3.6 Quantum Fourier Transform and period finding by Shor

Generalizing Simon's problem let us consider a function

(143) $$y = f(x)$$

defined on a finite interval discretized into 2^n elements characterized by an integer

(144) $$x \in \{0, 1, 2, \dots, 2^n - 1\}$$

(145) $$f: \underbrace{\{0,1\}^n}_{x} \longrightarrow \underbrace{\{0,1\}^y}_{y}$$

Let assume $f(x)$ has an unknown period r

$$1 << r << 2^n$$

(146) $$f(x + mr) = f(x) \qquad r, m \in \mathbb{N}$$

"normal" addition

$$x, x+mr \in \{0, 1, 2, \dots 2^n - 1\}$$

To find r is classically a difficult task even if the evaluation of $f(x)$ itself can be made in poly(n) steps!

A key element to finding periods is the discrete Fourier transformation:

$$f(x) \longrightarrow \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{\frac{2\pi i x y}{N}} f(y)$$

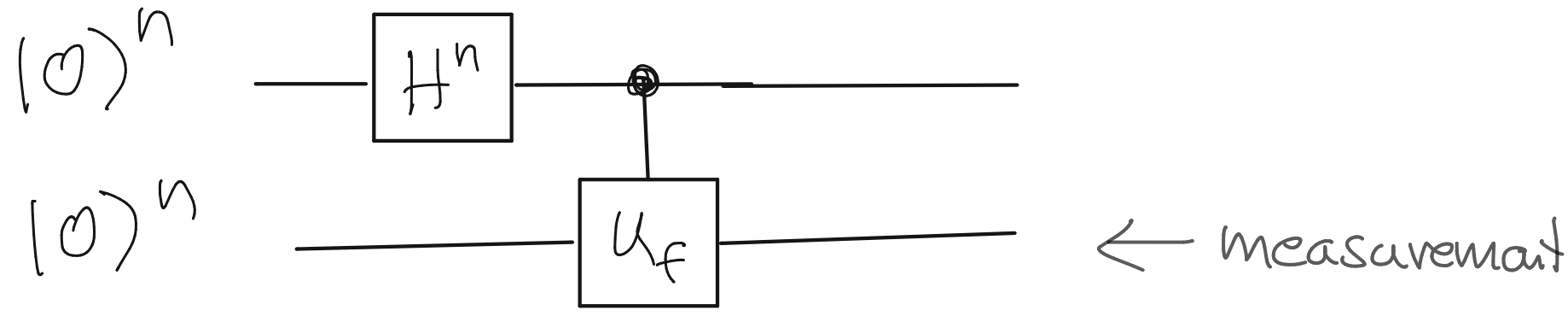
Since $N = 2^n$ the FTrafo requires exponentially many operations.

(A) Period finding using the quantum Fourier transformation

We will now show that given we can implement the quantum Fourier transformation $(x, y \in \mathbb{N})$

(147) QFT $|x\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{y=1}^{N-1} e^{\frac{2\pi i x y}{N}} |y\rangle$

we can determine the period r. Similar to Simon problem



$|\underline{0}\rangle = |0\rangle^n$

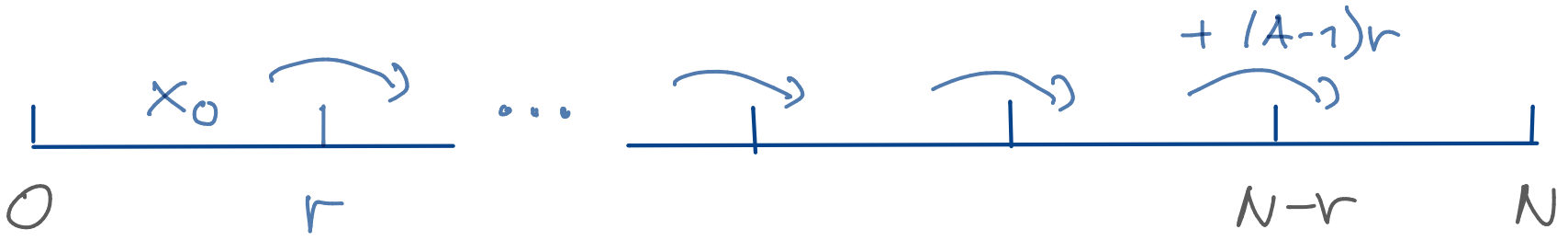
(148)
$$|\underline{0}\rangle|0\rangle \xrightarrow{H^n} \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|0\rangle$$
$$\xrightarrow{U_f} \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|f(x)\rangle$$

Measurement of 2nd register with result $f(x_0)$
(where x_0 is $0 \le x_0 < r$ but unknown)
projects 1st register to

$$(149) \qquad \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |x_0 + jr\rangle \qquad A \in \{0,1,2,\dots,2^n-1\}$$

where

$$(150) \qquad N - r \le x_0 + (A-1)r < N$$



or

$$(151) \qquad \boxed{A - 1 < \frac{N}{r} < A + 1} \qquad \frac{x_0}{r} < 1$$

If N/r is integer $\Rightarrow A = N/r$.

Problem: How to find r from eq. (149)?
Projection to computational basis would not give information about r.

$\Rightarrow$ QFT rule

$$QFT \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |x_0 + jr\rangle =$$

$$(152) \qquad = \frac{1}{\sqrt{NA}} \sum_{y=0}^{N-1} e^{\frac{2\pi i x_0 y}{N}} \sum_{j=0}^{A-1} e^{\frac{2\pi i r y j}{N}} |y\rangle$$

The probability to find a specific $|y\rangle$ in this state is

(153) $$p(y) = \frac{A}{N}\left[\frac{1}{A}\sum_{j=0}^{A-1} e^{2\pi i \frac{ry}{N}j}\right]^2$$

Here the unknown x_0 does no longer appear! ☺

$p(y)$ is large if $\frac{ry}{N}$ is an integer.

- E.g. if $\frac{N}{r} = A$ (see eq. (151)) than

$$\therefore\quad p(y) = \frac{1}{r}\left[\frac{1}{A}\sum_{j=0}^{A-1} e^{2\pi i \frac{jy}{A}}\right]^2 = \begin{cases} \frac{1}{r} & y = mA \\ 0 & \text{else} \end{cases}$$

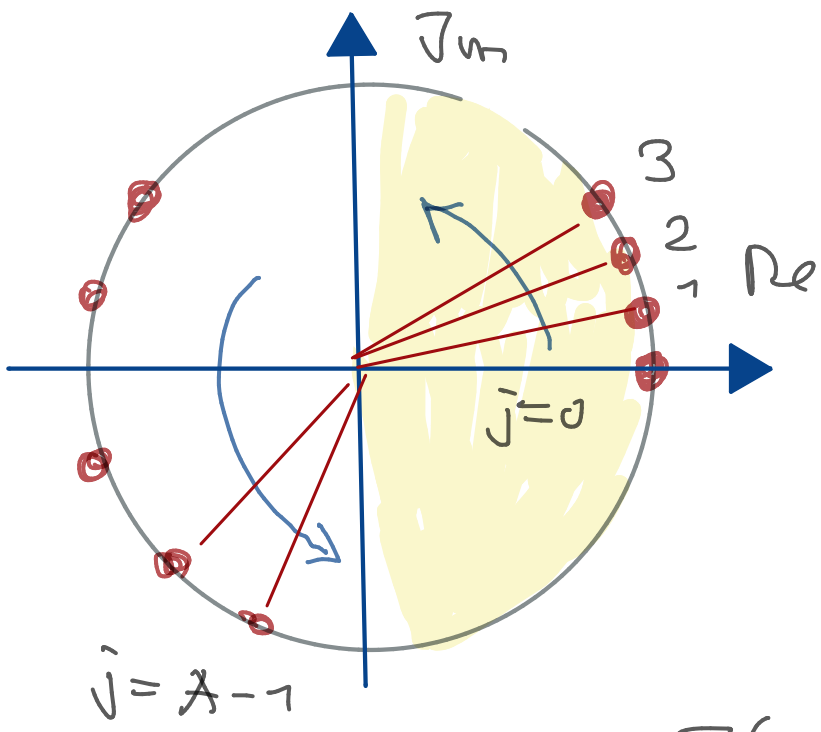
$\uparrow$ $\frac{N}{r} = A$

- In general:

(154) $$\theta_y \equiv 2\pi \frac{ry \pmod N}{N}$$

(155) $$\sum_{j=0}^{A-1} e^{ij\theta_y} = \frac{e^{iA\theta_y} - 1}{e^{i\theta_y} - 1}$$

For which values of y is this expression large?



Note $A - 1 < \frac{N}{r}$

⇒ all terms in (155) are in the same half of the complex plain if

$$-\frac{\pi r}{N} \le \theta_y \le \pi\frac{r}{N} \quad (156)$$

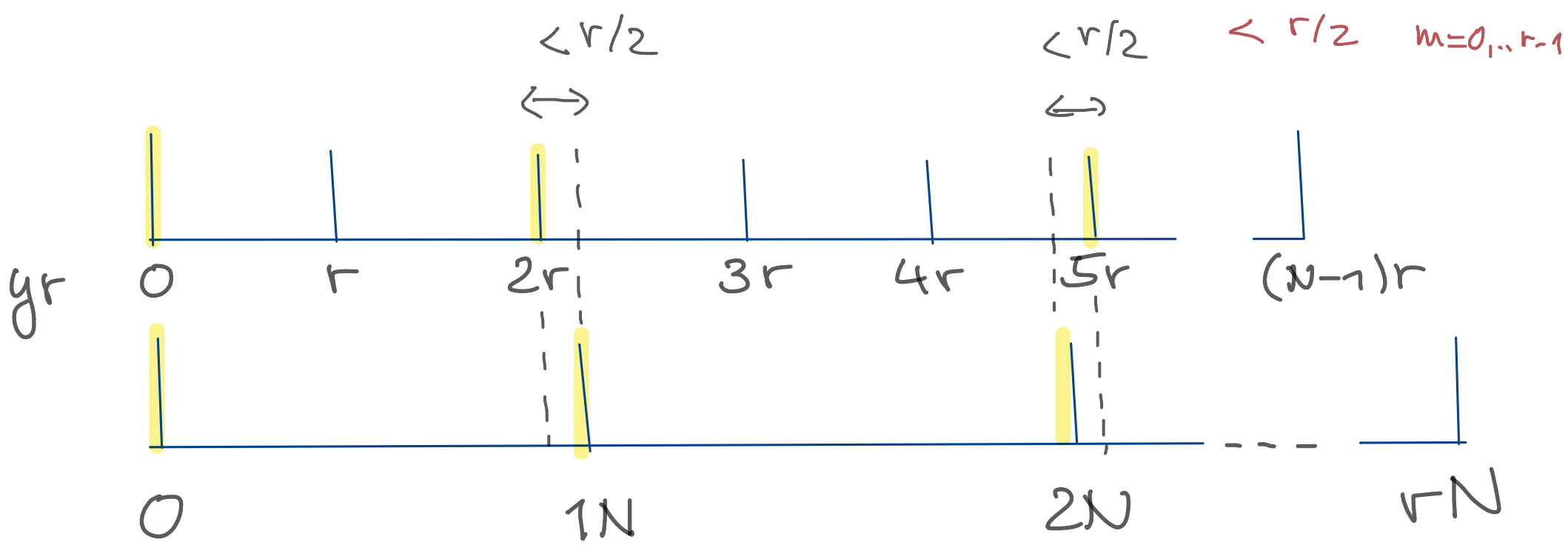
In this case $p(y)$ in (153) is extremal. Eq. (156) is equivalent to

$$(157) \qquad -\frac{r}{2} \leq yr \pmod N \leq \frac{r}{2}$$

There are exactly r values of y in $\{0,1,\dots,N-1\}$ which fulfill this condition:

there is always a point left or right of mN in distance $< r/2$ $\quad m=0,\dots r-1$

example

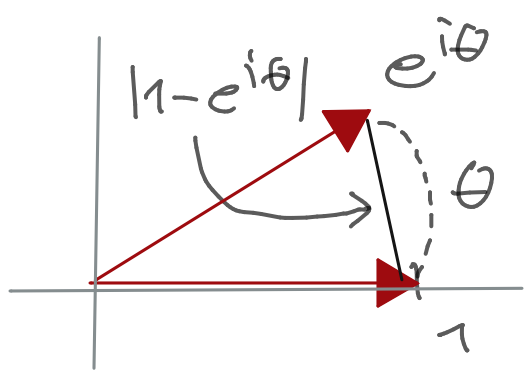


$y=0$ $\qquad$ $y=2$ $\qquad$ $y=5$ … fulfill (157)

Now we show that the measurement of the first register after QFTrafo yields with probability larger than $4/\pi^2 \simeq 0.405$ one of the r possible values of y that fulfill eq. (157)!

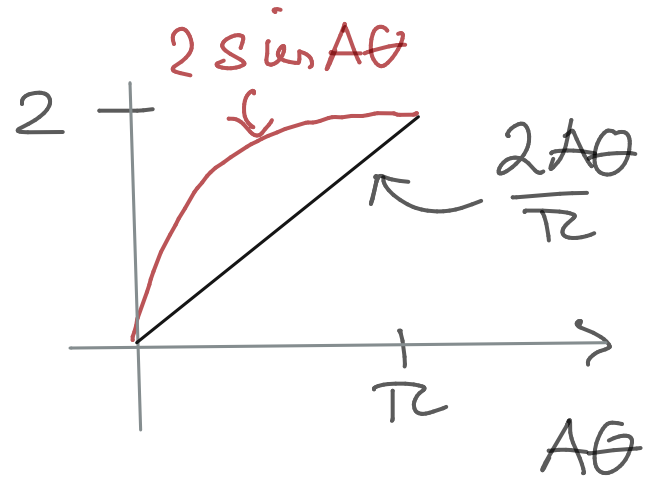
To see this note

$$|(1-e^{i\theta})| \leq |\theta|$$



furthermore for $A|\theta| \le \pi$

$$|1 - e^{iA\theta}| \ge \frac{2A|\theta|}{\pi}$$



since $|1-e^{iA\theta}| = |e^{i\frac{A\theta}{2}}|\,2\sin A\theta = 2\sin A\theta$.
This gives the estimate for $A|\theta| \le \pi$

$$\left|\frac{e^{iA\theta}-1}{e^{i\theta}-1}\right| \ge \frac{2A|\theta|}{\pi}\frac{1}{|\theta|} = \frac{2A}{\pi} \tag{158}$$

thus

$$p(y) = \frac{A}{N}\left|\frac{1}{A}\sum_{j=0}^{A-1} e^{ij\theta_y}\right|^2 = \frac{A}{N}\left|\frac{1}{A}\,\frac{e^{iA\theta_y}-1}{e^{i\theta_y}-1}\right|^2$$

$$\ge \frac{A}{N}\frac{4}{\pi^2} \underset{\text{eq.(157)}}{\ge} \frac{4}{\pi^2}\left(\frac{1}{r}-\frac{1}{N}\right) \ge \frac{4}{\pi^2}\frac{1}{r} \tag{159}$$

Since there are exact r values of y that fulfill (157) the total probability is

$$P_{tot} = \sum_{\substack{y \text{ that} \\ \text{fulfill (157)}}} p(y) \ge \frac{4}{\pi^2} \qquad \square \tag{160}$$

$\Rightarrow$ A measurement of QFT-transformed state projects with probability $P_{tot} \ge 4/\pi^2 \simeq 0.405$ to one of the y-values that fulfill eq. (157), i.e.

$$k\cdot\frac{N}{r} - \frac{1}{2} \le y \le k\frac{N}{r} + \frac{1}{2} \qquad k \in \{0,1,\dots,r-1\} \tag{161}$$

We see that knowledge of (one of these) y value

(162) $$y \longrightarrow \frac{k}{r}$$

With high probability k and r have no common divisor, which allows us to determine r. In the unlikely event that k and r have a common divisor the check if r is a period will give a "no" and we have to repeat the measurement to get a different y.

- Since the measurement of QFT transformed register gives a value of y that fulfills (157) only with finite probability we have to check if

(163) $$f(x) \overset{?}{=} f(x+r)$$

by evaluating U_f. If (163) is not fulfilled the actually detected value of y could be near a "true" value and we can check neighboring values or make a new measurement.

$\Rightarrow$ **Quantum Fourier transform allows to find the period of a function $f(x)$ with polynomial effort.**

(B) Implementation of Quantum Fourier transform

How to implement

$$(164)\quad \sum_{x=0}^{N-1} f(x)\,|x\rangle \longrightarrow \sum_{y=0}^{N-1} \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{\frac{2\pi i x y}{N}} f(x)\,|y\rangle$$

This operation corresponds to the multiplication with the $N \times N$ matrix

$$M_{xy} = \left(e^{\frac{2\pi i}{N}}\right)^{xy}$$

which is exponentially large in n $(N = 2^n)$.
Naively one would expect that this requires $O(N^2)$ elementary operations. ☹

This is however not the case!

- On the classical level there is the Fast-Fourier-Transform (FFT)

which only needs $O(N \log N)$ steps:

binary representation of x, y: $\quad x_j, y_j \in \{0,1\}$

$$(165)\quad x = x_{n-1} 2^{n-1} + x_{n-2} 2^{n-2} + \cdots + x_1 2 + x_0$$

$$y = y_{n-1} 2^{n-1} + y_{n-2} 2^{n-2} + \cdots + y_1 2 + y_0$$

In order to evaluate $\left(e^{\frac{2\pi i}{N}}\right)^{xy}$ we can ignore all terms in $x \cdot y$ that are multiples of $N = 2^n$, i.e.

(166)
$$\frac{x \cdot y}{N} = \frac{x \cdot y}{2^n} \hat{=} y_{n-1}\frac{x_0}{2} + y_{n-2}\left(\frac{x_1}{2} + \frac{x_0}{2^2}\right) + \cdots + y_0\left(\frac{x_{n-1}}{2} + \frac{x_{n-2}}{2^2} + \cdots + \frac{x_0}{2^n}\right)$$

FFT

$$= y_{n-1}[x_0] + y_{n-2}[x_0 x_1] + \cdots + y_0[x_0 x_1 \cdots x_{n-1}]$$

where

(167)
$$[x_0 x_1 \cdots x_k] \equiv \frac{x_k}{2} + \frac{x_{k-1}}{2^2} + \cdots + \frac{x_0}{2^{k-1}}$$

To evaluate this expression $\mathcal{O}(n)$ steps are needed i.e.

$$\tilde{f}(y) = \frac{1}{\sqrt{N}} \sum_{y=1}^{N-1} e^{2\pi i \frac{xy}{N}} f(x)$$

can be evaluated in $N \cdot \mathcal{O}(n) = N\mathcal{O}(\log N)$ steps. Speed-up is unfortunately only

$$\mathcal{O}(N^2) \xrightarrow[\text{FFT}]{} \mathcal{O}(N \log N) \quad \text{classical}$$

- Using quantum parallelism we can perform the Fouriertrafo much more efficiently!

$$QFT|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N} e^{2\pi i \frac{xy}{N}} |y\rangle =$$

(167) $$= \frac{1}{\sqrt{N}} \left(|0\rangle + e^{2\pi i [x_0]} |1\rangle\right)\left(|0\rangle + e^{2\pi i [x_0 x_1]} |1\rangle\right)$$
$$\cdots \left(|0\rangle + e^{2\pi i [x_0 x_1 x_2 \cdots x_{n-1}]} |1\rangle\right)$$

where

(168) $$[x_0 x_1 \cdots x_k] \equiv \frac{x_k}{2} + \frac{x_{k-1}}{2^2} + \cdots \frac{x_0}{2^k}$$

are the coefficients that appear in the FFT (166).

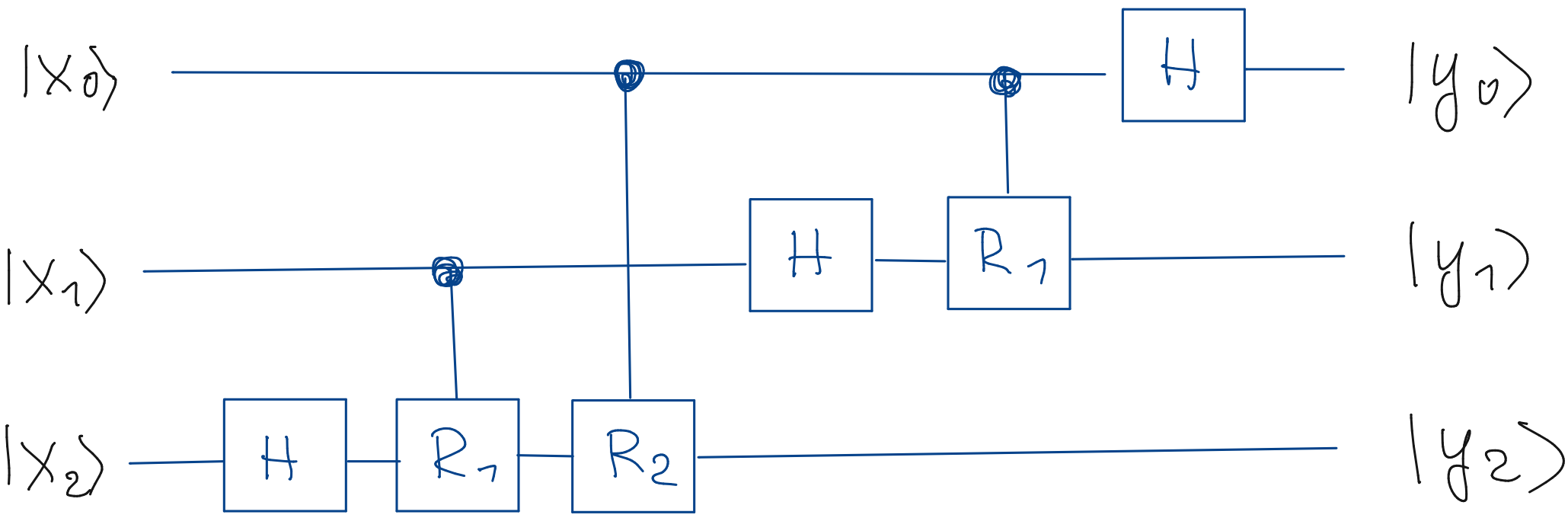
Now, eq. (167) can be efficiently implemented !

example $n=3$

$$x \longrightarrow x_0, x_1, x_2 \longrightarrow |x_0\rangle |x_1\rangle |x_3\rangle$$

binary representation $x_0, x_1, x_2 \in (0,1)$

$$x = x_0 + 2x_1 + 2^2 x_2$$



where

$$H|x_j\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i[x_j]}|1\rangle\right) \tag{169}$$

and

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2^k} \end{pmatrix} \tag{170}$$

i.e.

$$|x_0\rangle|x_1\rangle|x_2\rangle \xrightarrow{H^{(3)}} |x_0\rangle|x_1\rangle\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i[x_2]}|1\rangle\right)$$

$$\xrightarrow{R_1^{(3)}} |x_0\rangle|x_1\rangle\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i[x_2]}e^{i\pi\frac{x_1}{2}}|1\rangle\right)$$

$$\xrightarrow{R_2^{(3)}} |x_0\rangle|x_1\rangle\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\frac{x_2}{2}}e^{i\pi\frac{x_1}{2}}e^{i\pi\frac{x_0}{2^2}}|1\rangle\right)$$

$$(1\Rightarrow 1) \xrightarrow{H^{(2)}} \frac{1}{\sqrt{4}}|x_0\rangle\left(|0\rangle + e^{2\pi i[x_1]}|1\rangle\right)\left(|0\rangle + e^{2\pi i[x_0x_1x_2]}|1\rangle\right)$$

$$\xrightarrow{R_1^{(2)}} \frac{1}{\sqrt{4}}|x_0\rangle\left(|0\rangle + e^{2\pi i[x_0x_1]}|1\rangle\right)\left(|0\rangle + e^{2\pi i[x_0x_1x_2]}|1\rangle\right)$$

$$\xrightarrow{H^{(1)}} \frac{1}{\sqrt{8}}\left(|0\rangle + e^{2\pi i[x_0]}|1\rangle\right)\left(|0\rangle + e^{2\pi i[x_0x_1]}|1\rangle\right)$$

$$\cdot\left(|0\rangle + e^{2\pi i[x_0x_1x_2]}|1\rangle\right)$$

□

I.e. for the QF-Trafo one Hadamard and $n(n-1)/2$ R gates are required per input qubit

> QFTrafo requires $\mathcal{O}((\log N)^2)$ gates!

corollary:

> A Quantum computer can determine the period of a function $f: Z_N \to Z_N$ in
>
> $$\mathcal{O}((\log N)^2)$$
>
> steps, while a classical algorithm needs $\mathcal{O}(N \log N)$ steps

(C) Period finding and factorization into prime numbers

We now discuss how an efficient period-finding algorithm can be used to determine prime factors of large integer numbers

given N: what is $k \neq 1, N$ with

(172) $N = k \cdot r$?

Best known classical sieve

$$\mathcal{O}\left[\exp\left((\log N)^{1/3} (\log \log N)^{2/3}\right)\right]$$

$\Rightarrow$ NP problem (not proven however)

Here we make this a BQP problem

1. choose $a < N$ randomly
2. determine largest common divisor of a and N using e.g. the Euklid method
   $\Rightarrow$ poly($\log N$)
   - If a devisor exist the search is done!
   - With much much higher probability such a devisor does not exist $\Rightarrow$ step (3)
3. If a and N do not have a common divisor then there exists an r such that

(173) $$a^r \equiv 1 \mod N$$ (theorem of Euler)

4 The number r from (173) is the period of the function

(174) $$f_{N,a}(x) = a^x \mod N$$

5 This period can be found efficiently using QFTrafo with effort $O((\log N)^2)$

6 If r from step 5 is even $\Rightarrow$

(175) $$\underbrace{\left(a^{\frac{r}{2}} - 1\right)}_{=\alpha}\underbrace{\left(a^{\frac{r}{2}} + 1\right)}_{=\beta} = a^r - 1 = 0 \mod N$$

i.e.

$\alpha - \beta$ is a multiple of N !

$\Rightarrow$

(176) $$\alpha\beta = mN$$

Now determine largest common divisor of

(α, N) and of (β, N)

e.g. with Euklid algorithm. Either (α, N) or (β, N) must have a common divisor which is a fator of N !

If r from step 5 is odd ⇒ repeat procedure with different a

Determining the integer factors of an integer N can be done using a quantum algorithm in

poly(log(N)) steps

i.e. factorization ∈ BQP

An immediate consequence is that the RSA scheme of cryptography is no longer secure

⇒ quantum cryptography (later)

3.7 Gottesman-Knill theorem

A theorem that highlights how subtle the potential advantage of quantum circuits is, is the following

A quantum circuit that involves state preparation in the computational basis, Hadamard gates, phase gates, CNOT-gates and Pauli gates as well as measurements in the computational basis may be efficiently simulated on a classical machine

proof: later; used in fault-tolerant computation

Shore is not of this type!