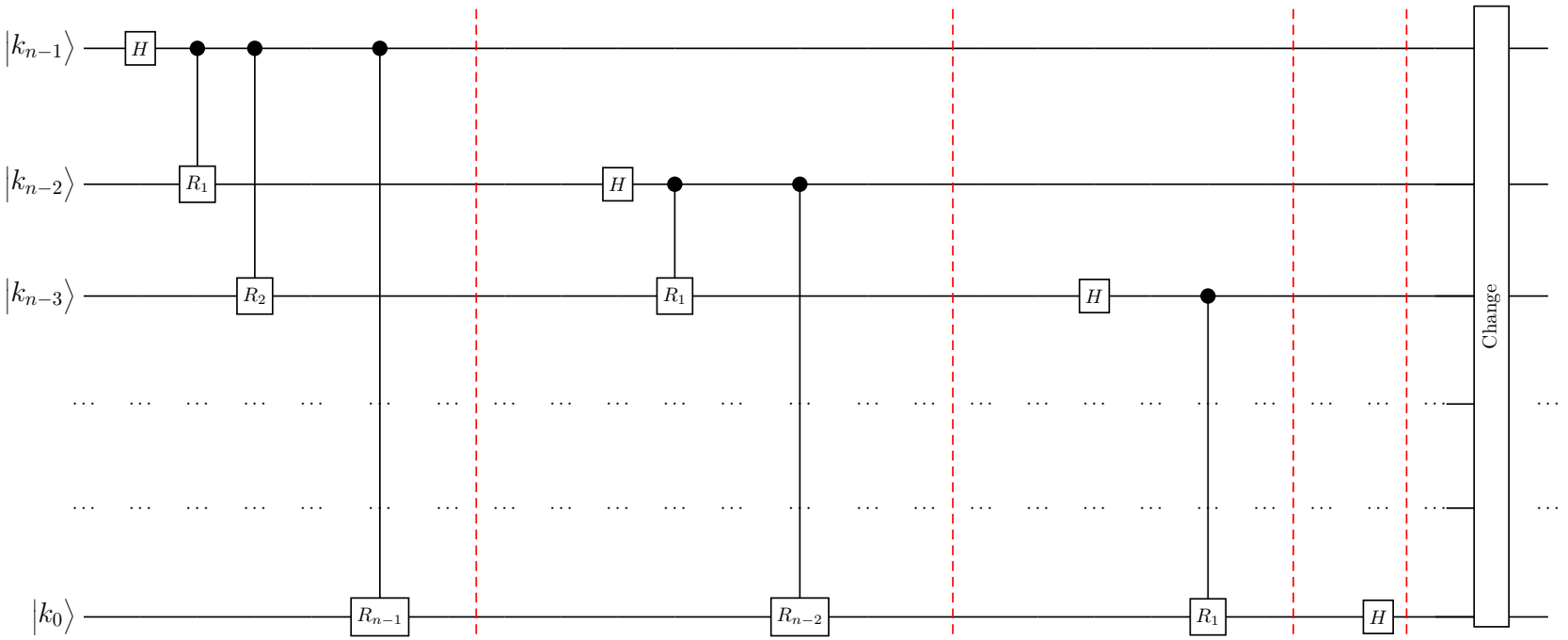
$(w = e^{i\frac{2\pi}{2^n}})$.

$$\frac{1}{\sqrt{2^n}}\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & w & w^2 & w^3 & \cdots & w^{2^n-1} \\ 1 & w^2 & w^4 & w^6 & \cdots & w^{2(2^n-1)} \\ 1 & w^3 & w^6 & w^9 & \cdots & w^{3(2^n-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & w^{2^n-1} & w^{2(2^n-1)} & w^{3(2^n-1)} & \cdots & w^{(2^n-1)(2^n-1)} \end{pmatrix}$$

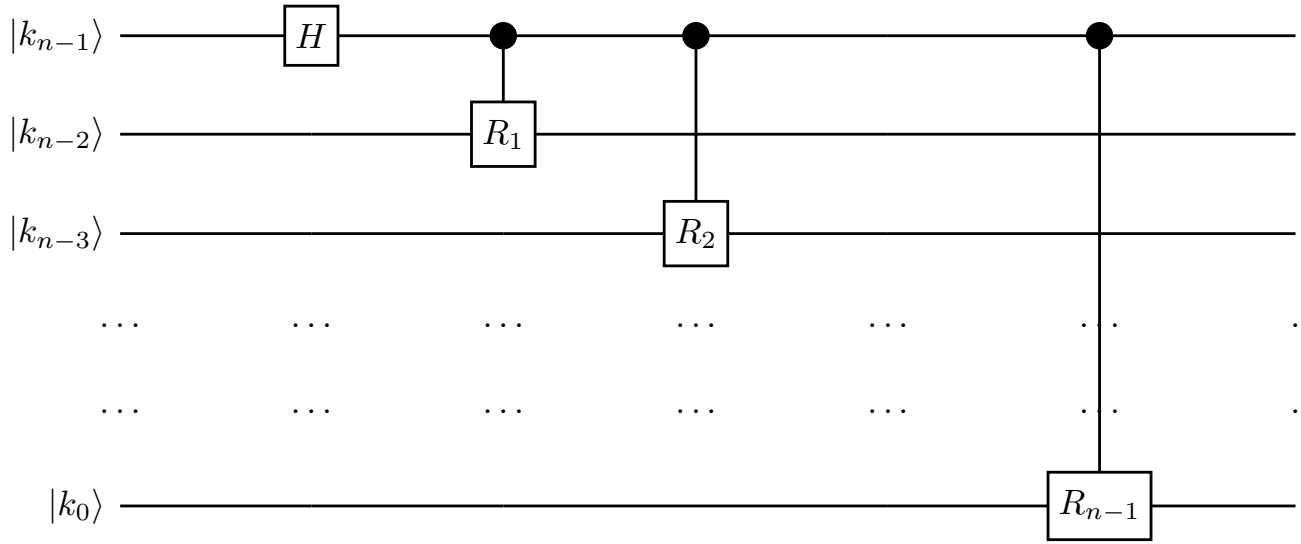
To show that the transformation is unitary we just need to observe that: $1 + z + \cdots + z^{q-1} = \frac{z^q-1}{z-1} = 0$, if $z = w^t$ and $z \neq 1$.

Implementation of $\mathcal{Q}_{2^n}$

$$\mathcal{Q}_{2^n}\,|k\rangle \quad = \quad \frac{1}{\sqrt{2^n}} \sum_{b=0}^{2^n-1} e^{-\frac{2\,i\,\pi\,k\,b}{2^n}}\,|b\rangle\,, \qquad \text{for} \quad |k\rangle = |k_{n-1}\cdots k_1 k_0\rangle\,.$$



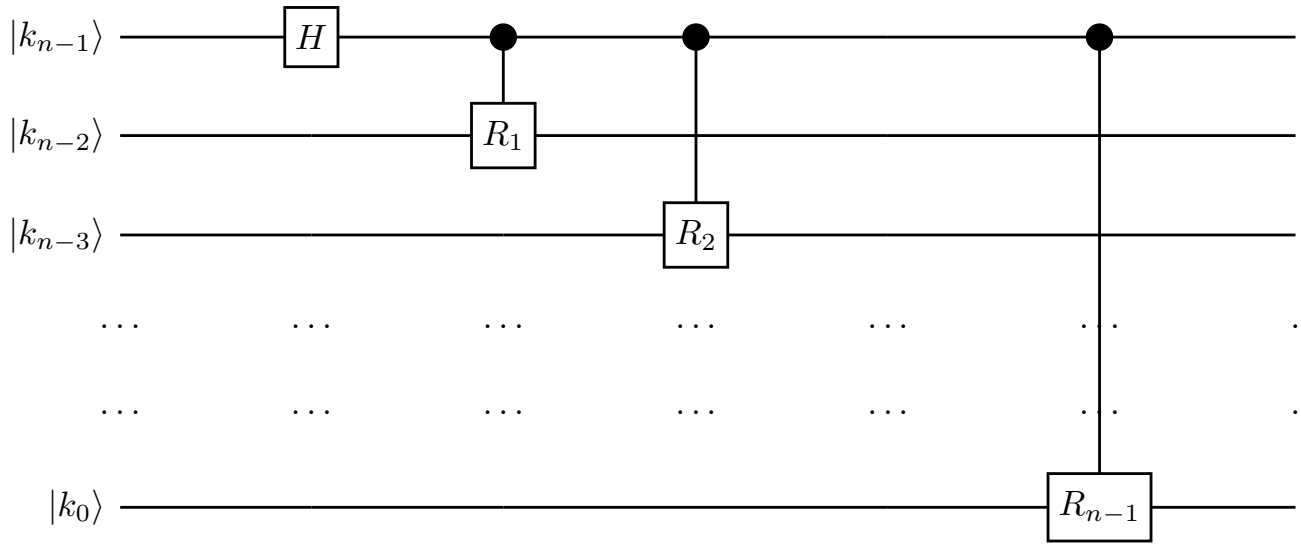
Implementation of $\mathcal{Q}_{2^n}$ - beginning (1)



$$|k\rangle \xrightarrow[H\otimes I^{n-1}]{} \frac{1}{\sqrt{2}}\left[|0\rangle + e^{-i\,\pi k_{n-1}}\,|1\rangle\right] \otimes |k_{n-2}\cdots k_0\rangle$$

$$\xrightarrow[\mathrm{ctr}(R_1)\otimes I^{n-2}]{} \frac{1}{\sqrt{2}}\left[|0\rangle + e^{-i\,\pi(k_{n-1}+\frac{k_{n-2}}{2})}\,|1\rangle\right] \otimes |k_{n-2}\cdots k_0\rangle\,.$$

Implementation of $\mathcal{Q}_{2^n}$ - beginning (2)



At the end of this sub-circuit we obtain

$$\frac{1}{\sqrt{2}}\left[|0\rangle + e^{-i\,\pi(k_{n-1}+\frac{k_{n-2}}{2}+\cdots+\frac{k_0}{2^{n-1}})}\,|1\rangle\right] \otimes |k_{n-2}\cdots k_0\rangle$$

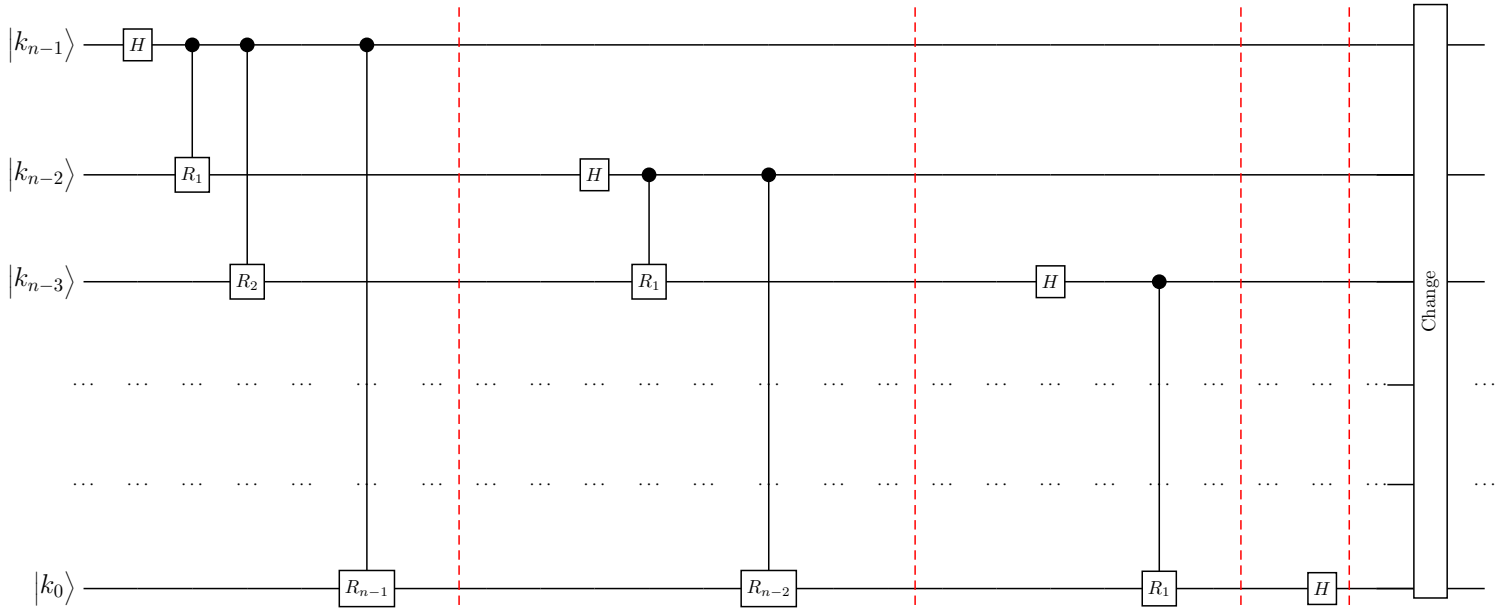
that is

$$\frac{1}{\sqrt{2}}\left[|0\rangle + e^{-\frac{2\,i\,\pi\,k}{2^n}}\,|1\rangle\right] \otimes |k_{n-2}\cdots k_0\rangle$$

or

$$\frac{1}{\sqrt{2}}\sum_{b_0=0}^{1} e^{-\frac{2\,i\,\pi\,k\,b_0}{2^n}}\,|b_0 k_{n-2}\cdots k_0\rangle\,.$$

Implementation of $\mathcal{Q}_{2^n}$ - end



$$|k\rangle \longmapsto \frac{1}{\sqrt{2^n}} \sum_{b_0=0}^{1} \sum_{b_1=0}^{1} \cdots \sum_{b_{n-1}=0}^{1} e^{-\frac{2\,i\,\pi\,k(b_0+2b_1+\cdots+2^{n-1}b_{n-1})}{2^n}} |b_0 b_1 \cdots b_{n-1}\rangle$$

$$\xrightarrow[Change]{} \frac{1}{\sqrt{2^n}} \sum_{b=0}^{2^n-1} e^{-\frac{2\,i\,\pi\,kb}{2^n}} |b\rangle = \mathcal{Q}_{2^n} |k\rangle$$

We used $\frac{n(n+1)}{2} + \lfloor \frac{n}{2} \rfloor$ $(\leq n^2)$ $\leq$ 2-qubit gates.

Algorithm to find r - steps 1 and 2

Step 1

- N odd that is not a power of a prime number, $y \in \mathbb{Z}_{\mathrm{N}}^*$;
- $L = \lceil \log_2 \mathrm{N} \rceil$;
- n such that $\mathrm{N}^2 \leq 2^n < 2\mathrm{N}^2$ $(n \in [2\log_2 \mathrm{N}, 2\log_2 \mathrm{N} + 1[\,)$;
- Two registers: the first with n qubits and the second with L;
- $$\begin{array}{rccc} f: & \mathbb{Z}_{2^n} & \to & \mathbb{Z}_{2^L}\,. \\ & m & \mapsto & y^m \pmod{\mathrm{N}} \end{array}$$

Step 2 Evaluate $U_f\,(H^{\otimes n} \otimes I_L)$ at $|0\rangle \otimes |0\rangle$. We obtain

$$|0\rangle\,|0\rangle \xmapsto[H^{\otimes n}\otimes I_L]{} \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes |0\rangle \xmapsto{U_f} \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes |f(x)\rangle\,.$$

Algorithm to find r - step 3

Step 3

- We observe the second register and find $b \in \mathbb{Z}_N$, with $b = f(a)$ e $0 \leq a < r$;
- In the first register we have

$$|\alpha\rangle = \frac{1}{\sqrt{M_a}} \sum_{k=0}^{M_a - 1} |a + kr\rangle \, .$$

  where M_a the larger integer such that $(M_a - 1)r + a < 2^n$;
- We apply $\mathcal{Q}_{2^n}$ to the first register and we get

$$\mathcal{Q}_{2^n} |\alpha\rangle = \sum_{c=0}^{2^n - 1} \tilde{\alpha}(c) |c\rangle \, , \quad \text{with } \tilde{\alpha}(c) = \frac{1}{\sqrt{M_a 2^n}} \sum_{k=0}^{M_a - 1} e^{-\frac{2\pi \, ic(a+kr)}{2^n}}$$

Preparation to the last step

For $0 \leq s < r$ with $\gcd(s, r) = 1$ let $c_s \in \{0, \ldots 2^n - 1\}$ be (unique):

$$c_s r \in \left[s2^n - \frac{r}{2}, s2^n + \frac{r}{2} \right[.$$

Notice that:

- $\left| \frac{c_s}{2^n} - \frac{s}{r} \right| < \frac{1}{2^{n+1}} < \frac{1}{2\mathrm{N}^2} < \frac{1}{2r^2} \quad (r^2 < \mathrm{N}^2 < 2^n)$;
- $\frac{s}{r}$ is a convergent of the fraction $\frac{c_s}{2^n}$;
- If the observed c is one of the c_s then we can find r.

Question

What is the probability of **observing** *an element of* $D = \{c_s : 0 \leq s < r,\ (s, r) = 1\}$ *in the previous step?*

Algorithm to find r - step 4

Theorem 4

The probability of the observed c in the previous step belongs to D is greater or equal to $\frac{1}{10\log(\log(\mathrm{N}))}$.

Proof:

$$
\begin{aligned}
P(c_s) &= \frac{1}{M_a 2^n}\left|\sum_{k=0}^{M_a-1} e^{-\frac{2\pi\, i c_s (a+kr)}{2^n}}\right|^2 = \frac{1}{M_a 2^n}\left|\sum_{k=0}^{M_a-1} e^{-\frac{2\pi\, i c_s\, kr}{2^n}}\right|^2 \\
&\geq \frac{1}{M_a 2^n}\left|\sum_{k=0}^{M_a-1} e^{-\frac{\pi\, i\, kr}{2^n}}\right|^2 \geq \frac{2^{n+2}}{\pi^2 r^2 M_a}\left(1-\left(\frac{\pi r}{2^{n+1}}\right)^2\right) \\
&\geq \frac{4}{\pi^2 r}\left(1-\left(\frac{\pi r}{2^{n+1}}\right)^2\right).
\end{aligned}
$$

Algorithm to find r - step 4 (continuation)

The requested probability is

$$\begin{aligned} P &\geq \varphi(r) \cdot \frac{4}{\pi^2 r} \left(1 - \left(\frac{\pi r}{2^{n+1}}\right)^2\right) \\ &\geq \frac{\varphi(r)}{r} \cdot \underbrace{\frac{4}{\pi^2}\left(1 - \frac{\pi^2}{4\mathrm{N}^2}\right)}_{\geq \frac{2}{5}} \quad \text{as } r < \mathrm{N} \text{ and } 2^n \geq \mathrm{N}^2 \\ &\geq \frac{1}{10\log(\log(\mathrm{N}))} \quad \text{for all } N. \end{aligned}$$

Final step

By repeating the process $B \log(\log(\mathrm{N}))$ times, the probability of observing an element of D is

$$1 - \left(1 - \frac{1}{10 \log(\log(\mathrm{N}))}\right)^{B \log(\log(\mathrm{N}))} \geq 1 - e^{-10\,B}.$$