Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Theoretical background of Shor's Algorithm

Damian Steiger

Prime factorization of *n*-bit integer:

classically requires $\exp\left(\Theta\left(n^{1/3} log^{2/3} n\right)\right)$

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

Reference: [1]

CONTENT

-Classical part of Shor’s Algorithm

-Quantum Fourier Transform

-Period Finding

-Summary

So far ...

Factoring N

↓

Finding a nontrivial square root of 1 mod N

↓

Finding the period r of the function

$$f(b) = a^b \bmod \mathrm{N}$$

(fixed a and fixed N)

Reference: [2],[4]

Quantum Fourier Transform

$$M = 2^m$$

m qubits

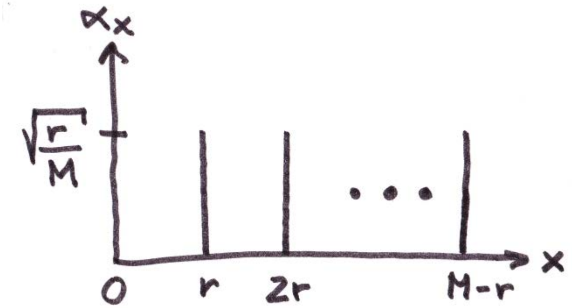
$$QFT_M = \frac{1}{\sqrt{M}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2M-2} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3M-3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{M-1} & \omega^{2M-2} & \omega^{3M-3} & \cdots & \omega^{(M-1)(M-1)} \end{pmatrix} \qquad \omega = e^{\frac{2\pi i}{M}}$$

Example

$$QFT_M\,|0\rangle = QFT_M \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \frac{1}{\sqrt{M}} \sum_{x=i}^{M-1} |x\rangle$$

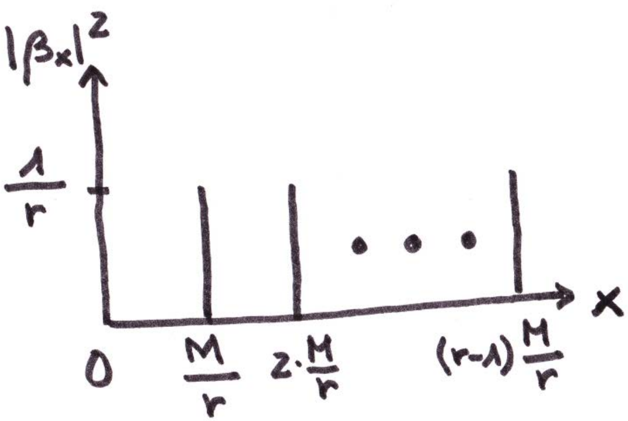
Reference: [4]

Quantum Fourier Transform (suppose $M = 0 \; mod \; r$)



$$\alpha_x = \begin{cases} \sqrt{\frac{r}{M}} & \text{if } x = j \cdot r, \; j \in \mathbb{N} \\ 0 & \text{otherwise} \end{cases}$$

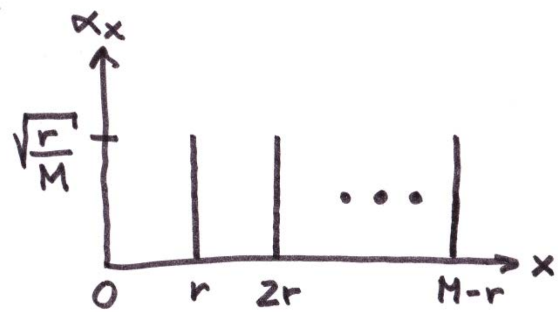
$$QFT_M |\alpha\rangle = |\beta\rangle$$

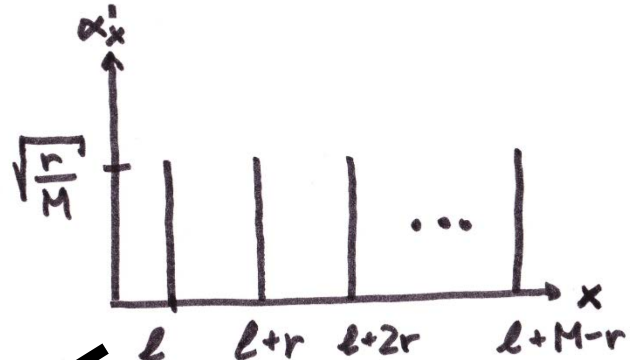


1)
Input has period r
Output has period M/r

Reference: [2],[4]

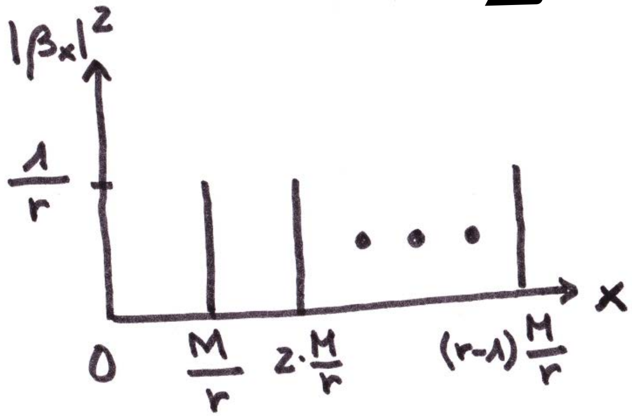
Quantum Fourier Transform (suppose $M = 0 \; mod \; r$)





$QFT_M|\alpha\rangle = |\beta\rangle$

$QFT_M|\alpha'\rangle = |\beta\rangle$

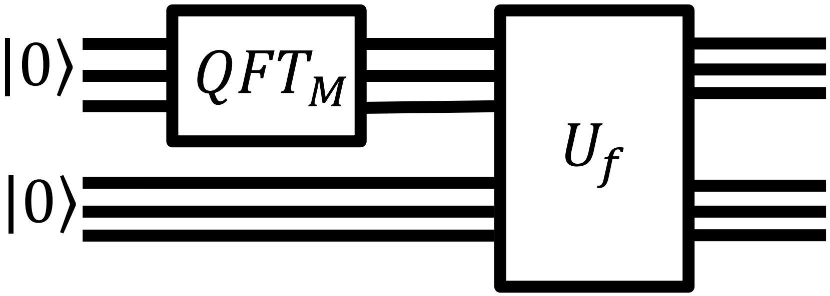


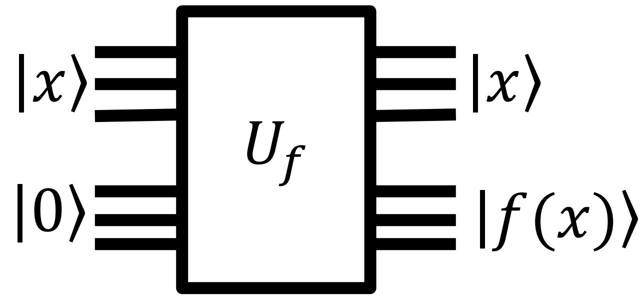
1)
Input has period r
Output has period M/r
2)
$|\beta_x|^2$ doesn't change if input is shifted

Reference: [2],[4]

Period finding

$$f(b) = 2^b \; mod \; 21$$

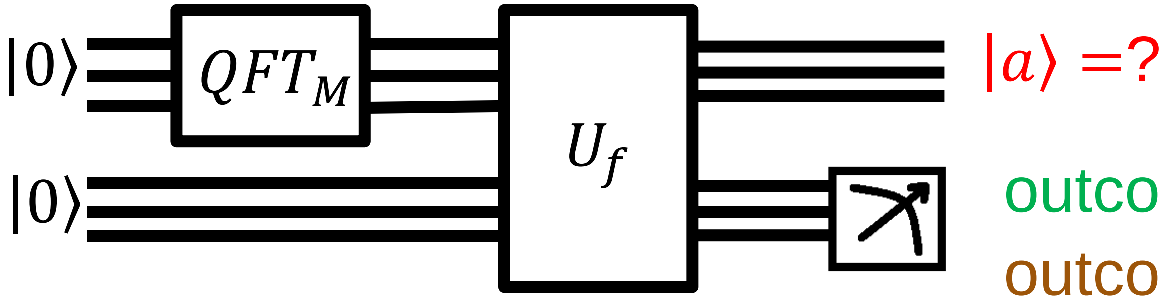




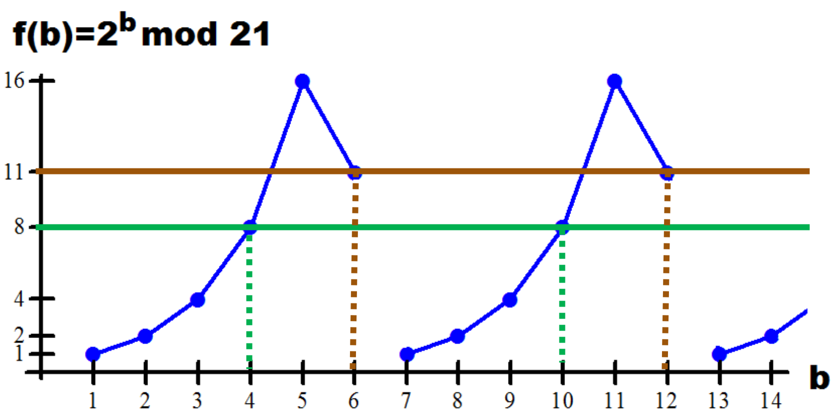
$$|0\rangle|0\rangle \longrightarrow \frac{1}{\sqrt{M}}\sum_{x=0}^{M-1}|x\rangle\,|0\rangle \longrightarrow \frac{1}{\sqrt{M}}\sum_{x=0}^{M-1}|x\rangle\,|f(x)\rangle$$

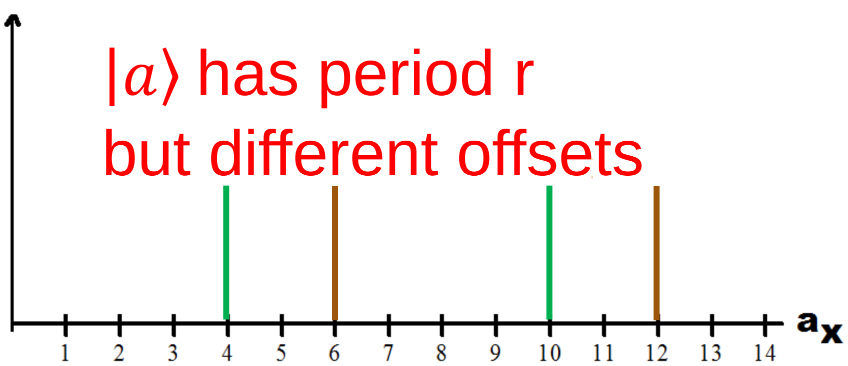
Reference: [2],[4]

Period finding $f(b) = 2^b \; mod \; 21$



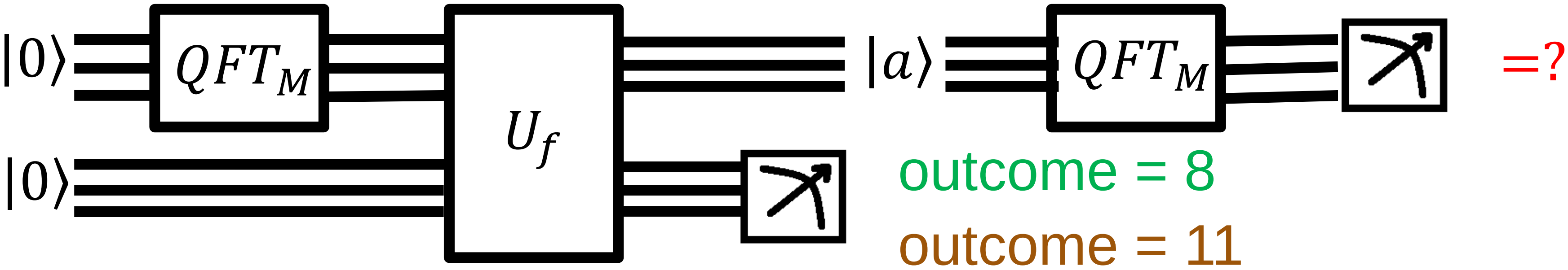
$$|0\rangle|0\rangle \longrightarrow \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle\,|0\rangle \longrightarrow \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle\,|f(x)\rangle$$



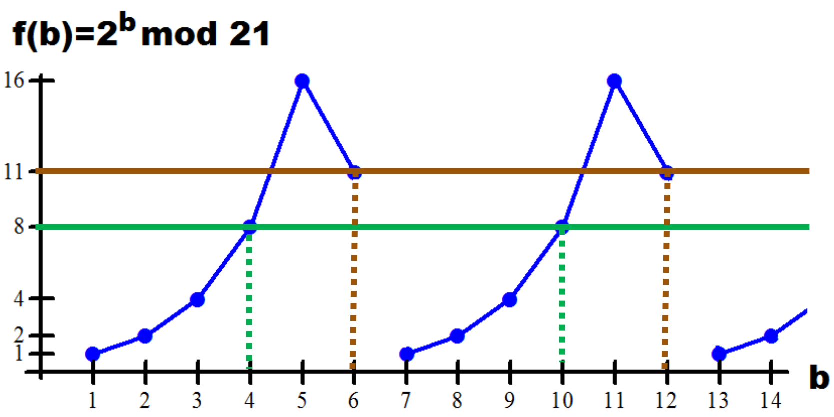


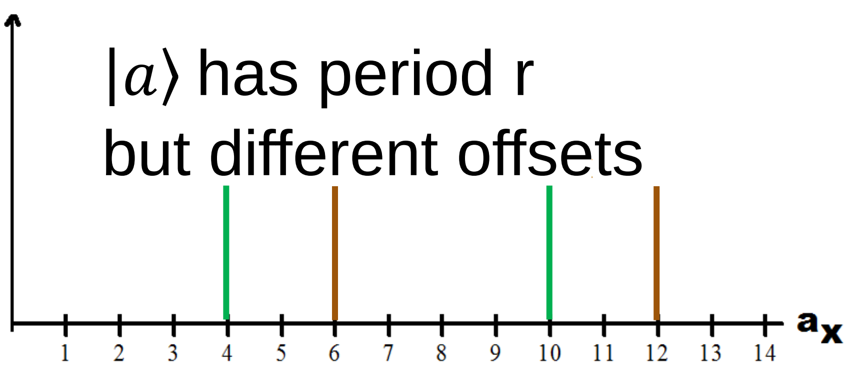
Period finding

$$f(b) = 2^b \; mod \; 21$$

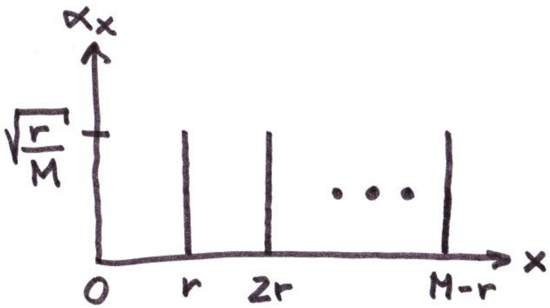


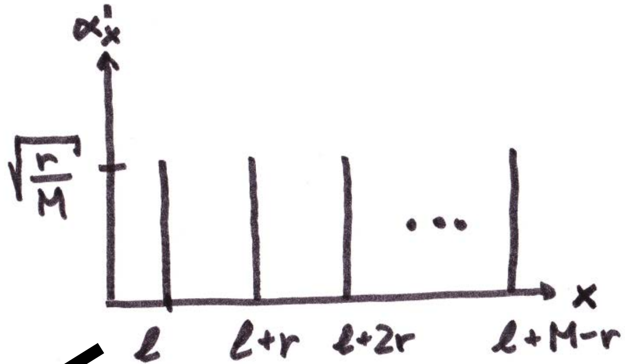
$$|0\rangle|0\rangle \rightarrow \frac{1}{\sqrt{M}}\sum_{x=0}^{M-1}|x\rangle\,|0\rangle \rightarrow \frac{1}{\sqrt{M}}\sum_{x=0}^{M-1}|x\rangle\,|f(x)\rangle$$





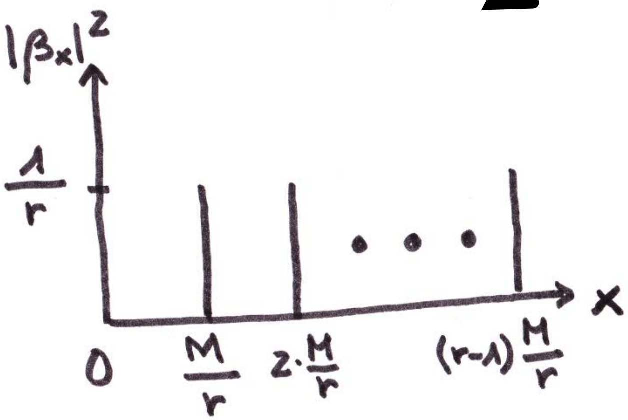
Quantum Fourier Transform (suppose $M = 0 \; mod \; r$)





$QFT_M|\alpha\rangle = |\beta\rangle$

$QFT_M|\alpha'\rangle = |\beta\rangle$

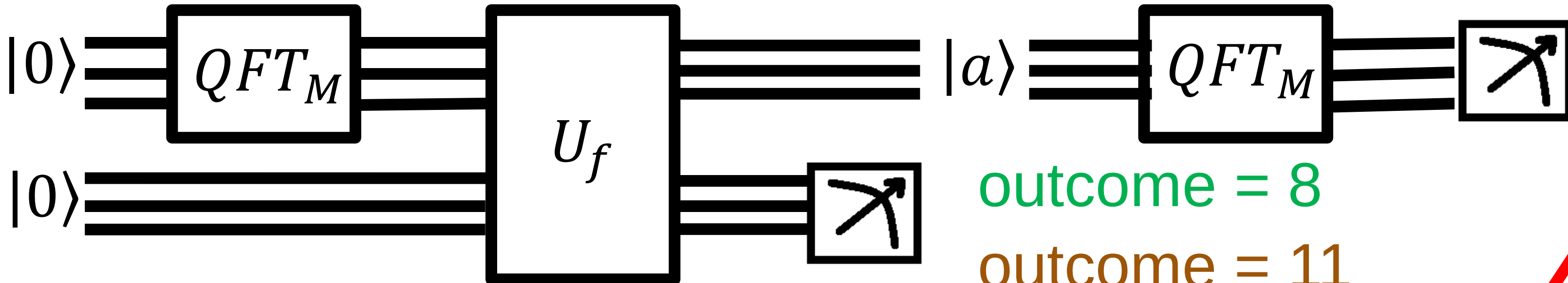


1)
Input has period r
Output has period M/r
2)
$|\beta_x|^2$ doesn't change if input is shifted

Reference: [2],[4]

Period finding

$$f(b) = 2^b \; mod \; 21$$

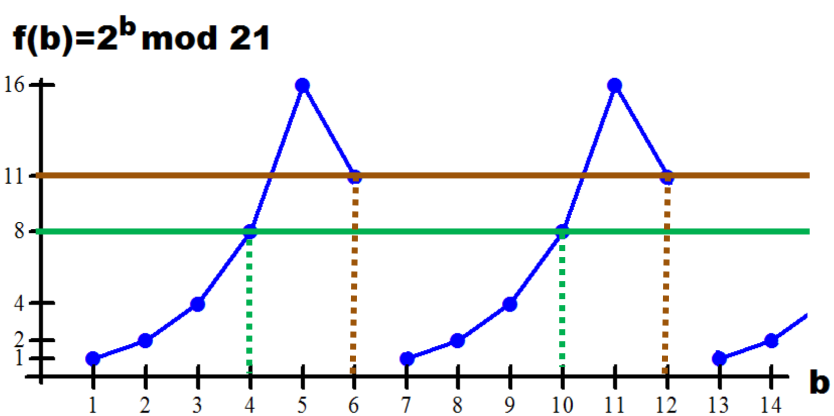


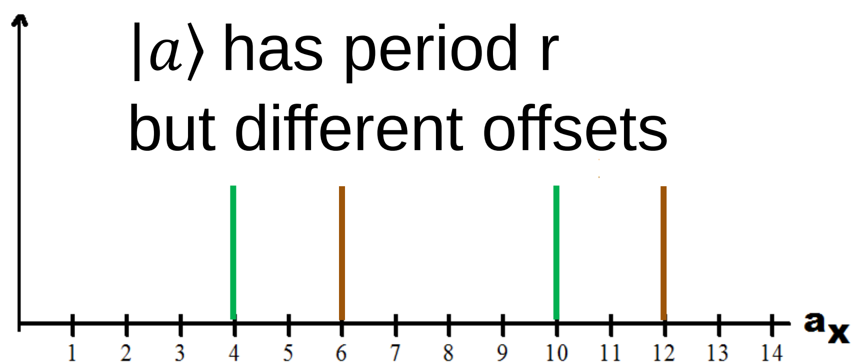
outcome = 8

outcome = 11

$$|0\rangle|0\rangle \rightarrow \frac{1}{\sqrt{M}}\sum_{x=0}^{M-1}|x\rangle|0\rangle \rightarrow \frac{1}{\sqrt{M}}\sum_{x=0}^{M-1}|x\rangle|f(x)\rangle$$

Output:
Multiples of M/r





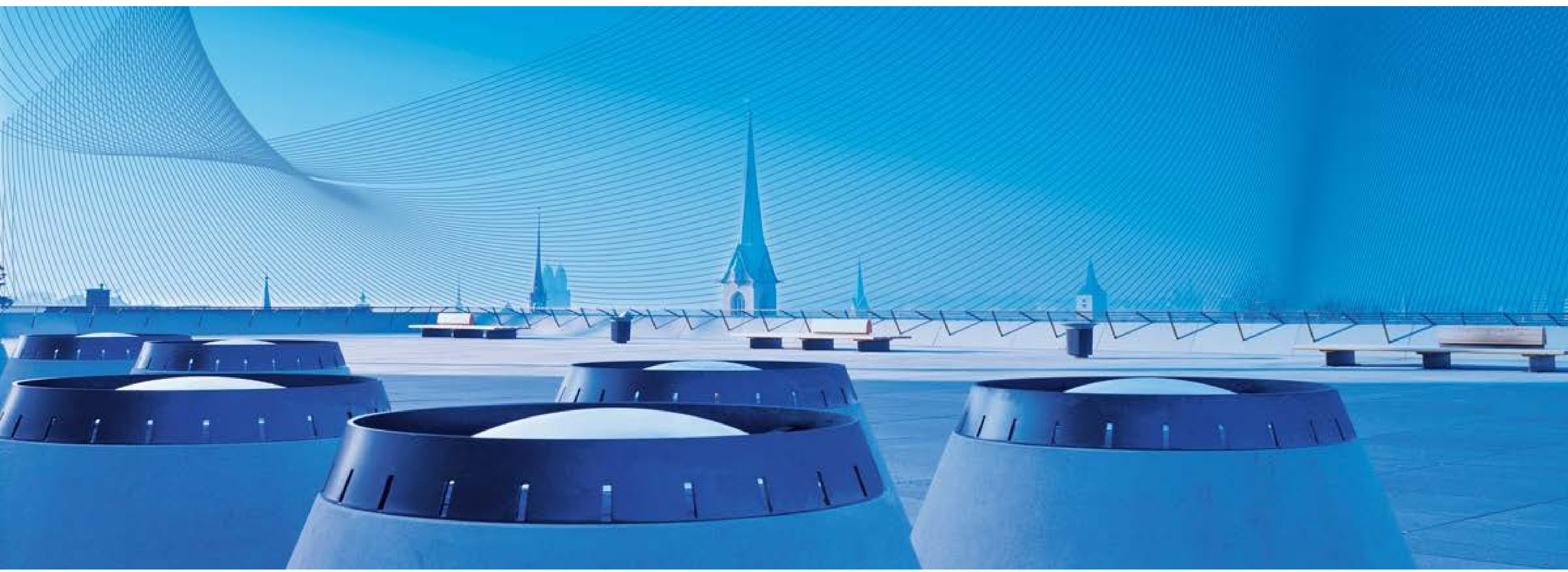
Period finding

- Quantum circuit outputs s random multiples of M/r
  With probability $1 - k/2^s$, gcd of these outputs will be M/r.

- Assumption that M is a multiple of the period r is not necessary. Choose M to be a power of 2 and $M \approx N^2$

Reference: [2]

Thank you for your attention!



Used References

[1] M. A. Nielsen, I.L. Chuang
Quantum Compuation and Quantum Information
See chapt. 5

[2] Dasgupta, Papadimitriou, Vazirani
Algorithms
www.cs.berkeley.edu/~vazirani/algorithms.html
See chapt. 10

[3] Shor Pieter W.
Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.
arXiv:quant-ph/9508027 (1995)

[4] U. Vazirani
CS191x Quantum Mechanics and Quantum Computation
www.edx.org (spring 2013)