EURO^2

Basic Quantum Computing Algorithms and Their Implementation in Qiskit

Jiří Tomčala

IT4Innovations,
VŠB - Technical University of Ostrava

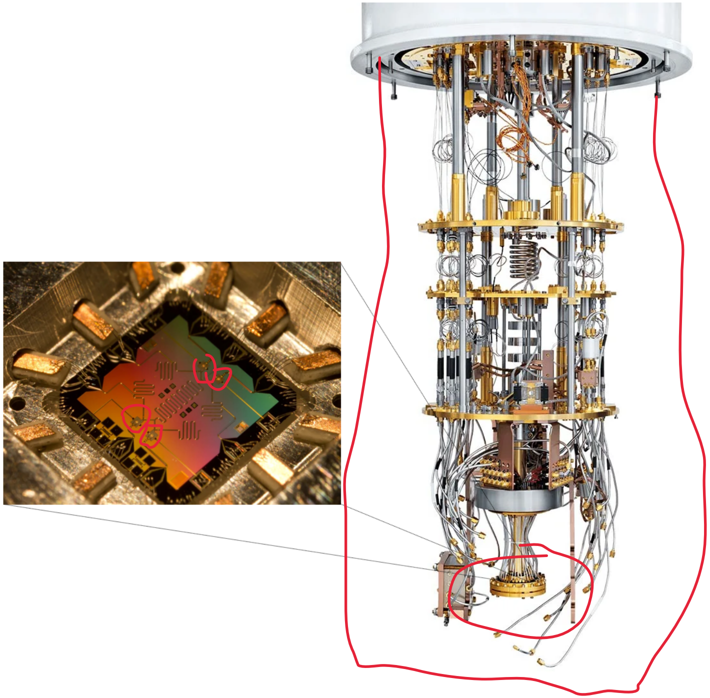
3 – 5 April 2023

Part I

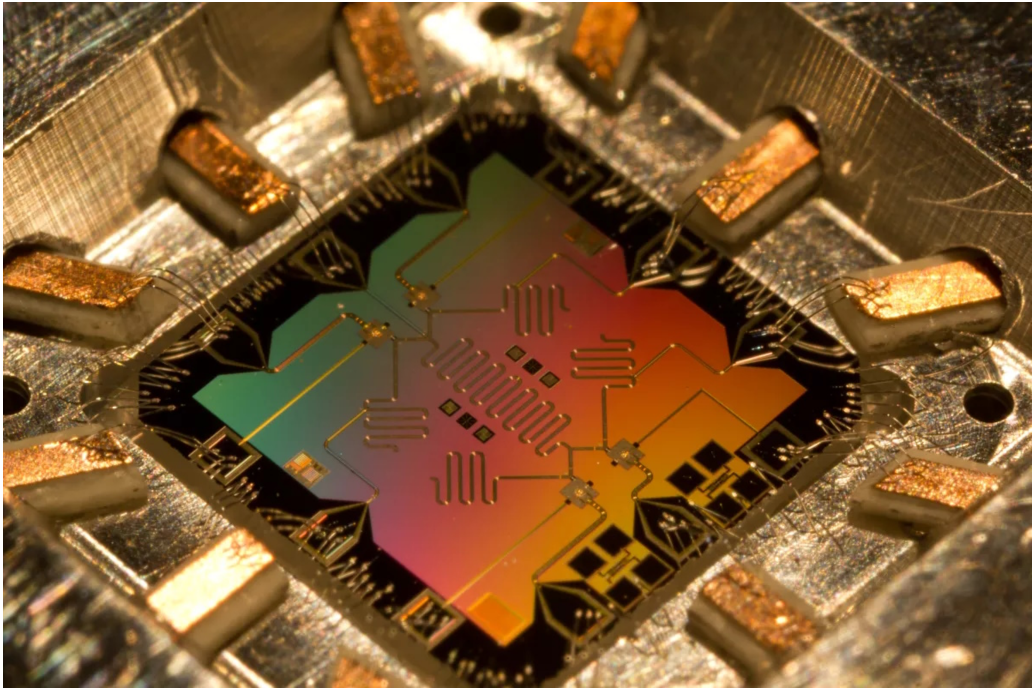
Introduction to Quantum Computing

Hardware

Superconducting technology:

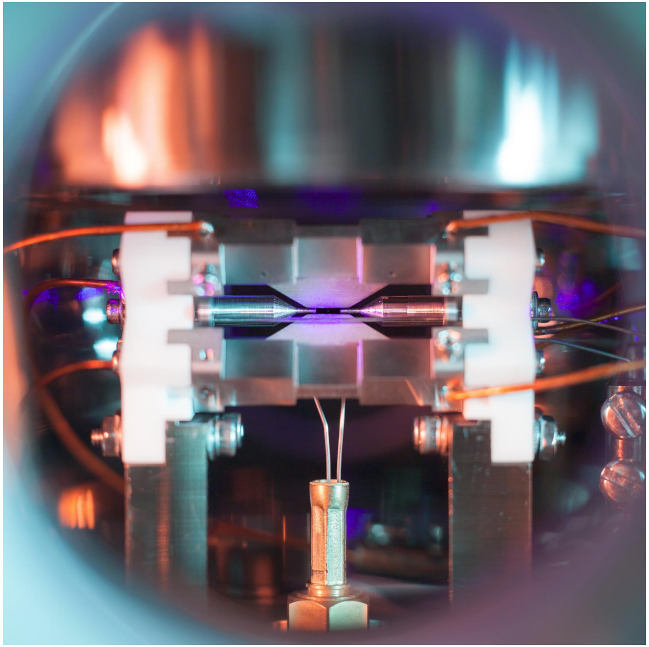


Hardware

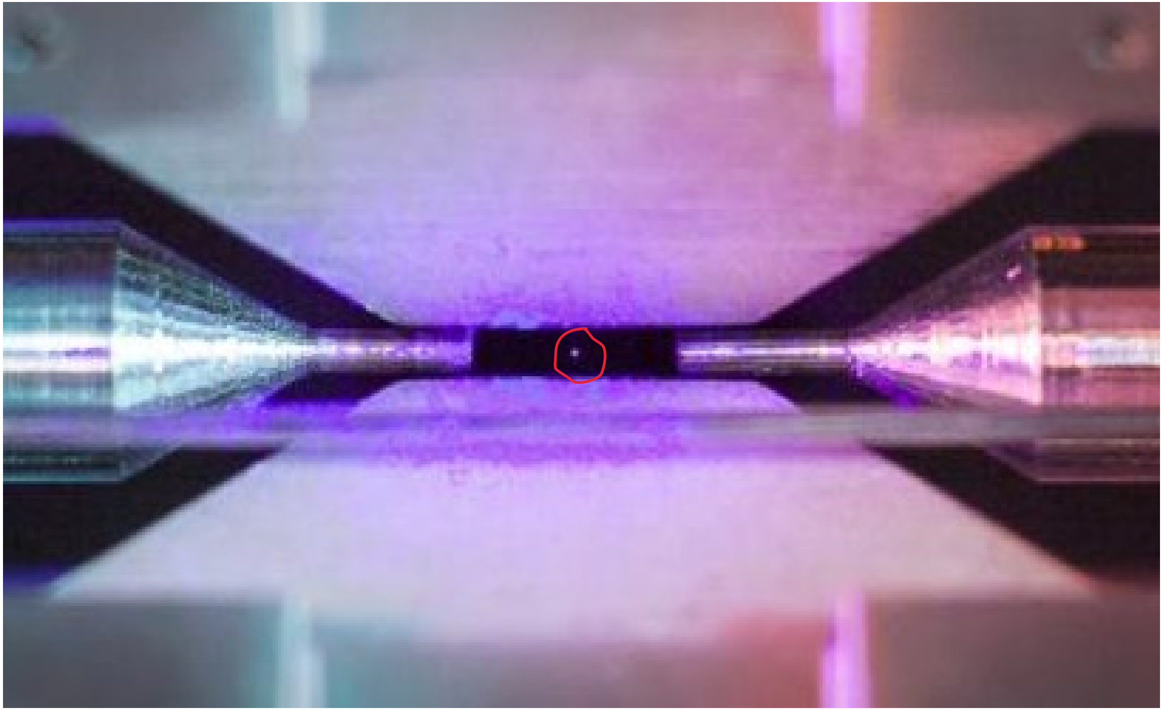


Hardware

Trapped-ion technology:



Hardware



Qubit

ϕ ... PHASE

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$$

$$\alpha = \cos\frac{\theta}{2}$$

$$\beta = e^{i\phi}\sin\frac{\theta}{2} = (\cos\phi + i\sin\phi)\sin\frac{\theta}{2}$$

$$\Pr(|0\rangle) = |\alpha|^2 = \cos^2\frac{\theta}{2}$$

$$\Pr(|1\rangle) = |\beta|^2 = |e^{i\phi}|^2\sin^2\frac{\theta}{2} = \sin^2\frac{\theta}{2}$$

$$\Pr(|0\rangle) + \Pr(|1\rangle) = \cos^2\frac{\theta}{2} + \sin^2\frac{\theta}{2} = 1$$

Z

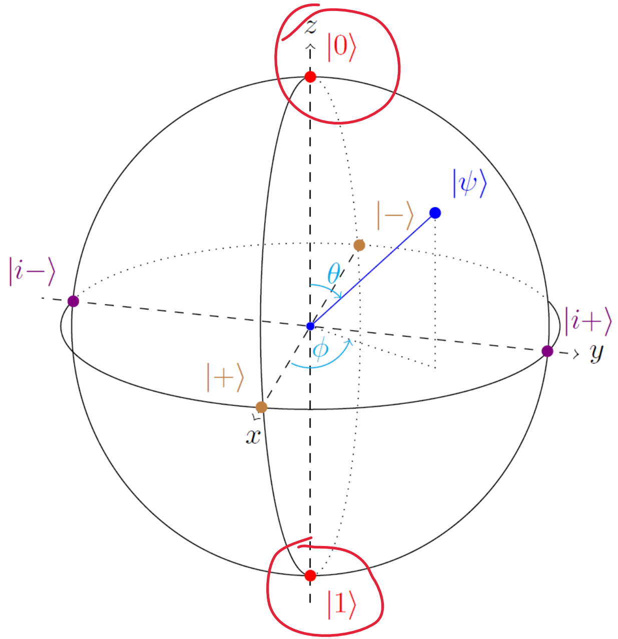


Figure. Bloch sphere.

Qubit

$$\alpha = \frac{1}{\sqrt{2}} \rightarrow |\alpha|^2 = \frac{1}{2}$$

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

$$\alpha = \cos\frac{\theta}{2}$$

$$\beta = e^{i\phi}\sin\frac{\theta}{2} = (\cos\phi + i\sin\phi)\sin\frac{\theta}{2}$$

$$|+\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle$$

$$|-\rangle = \frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle$$

$$|i+\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + i\frac{1}{\sqrt{2}}\,|1\rangle$$

$$|i-\rangle = \frac{1}{\sqrt{2}}\,|0\rangle - i\frac{1}{\sqrt{2}}\,|1\rangle$$

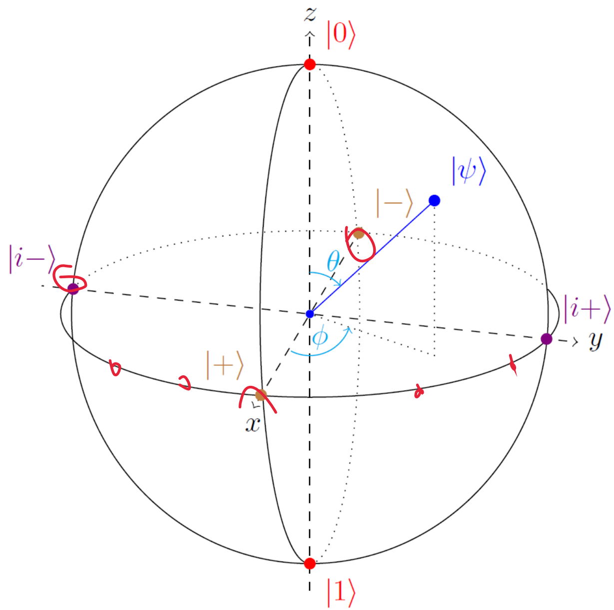


Figure. Bloch sphere.

X = NOT

H = HADAMARD

1-qubit quantum gates

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

GATE

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \left[|0\rangle\;|1\rangle\right]\begin{bmatrix}\alpha\\ \beta\end{bmatrix} \Rightarrow \begin{bmatrix}\alpha\\ \beta\end{bmatrix}$$

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \qquad |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$$

$$X\,|\psi\rangle = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \begin{bmatrix}\beta\\ \alpha\end{bmatrix}$$

$$H\,|\psi\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}\alpha+\beta\\ \alpha-\beta\end{bmatrix}$$

$$H\,|0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ 1\end{bmatrix} = |+\rangle$$

$$H\,|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ -1\end{bmatrix} = |-\rangle$$

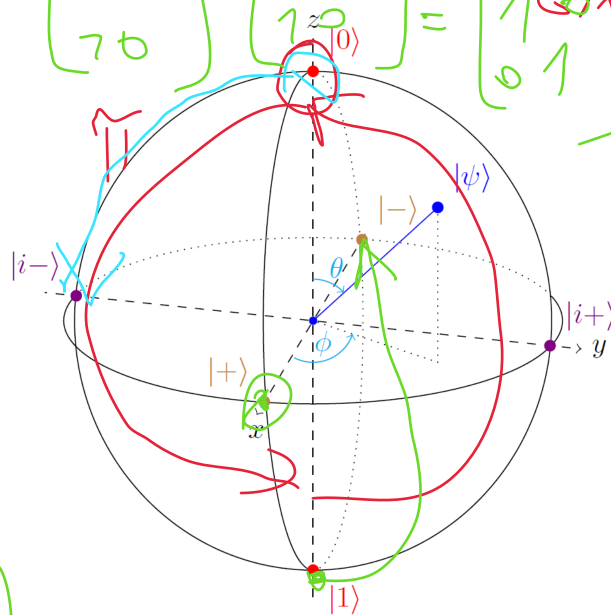


Figure. Bloch sphere.

1-QUBIT QUANTUM GATES

$P(\pi) = Z$ $\quad$ $P\left(\frac{\pi}{4}\right) = T$

$P\left(\frac{\pi}{2}\right) = S$

$$P(\lambda)\left|\psi\right\rangle = \begin{bmatrix}1 & 0\\ 0 & e^{i\lambda}\end{bmatrix}\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \begin{bmatrix}\alpha\\ e^{i\lambda}\beta\end{bmatrix}$$

$$Z\left|\psi\right\rangle = \begin{bmatrix}1 & 0\\ 0 & e^{i\pi}\end{bmatrix}\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \begin{bmatrix}\alpha\\ -\beta\end{bmatrix}$$

$$S\left|\psi\right\rangle = \begin{bmatrix}1 & 0\\ 0 & e^{i\frac{\pi}{2}}\end{bmatrix}\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \begin{bmatrix}\alpha\\ i\beta\end{bmatrix}$$

$$T\left|\psi\right\rangle = \begin{bmatrix}1 & 0\\ 0 & e^{i\frac{\pi}{4}}\end{bmatrix}\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \begin{bmatrix}\alpha\\ e^{i\frac{\pi}{4}}\beta\end{bmatrix} = \begin{bmatrix}\alpha\\ \frac{1}{\sqrt{2}}(1+i)\beta\end{bmatrix}$$

$Z\left|+\right\rangle = \left|-\right\rangle \quad Z\left|-\right\rangle = \left|+\right\rangle \quad S\left|+\right\rangle = \left|i+\right\rangle$

$Z\left|i-\right\rangle = S|S\left|i-\right\rangle = T|T|T|T\left|i-\right\rangle = \left|i+\right\rangle$

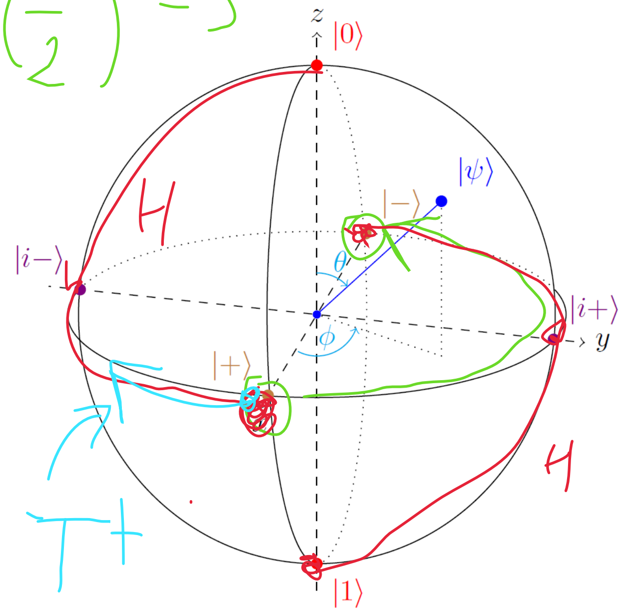
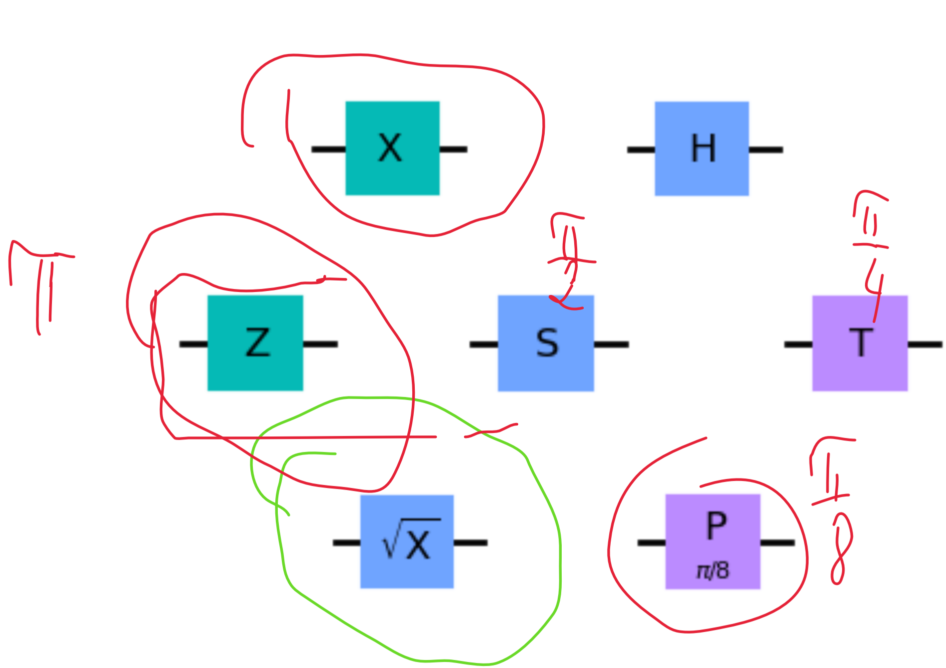


Figure. Bloch sphere.

Implementation in Qiskit



$S^{\dagger}: \; -\frac{\pi}{2}$

$T^{\dagger}: \; -\frac{\pi}{4}$

2-QUBIT QUANTUM GATES

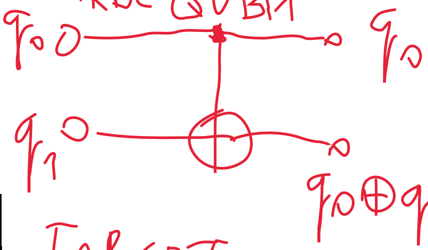
$$\Pr(|00\rangle) = |\alpha_{00}|^2$$

q_1	q_0	q_1
0	0	0
0	1	1
1	0	1
1	1	0

$$|\psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle = \big[|00\rangle\ |01\rangle\ |10\rangle\ |11\rangle\big] \begin{bmatrix}\alpha_{00}\\ \alpha_{01}\\ \alpha_{10}\\ \alpha_{11}\end{bmatrix} \Rightarrow \begin{bmatrix}\alpha_{00}\\ \alpha_{01}\\ \alpha_{10}\\ \alpha_{11}\end{bmatrix}$$

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

CONTROL QUBIT



TARGET

$$\text{CNOT} = \boxed{CX}\,|\psi\rangle = \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}\begin{bmatrix}\alpha_{00}\\ \alpha_{01}\\ \alpha_{10}\\ \alpha_{11}\end{bmatrix} = \begin{bmatrix}\alpha_{00}\\ \alpha_{01}\\ \alpha_{11}\\ \alpha_{10}\end{bmatrix}$$

$$CP(\lambda)\,|\psi\rangle = \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&e^{i\lambda}\end{bmatrix}\begin{bmatrix}\alpha_{00}\\ \alpha_{01}\\ \alpha_{10}\\ \alpha_{11}\end{bmatrix} = \begin{bmatrix}\alpha_{00}\\ \alpha_{01}\\ \alpha_{10}\\ e^{i\lambda}\alpha_{11}\end{bmatrix}$$

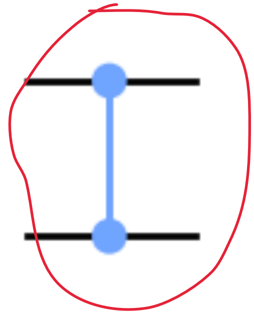
$$SWAP\,|\psi\rangle = \begin{bmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{bmatrix}\begin{bmatrix}\alpha_{00}\\ \alpha_{01}\\ \alpha_{10}\\ \alpha_{11}\end{bmatrix} = \begin{bmatrix}\alpha_{00}\\ \alpha_{10}\\ \alpha_{01}\\ \alpha_{11}\end{bmatrix}$$

Implementation in Qiskit

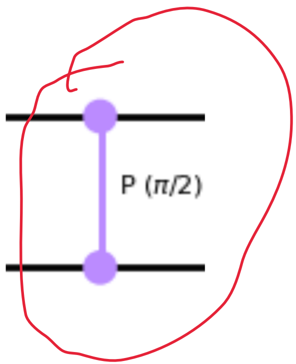
$CZ = CP(\pi)$

CX

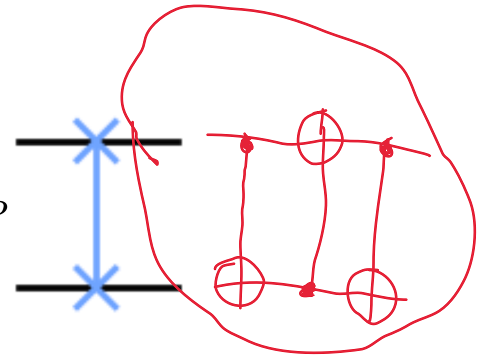
CZ



$CP(\pi/2)$



$SWAP$



Part II

Quantum entanglement

Bell states $= EPR$

$50\% \; |00\rangle$

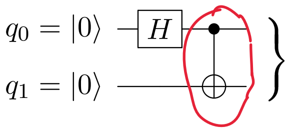
$50\% \; |11\rangle$

$|00\rangle = |0\rangle \otimes |0\rangle$

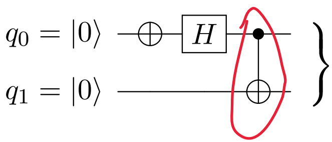
$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$

$\alpha_{00} = \frac{1}{\sqrt{2}} \quad \alpha_{10} = 0$

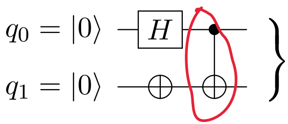
$\alpha_{11} = \frac{1}{\sqrt{2}} \quad \alpha_{01} = 0$



$$|\psi_e\rangle = \boxed{CX}\,\boxed{H}\,|00\rangle = CX\left(\tfrac{1}{\sqrt{2}}\,|00\rangle + \tfrac{1}{\sqrt{2}}\,|01\rangle\right) = \tfrac{1}{\sqrt{2}}\,|00\rangle + \tfrac{1}{\sqrt{2}}\,|11\rangle = |\Phi^+\rangle$$

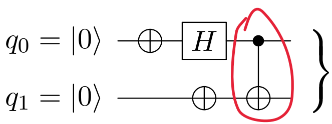


$$|\psi_e\rangle = CX|H\,|00\rangle = CX\left(\tfrac{1}{\sqrt{2}}\,|00\rangle - \tfrac{1}{\sqrt{2}}\,|01\rangle\right) = \tfrac{1}{\sqrt{2}}\,|00\rangle - \tfrac{1}{\sqrt{2}}\,|11\rangle = |\Phi^-\rangle$$



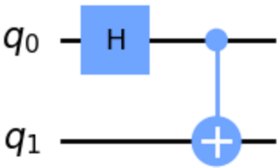
$$|\psi_e\rangle = CX|H\,|00\rangle = CX\left(\tfrac{1}{\sqrt{2}}\,|10\rangle + \tfrac{1}{\sqrt{2}}\,|11\rangle\right) = \tfrac{1}{\sqrt{2}}\,|10\rangle + \tfrac{1}{\sqrt{2}}\,|01\rangle = |\Psi^+\rangle$$

$|\psi^-\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$

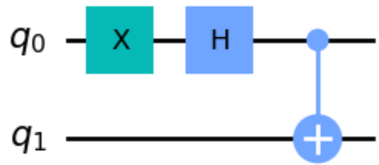


$$|\psi_e\rangle = CX|H\,|00\rangle = CX\left(\tfrac{1}{\sqrt{2}}\,|10\rangle - \tfrac{1}{\sqrt{2}}\,|11\rangle\right) = \tfrac{1}{\sqrt{2}}\,|10\rangle - \tfrac{1}{\sqrt{2}}\,|01\rangle = -|\Psi^-\rangle$$

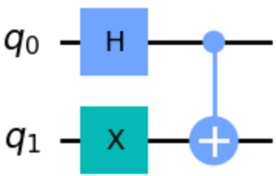
Implementation in Qiskit



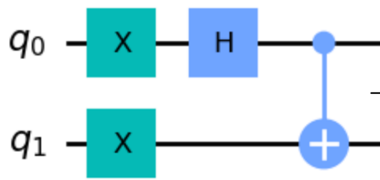
$|\Phi^+\rangle$



$|\Phi^-\rangle$



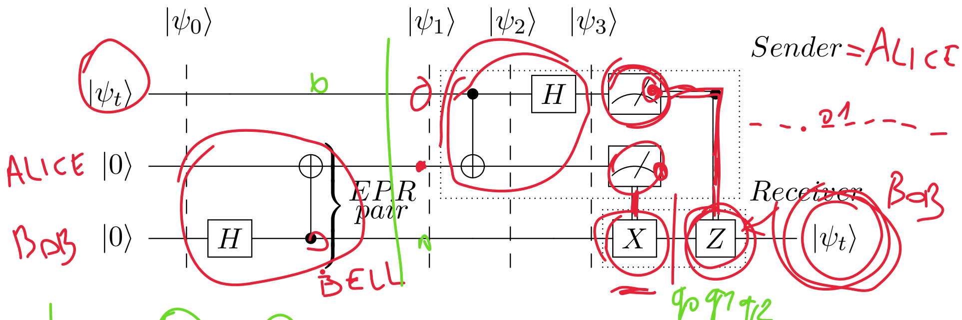
$|\Psi^+\rangle$



$-|\Psi^-\rangle$

Part III

Quantum teleportation



$$|\psi_t\rangle = \alpha_t |0\rangle + \beta_t |1\rangle \quad |\psi_0\rangle = |\psi_t\rangle \otimes |00\rangle = \alpha_t |000\rangle + \beta_t |100\rangle$$

$$|\psi_1\rangle = \frac{\alpha_t}{\sqrt{2}} |000\rangle + \frac{\alpha_t}{\sqrt{2}} |011\rangle + \frac{\beta_t}{\sqrt{2}} |100\rangle + \frac{\beta_t}{\sqrt{2}} |111\rangle$$

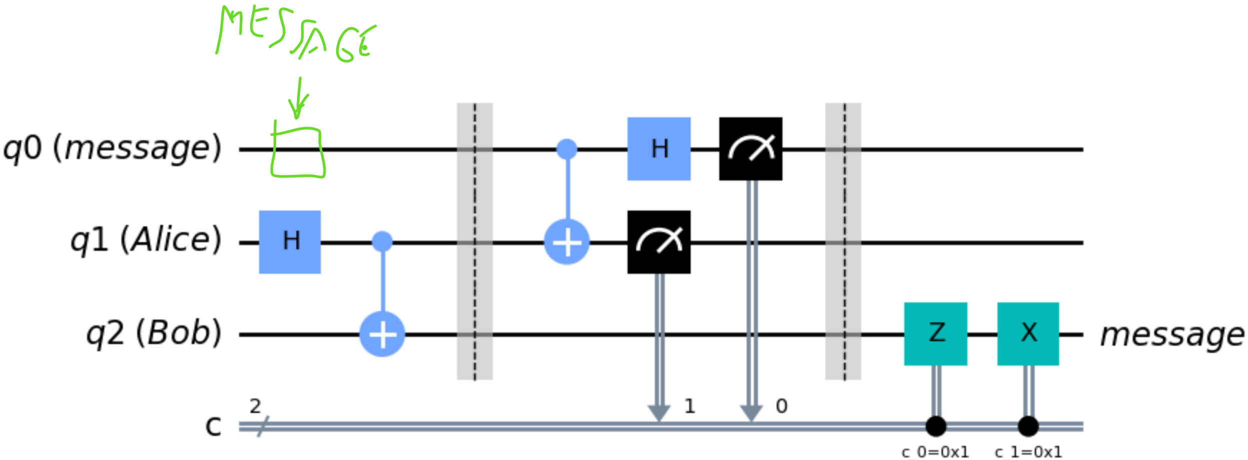
$$|\psi_2\rangle = \frac{\alpha_t}{\sqrt{2}} |000\rangle + \frac{\alpha_t}{\sqrt{2}} |011\rangle + \frac{\beta_t}{\sqrt{2}} |110\rangle + \frac{\beta_t}{\sqrt{2}} |101\rangle$$

$$|\psi_3\rangle = \frac{1}{2} |00\rangle \otimes (\alpha_t |0\rangle + \beta_t |1\rangle) + \frac{1}{2} |01\rangle \otimes (\alpha_t |1\rangle + \beta_t |0\rangle) +$$

$$+ \frac{1}{2} |10\rangle \otimes (\alpha_t |0\rangle - \beta_t |1\rangle) + \frac{1}{2} |11\rangle \otimes (\alpha_t |1\rangle - \beta_t |0\rangle) =$$

$$= \frac{1}{2} |00\rangle \otimes |\psi_t\rangle + \frac{1}{2} |01\rangle \otimes \left|\overline{\psi_t}\right\rangle + \frac{1}{2} |10\rangle \otimes \left|\psi_t^\dagger\right\rangle + \frac{1}{2} |11\rangle \otimes \left|\overline{\psi_t^\dagger}\right\rangle$$

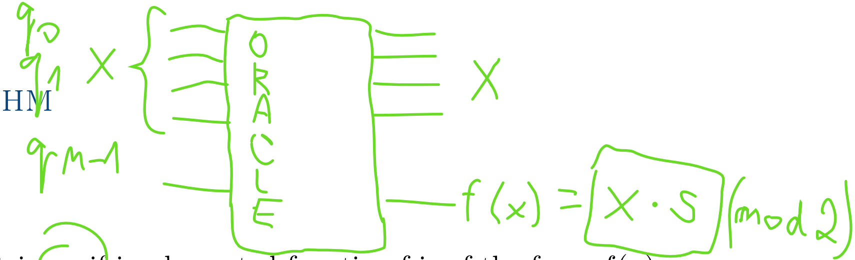
Implementation in Qiskit



Part IV

Bernstein-Vazirani + Deutch-Jozsa algorithm

Bernstein-Vazirani algorithm



$x\cdot s = x_0 s_0 \oplus x_1 s_1 \oplus x_2 s_2 \oplus$
(mod 2)

The problem statement: Find the secret string s if implemented function f is of the form $f(x) = x\cdot s$.

$$|0\rangle^n \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \xrightarrow{f} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle$$

$$\xrightarrow{H^{\otimes n}} \frac{1}{2^n} \sum_{y\in\{0,1\}^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)+x\cdot y} |y\rangle = |s\rangle$$

$n=4$

$$f(x)+x\cdot y = x\cdot s + x\cdot y = x\cdot(s\oplus y) = \begin{cases} 0 & (s=y) \\ 0,1,0,1\ldots & (s\neq y) \end{cases}$$

1 2 3 4

0001 0010 0100 1000 $= X$

$\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$

s_0 s_1 s_2 s_3 $= S = S_3 S_2 S_1 S_0$

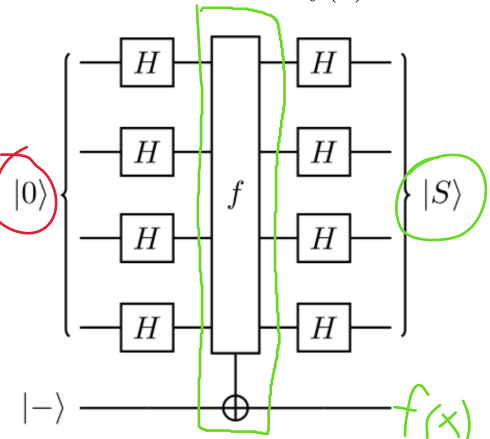
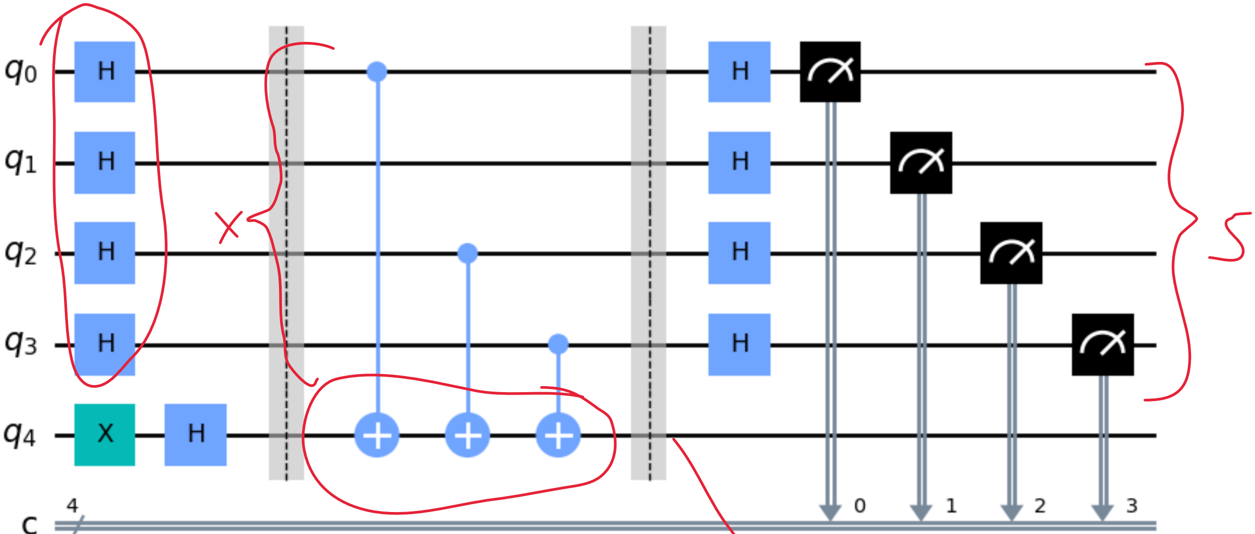


Figure. Bernstein-Vazirani circuit.

Implementation in Qiskit

$s_3 s_2 s_1 s_0$

ORACLE



x

s

$f(x) = x \cdot s$

Deutch-Jozsa algorithm

0000 | CONST. | BALANCED
0001 | 0 1 | 0
0010 | 0 1 | 1
⋮ | 0 1 | 0
 | 0 1 | 1
 | ⋮ | 0

$$\frac{2^n}{2}+1 = \underbrace{2^{n-1}+1}$$

<u>The problem statement:</u> Decide whether the implemented function f is constant or balanced.

$$|0\rangle^n \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle \xrightarrow{f} \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|x\rangle$$

$$\xrightarrow{H^{\otimes n}} \frac{1}{2^n}\sum_{y\in\{0,1\}^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)+x\cdot y}|y\rangle = |s\rangle$$

$$|s\rangle \begin{cases} = 0 \rightarrow \boxed{f \text{ is constant}} \\ \neq 0 \rightarrow f \text{ is balanced} \end{cases}$$

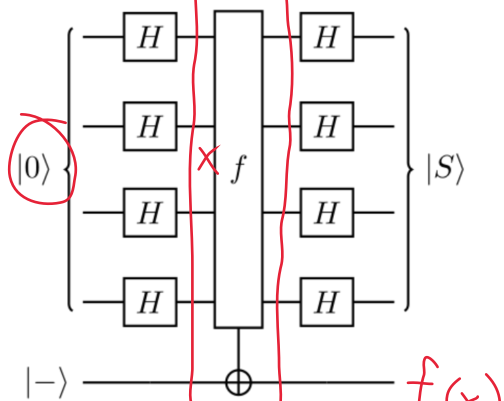
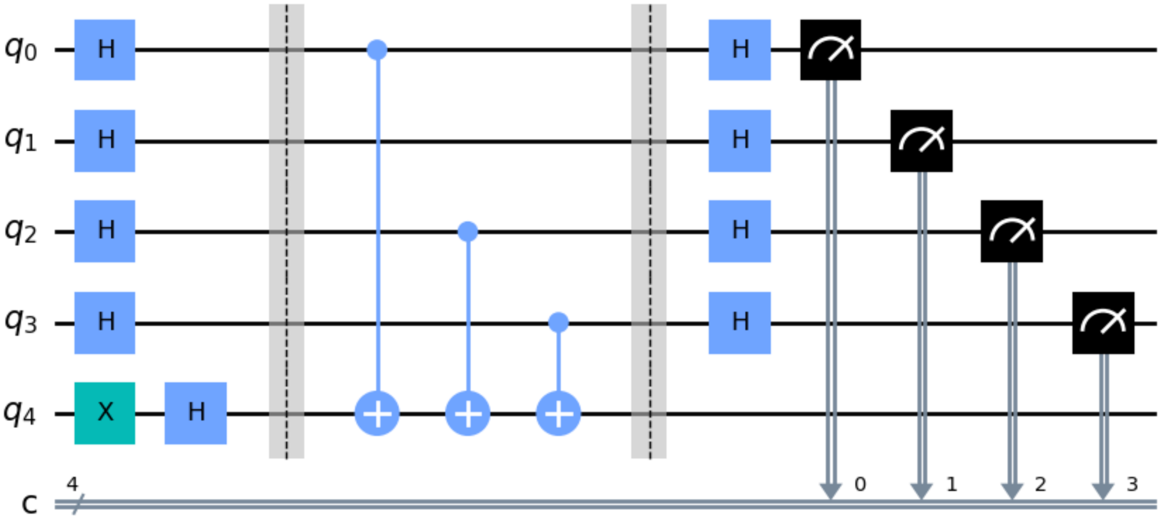


Figure. Deutch-Jozsa circuit.

$$\frac{1}{4}\left(|0000\rangle + |0001\rangle + \quad + |1111\rangle\right)$$

Implementation in Qiskit



Part V

Simon's algorithm

Simon's algorithm

$f : \{0,1\}^n \to \{0,1\}^n$

x		$f(x)$
0000	$\to$	1111
0001	$\to$	1110
=		
1111	$\to$	0000

The problem statement: Decide whether the implemented function f is periodic or not.

$$
|0\rangle^{\otimes n}|0\rangle^{\otimes n} \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|0\rangle^{\otimes n}
$$

$$
\xrightarrow{U_f} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|f(x)\rangle
$$

$$
\xrightarrow{H^{\otimes n}} \frac{1}{2^n} \sum_{y\in\{0,1\}^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y}|y\rangle|f(x)\rangle
$$

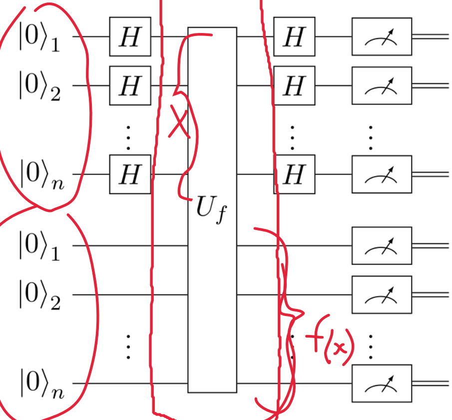


Figure. Simon's circuit.

ORACLE

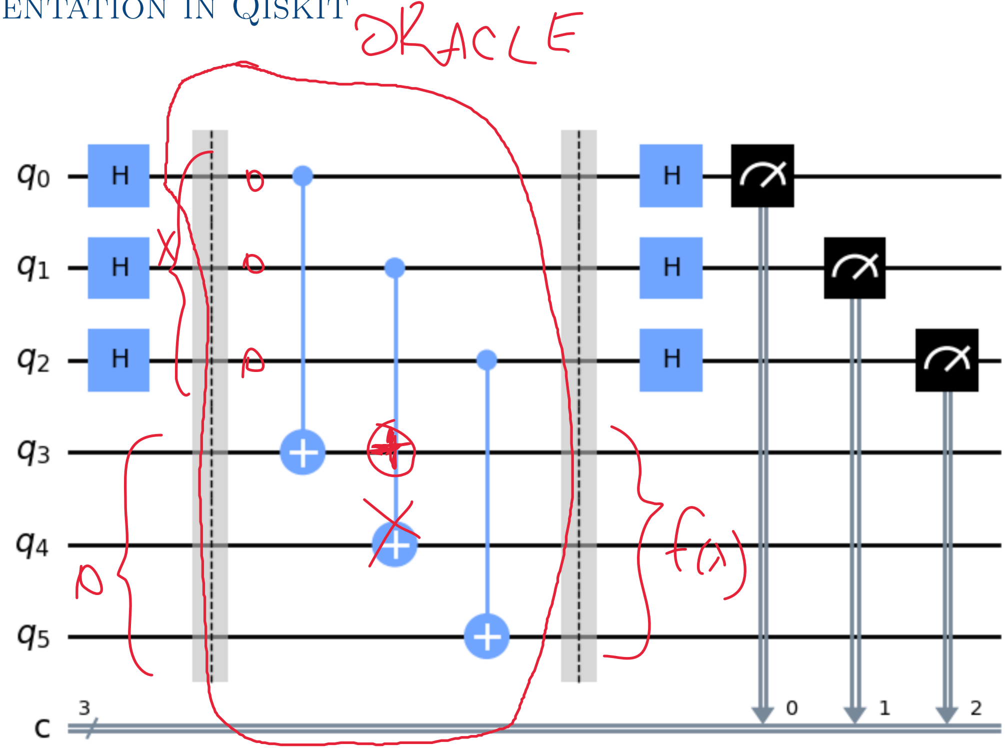
Quantum state after measuring the lower register:

$$
f \text{ is not periodic} \to \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{x_1\cdot y}|y\rangle|f(x_1)\rangle
$$

$$
f \text{ is periodic} \to \frac{1}{\sqrt{2^{n+1+\dots}}} \sum_{y\in\{0,1\}^n} \left[(-1)^{x_1\cdot y} + (-1)^{x_2\cdot y} + \dots\right]|y\rangle|f(x_1)\rangle
$$

$f(x_1) = f(x_2)$

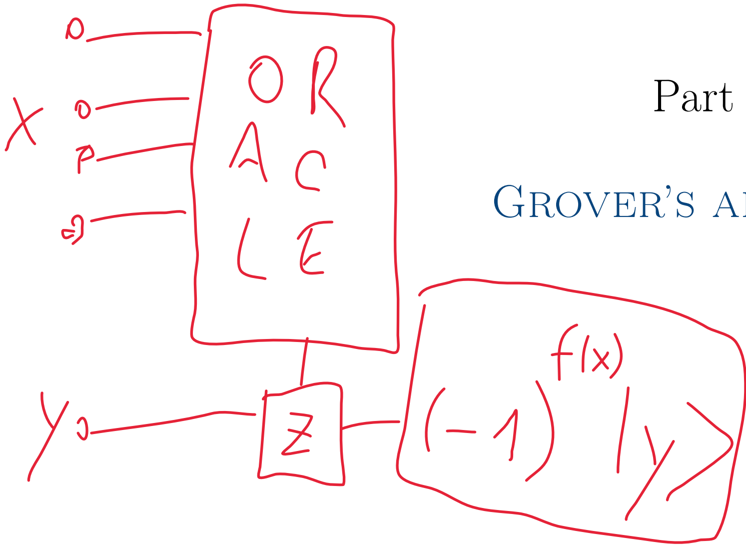
Implementation in Qiskit



Part VI

Grover's algorithm

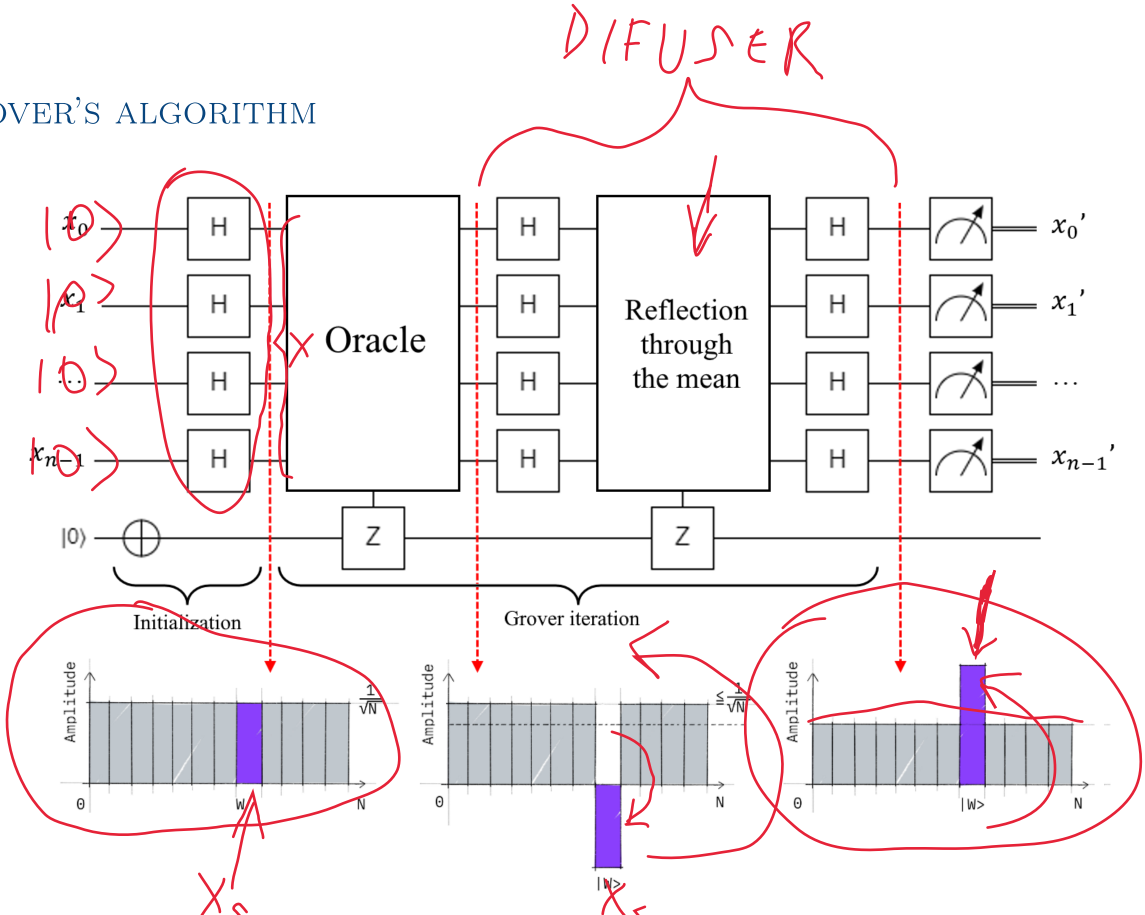
$$f(x) = \begin{cases} 0 & x \neq x_s \\ 1 & x = x_s \end{cases}$$



$$f(x_s) = 1 \Rightarrow x_s = ?$$

$$f(x) = 0 \Rightarrow x \neq x_s$$

Grover's algorithm

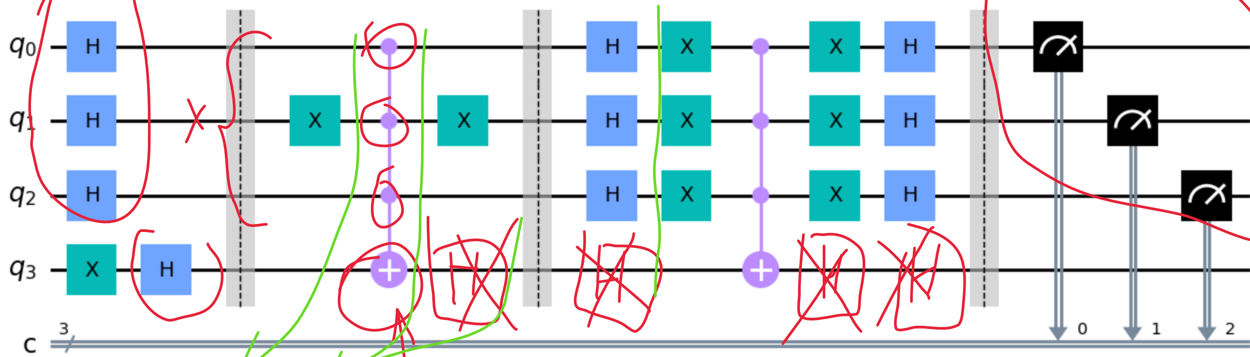


Implementation in Qiskit

$Z = HXH$

ORACLE

DIFUSER



$x_s = |101\rangle$

$|\psi\rangle = \frac{1}{\sqrt{8}}\left(|000\rangle + |001\rangle + \dots - |101\rangle + |110\rangle + |111\rangle\right)$

Part VII

Quantum Fourier transform

Quantum Fourier transform

$N = 2^n$

n - qubits

$$\text{IDFT: } x_n = \frac{1}{N}\sum_{k=0}^{N-1} X_k \cdot e^{2\pi i \frac{kn}{N}}$$

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

$$\frac{y}{N} = \frac{y_1 y_2 \dots y_n}{2^n} = \sum_{k=1}^{n}\frac{y_k}{2^k} \longrightarrow \quad \text{QFT}\,|x\rangle = \frac{1}{\sqrt{N}}\sum_{y=0}^{N-1} e^{2\pi i x \sum_{k=1}^{n}\frac{y_k}{2^k}}\,|y_1 y_2 \dots y_n\rangle$$

$$\text{QFT}\,|x\rangle = \frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}\prod_{k=1}^{2^n} e^{2\pi i x \frac{y_k}{2^k}}\,|y_1 y_2 \dots y_n\rangle$$

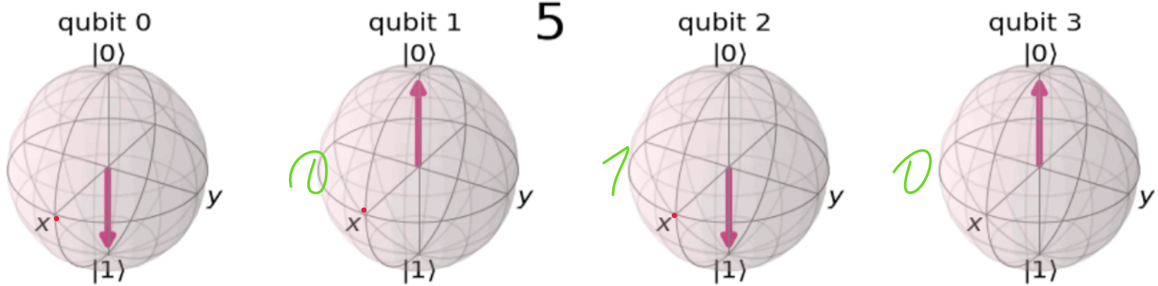
$$\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots$$

$$\text{QFT}\,|x\rangle = \frac{1}{\sqrt{2^n}}\Big(|0\rangle + e^{i\pi x}\,|1\rangle\Big) \otimes \Big(|0\rangle + e^{i\frac{\pi}{2}x}\,|1\rangle\Big) \otimes \Big(|0\rangle + e^{i\frac{\pi}{4}x}\,|1\rangle\Big) \otimes \cdots\cdots \otimes \Big(|0\rangle + e^{i\frac{\pi}{2^{n-1}}x}\,|1\rangle\Big)$$

π $\quad \frac{\pi}{2}$ $\quad \frac{\pi}{4}$

Quantum Fourier transform

q_3 q_2 q_1 q_0
0 1 0 1

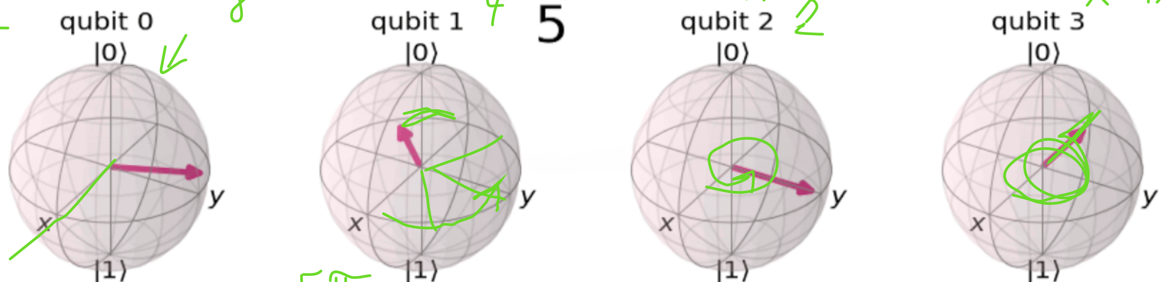


5

$5 \cdot \frac{\pi}{8}$ $x \cdot \frac{\pi}{4}$ $x \cdot \frac{\pi}{2}$ $x \cdot \pi$

$\tilde{5}$

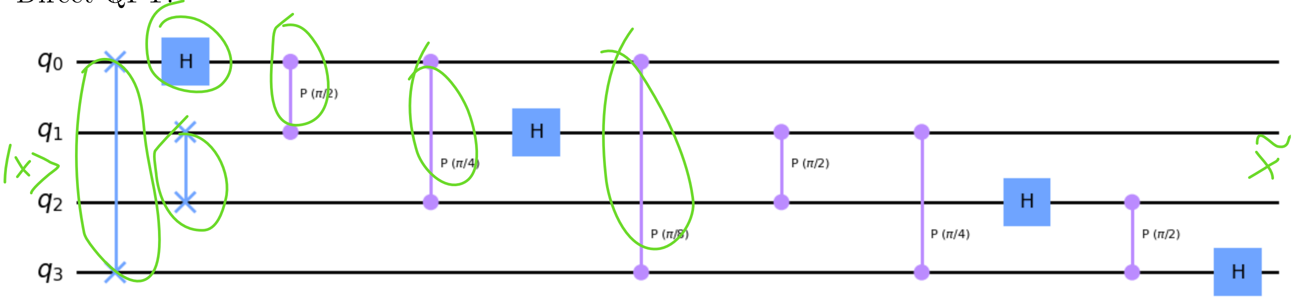
$x \cdot \frac{\pi}{8}$



$\frac{5\pi}{4}$

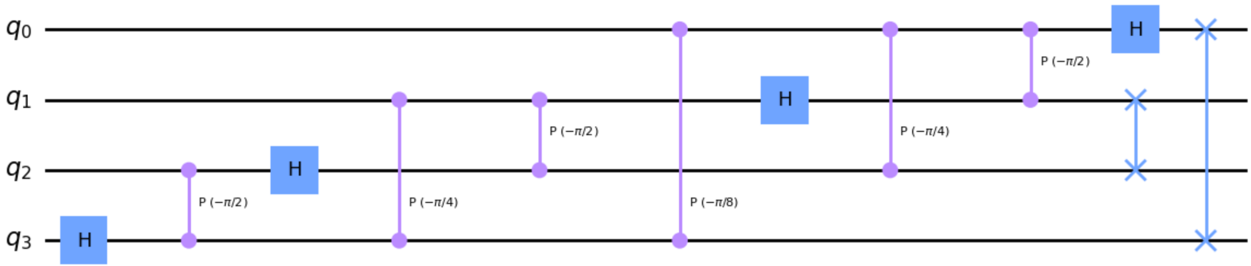
Implementation in Qiskit

Direct QFT:



Implementation in Qiskit

Inverse QFT:



Part VIII

Quantum phase estimation

Quantum phase estimation

Z CZ P($\frac{\pi}{16}$)

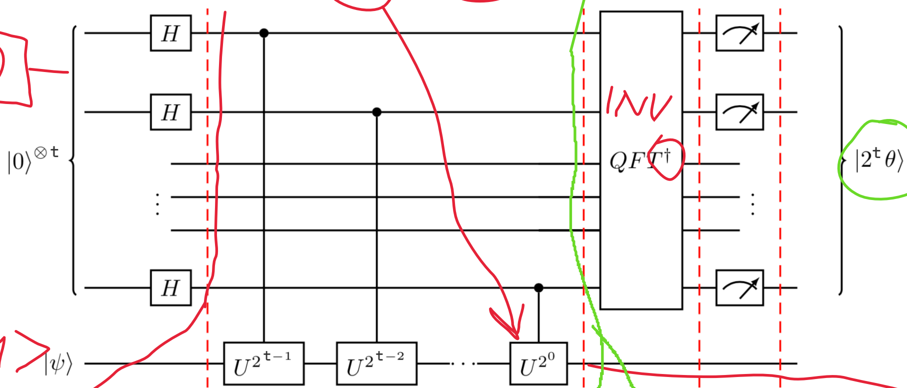
The problem statement:

Estimate the phase of an eigenvalue $e^{2\pi i\theta}$ of a unitary operator U, provided with the corresponding eigenstate ψ:

θ PHASE SHIFT

$$U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$$

H>



U U

U^2

$|1\rangle$

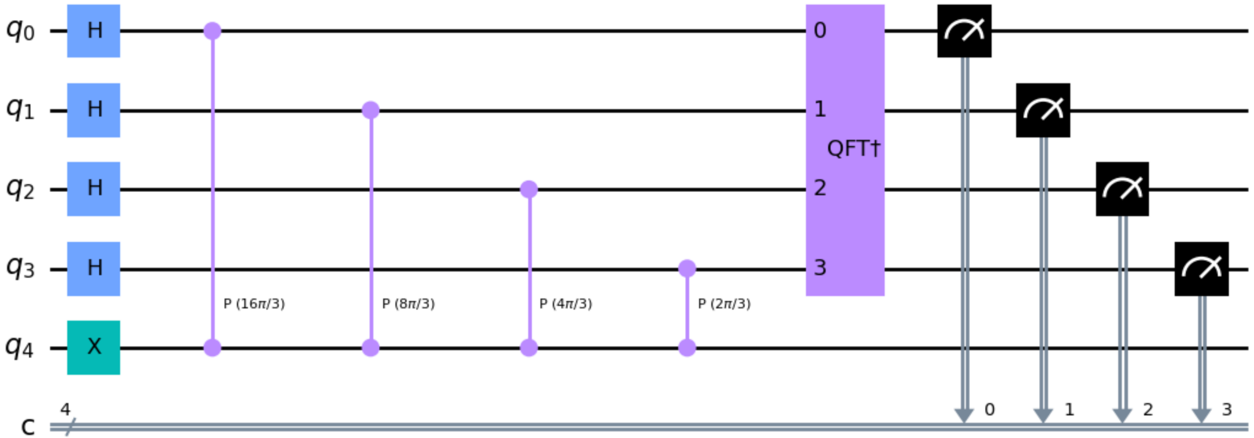
INV

IQFT

$$|0\rangle^{\otimes t} \to \underbrace{\frac{1}{\sqrt{2^t}}\Big(|0\rangle+|1\rangle\Big)^{\otimes t}}_{\varphi=0} \to \frac{1}{\sqrt{2^t}}\Big(|0\rangle+e^{2\pi i\theta 2^{t-1}}|1\rangle\Big)\otimes\Big(|0\rangle+e^{2\pi i\theta 2^{t-2}}|1\rangle\Big)\otimes\cdots\otimes\Big(|0\rangle+e^{2\pi i\theta 2^{0}}|1\rangle\Big) = \text{QFT}\,|2^t\theta\rangle$$

2^{t-1} 2^{t-2}

Implementation in Qiskit



Part IX

Shor's algorithm

Shor's algorithm

$N = P \times R$

$2^{2048} \approx 616$ DIGITS

RSA

The problem statement:

Find factors P, R of number N.

$\gcd(3,15) = 3$

$N = 15$

$\gcd(5,15) = 5$

Shor's algorithm procedure:

1. Pick a random integer number a such that: $1 < a < N$.
2. If $\gcd(a, N) \neq 1$ then $P = a$ and $R = N/a$.
3. Otherwise, find the period r of function $\boxed{f(x) = a^x \bmod N}$.
4. If r is odd then go back to step 1 and choose different a.
5. Otherwise, factors $P, R = \boxed{\gcd(a^{r/2} \pm 1, N)}$. $= \gcd(4 \pm 1, 15)$

$a = 2$

$f(0) = 2^0 \bmod 15 = 1$

$f(x) = 2^x (\bmod 15)$

$f(1) = 2 \bmod 15 = 2$

$f(2) = 4$

$f(3) = 8$

$f(4) = 2^4 \bmod 15 = 1$

$f(5) = 2^5 \bmod 15 = 2$

A quantum computer can be used for step 3, in which it is necessary to create a quantum circuit implementing the modular exponentiation function $f(x) = a^x \bmod N$ and use this circuit instead of the U operator in the quantum phase estimation circuit.
The resulting circuit is called a period-finder circuit and the measured result at the output can then be used to determine the searched period.

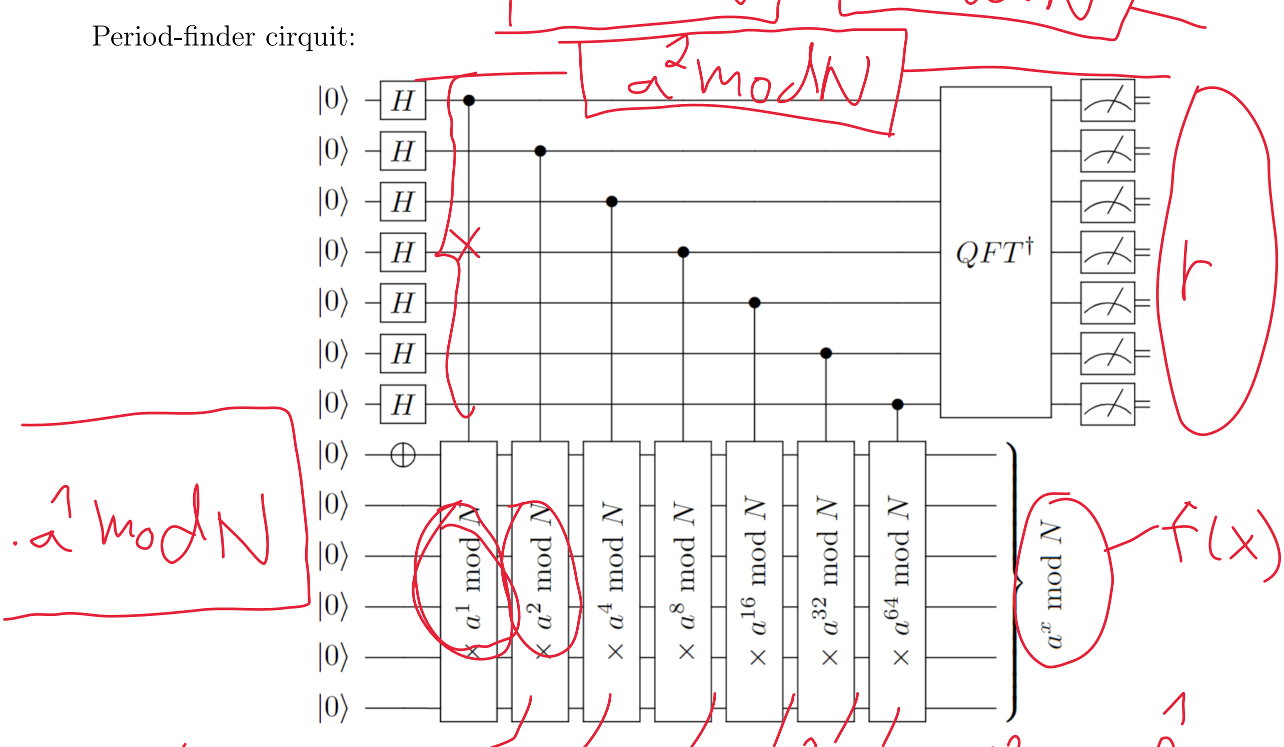
$r = 4$

$f(x) = f(x+4)$

$((y \cdot a^1 \bmod N) \cdot a^1) \bmod N = y a^2 \pmod N$

Shor's algorithm

Period-finder cirquit:



$x = (x_3 x_2 x_1 x_0)_2 = x_3 2^3 + x_2 2^2 + x_1 2^1 + x_0 2^0$

N = 35 a = 6 $f(x) = 6^x \bmod 35$

Implementation in Qiskit

$f(6) = 1$

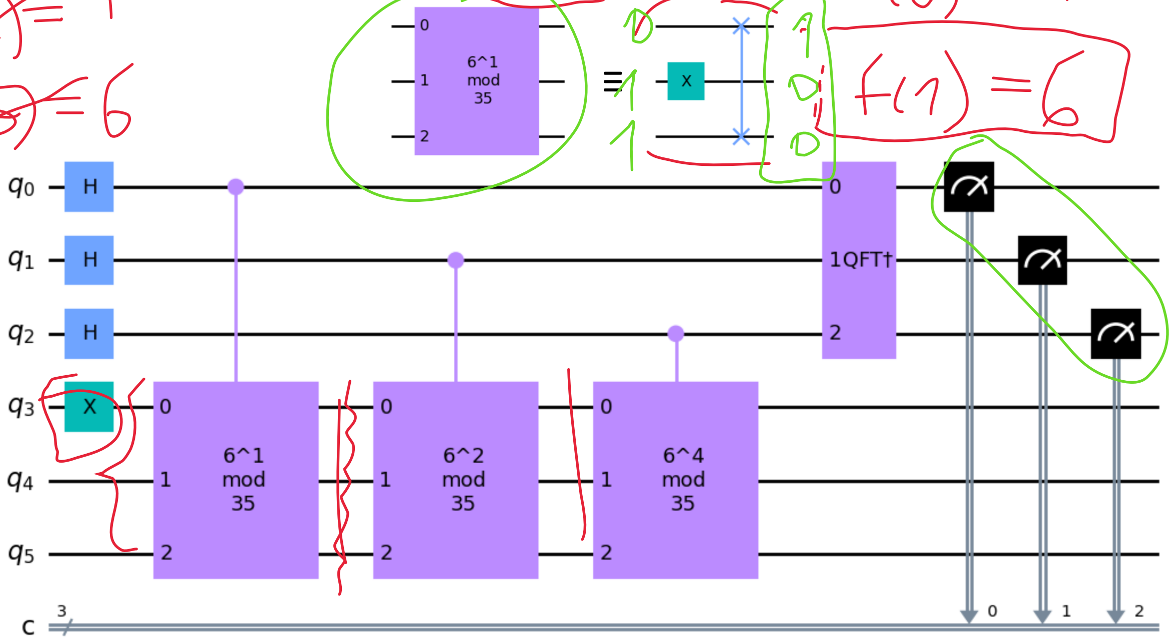
Implementation of the function $g(y) = (y \times 6) \bmod 35$ and below that the overall period-finder circuit designed to find the period of the function $f(x) = 6^x \bmod 35$:

~~$f(2) = 1$~~

~~$f(3) = 6$~~

$f(6) = 1$

$f(1) = 6$



1
0
0

$r = 2 \quad a = 6 \quad N = 35$

$$P, R = \gcd(6^1 \pm 1, 35) = \begin{cases} 7 \\ 5 \end{cases}$$

Thanks

This project has received funding from the European High-Performance Computing Joint Undertaking (JU) under grant agreement No 101101903. The JU receives support from the Digital Europe Programme and Germany, Bulgaria, Austria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Greece, Hungary, Ireland, Italy, Lithuania, Latvia, Poland, Portugal, Romania, Slovenia, Spain, Sweden, France, Netherlands, Belgium, Luxembourg, Slovakia, Norway, Türkiye, Republic of North Macedonia, Iceland, Montenegro, Serbia