EURO^2

Basic Quantum Computing Algorithms and Their Implementation in Cirq

Jiří Tomčala

IT4Innovations,
VŠB - Technical University of Ostrava

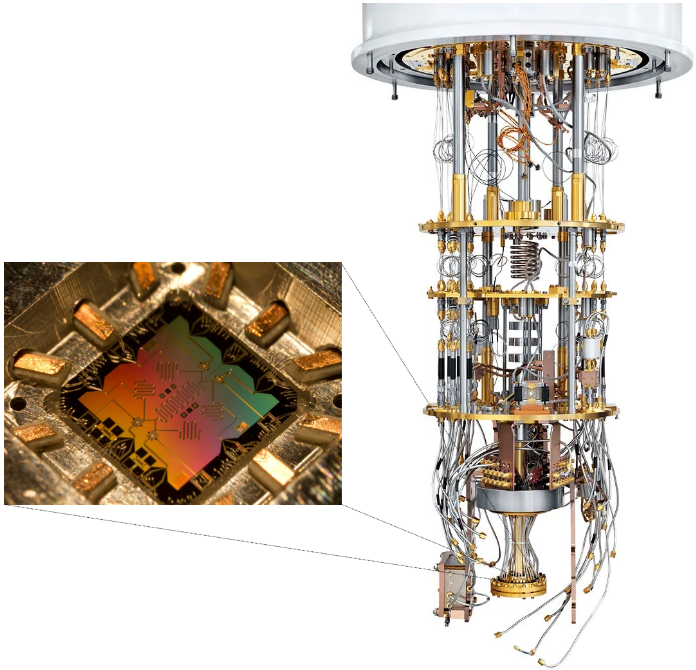
5 – 6 September 2023

Part I

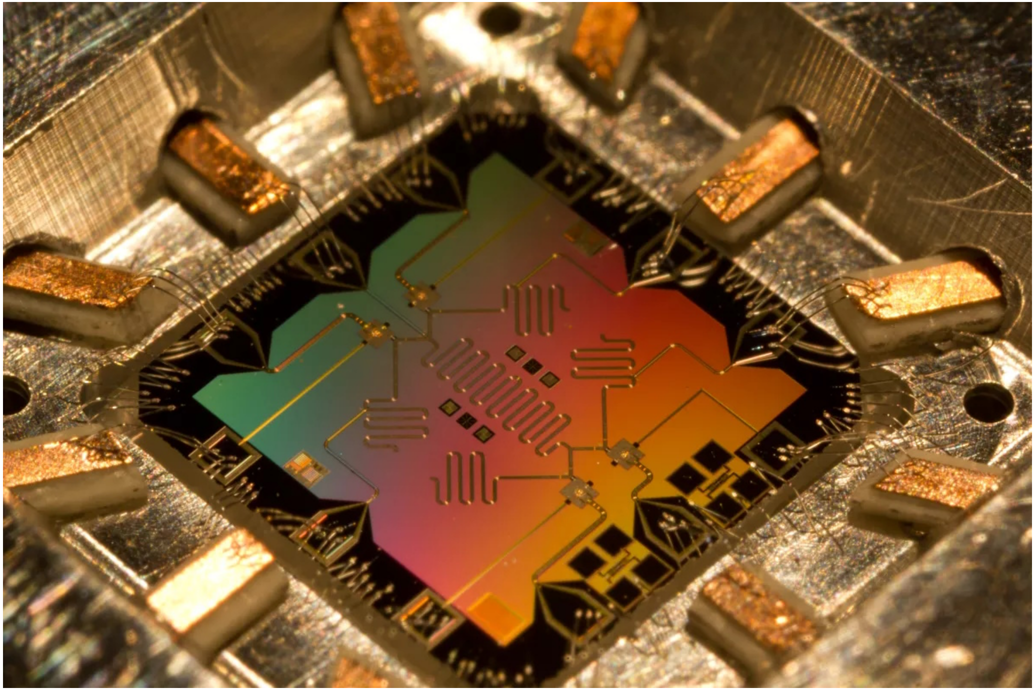
Introduction to Quantum Computing

Hardware

Superconducting technology:

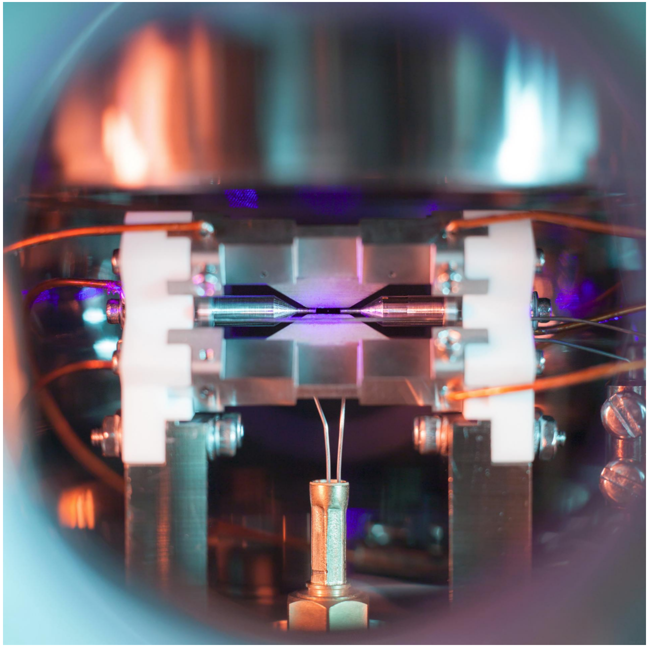


Hardware

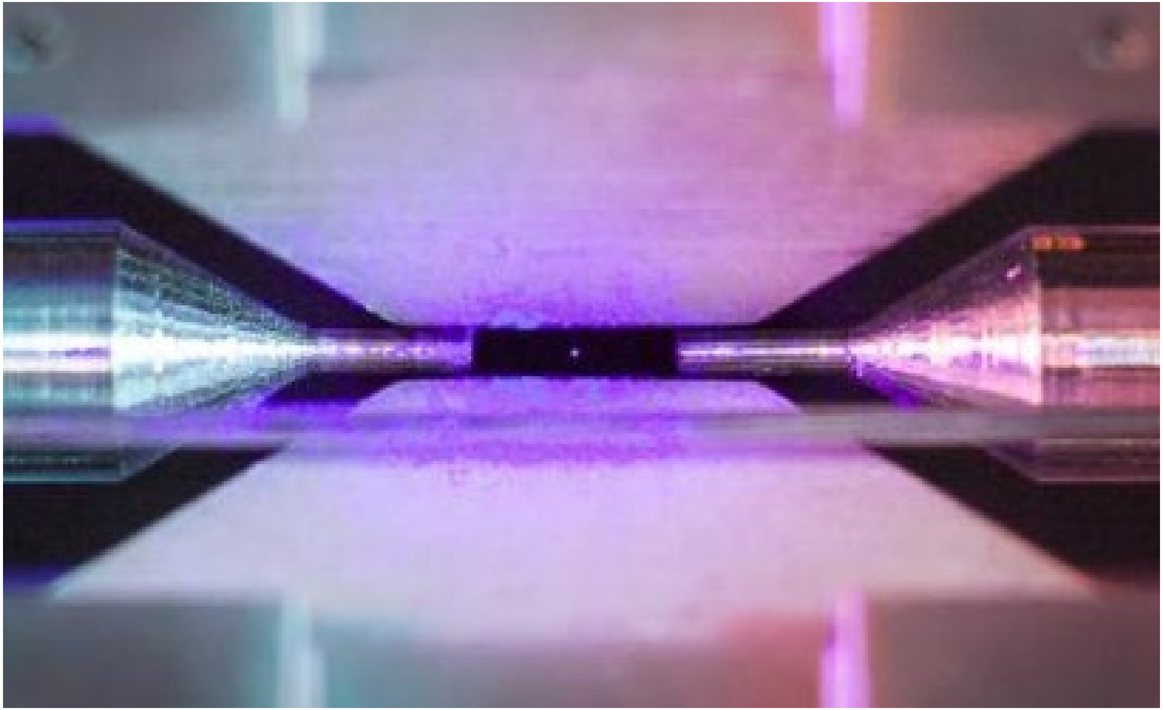


Hardware

Trapped-ion technology:



Hardware



Qubit

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

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

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

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

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

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

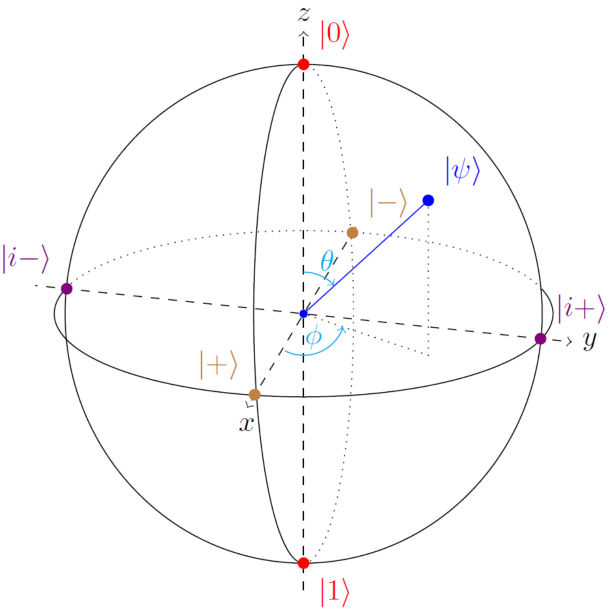


Figure. Bloch sphere.

Qubit

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

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

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

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

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

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

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

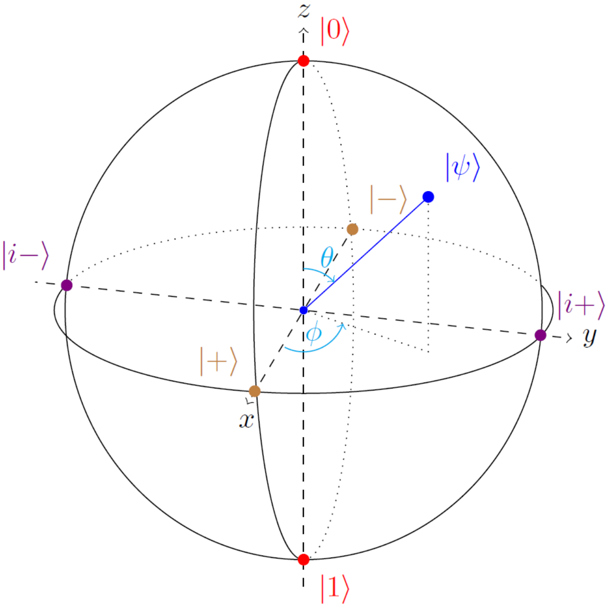


Figure. Bloch sphere.

1-qubit quantum gates

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

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

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

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

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

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

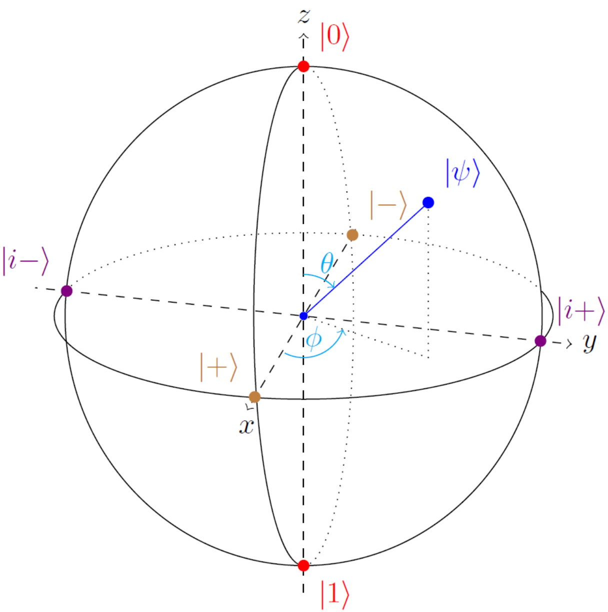


Figure. Bloch sphere.

1-qubit quantum gates

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

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

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

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

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

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

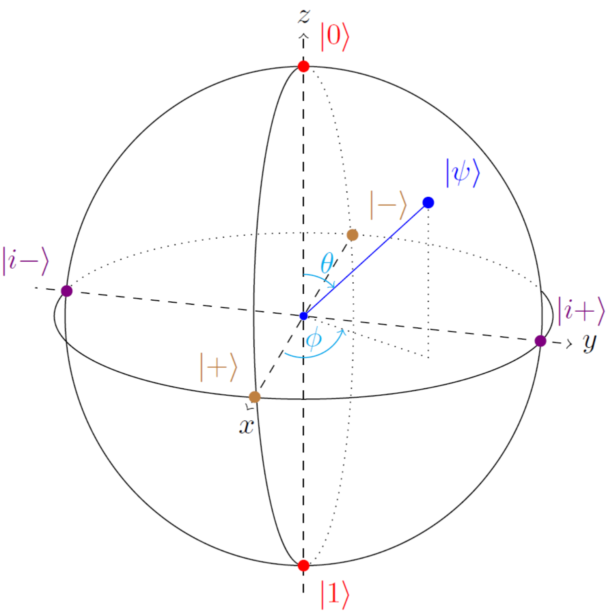
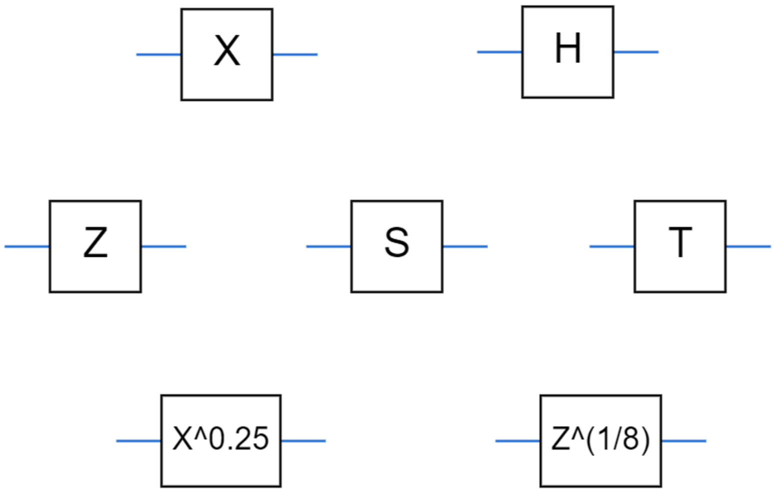


Figure. Bloch sphere.

Implementation in Cirq



2-QUBIT QUANTUM GATES

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle = \begin{bmatrix}|00\rangle & |01\rangle & |10\rangle & |11\rangle\end{bmatrix}\begin{bmatrix}\alpha_{00}\\ \alpha_{01}\\ \alpha_{10}\\ \alpha_{11}\end{bmatrix} \Rightarrow \begin{bmatrix}\alpha_{00}\\ \alpha_{01}\\ \alpha_{10}\\ \alpha_{11}\end{bmatrix}$$

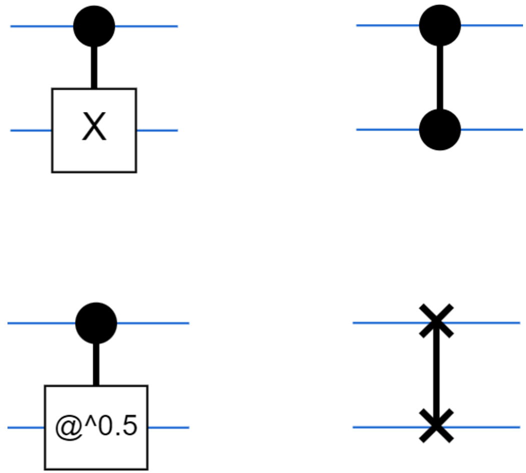
$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

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

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

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

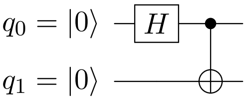
Implementation in Cirq



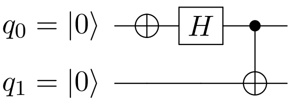
Part II

Quantum entanglement

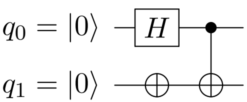
Bell states



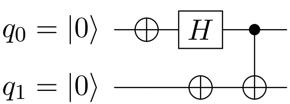
$$|\psi_e\rangle = CX|H\,|00\rangle = CX\left(\frac{1}{\sqrt{2}}\,|00\rangle + \frac{1}{\sqrt{2}}\,|01\rangle\right) = \frac{1}{\sqrt{2}}\,|00\rangle + \frac{1}{\sqrt{2}}\,|11\rangle = |\Phi^+\rangle$$



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

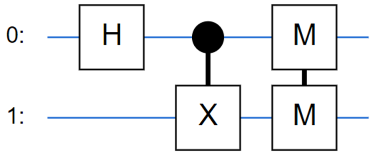


$$|\psi_e\rangle = CX|H\,|00\rangle = CX\left(\frac{1}{\sqrt{2}}\,|10\rangle + \frac{1}{\sqrt{2}}\,|11\rangle\right) = \frac{1}{\sqrt{2}}\,|10\rangle + \frac{1}{\sqrt{2}}\,|01\rangle = |\Psi^+\rangle$$

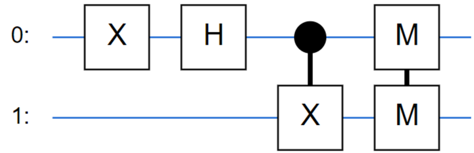


$$|\psi_e\rangle = CX|H\,|00\rangle = CX\left(\frac{1}{\sqrt{2}}\,|10\rangle - \frac{1}{\sqrt{2}}\,|11\rangle\right) = \frac{1}{\sqrt{2}}\,|10\rangle - \frac{1}{\sqrt{2}}\,|01\rangle = -\,|\Psi^-\rangle$$

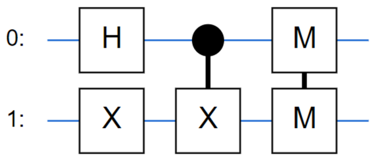
Implementation in Cirq



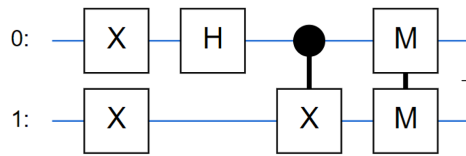
$|\Phi^+\rangle$



$|\Phi^-\rangle$



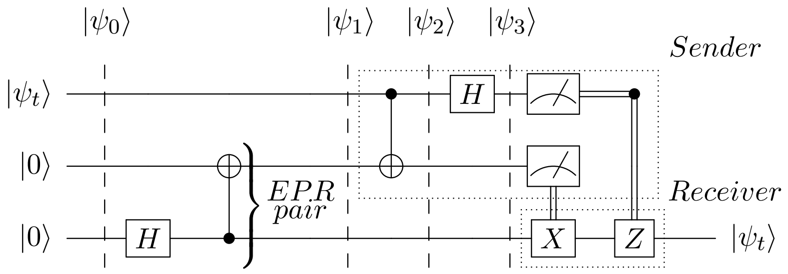
$|\Psi^+\rangle$



$-|\Psi^-\rangle$

Part III

Quantum teleportation



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

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

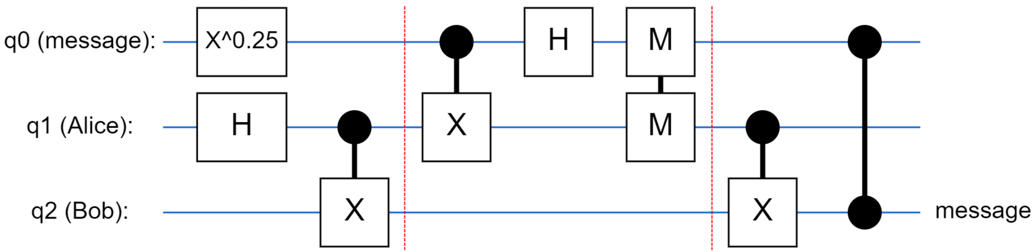
$$|\psi_2\rangle = \frac{\alpha_t}{\sqrt{2}} |000\rangle + \frac{\alpha_t}{\sqrt{2}} |011\rangle + \frac{\beta_t}{\sqrt{2}} |110\rangle + \frac{\beta_t}{\sqrt{2}} |101\rangle$$

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

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

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

Implementation in Cirq



Part IV

Bernstein-Vazirani + Deutch-Jozsa algorithm

Bernstein-Vazirani algorithm

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

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

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

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

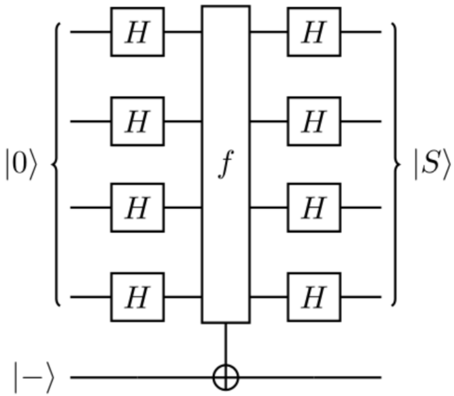
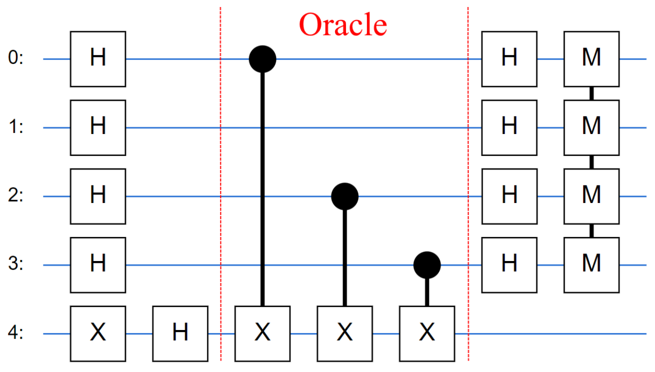


Figure. Bernstein-Vazirani circuit.

Implementation in Cirq



Deutch-Jozsa algorithm

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

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

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

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

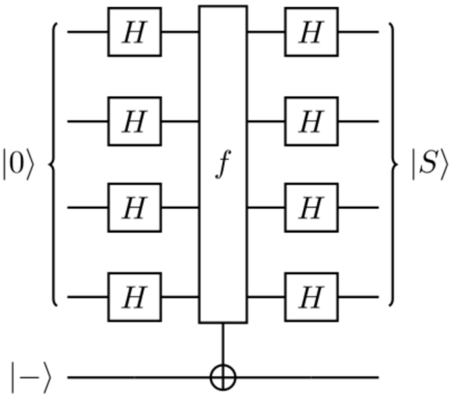
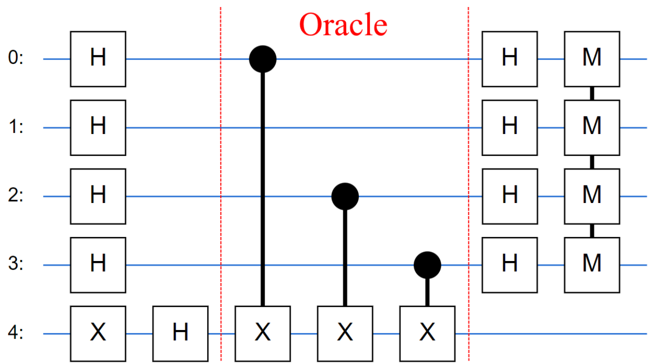


Figure. Deutch-Jozsa circuit.

Implementation in Cirq



Part V

Simon's algorithm

Simon's algorithm

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

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

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

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

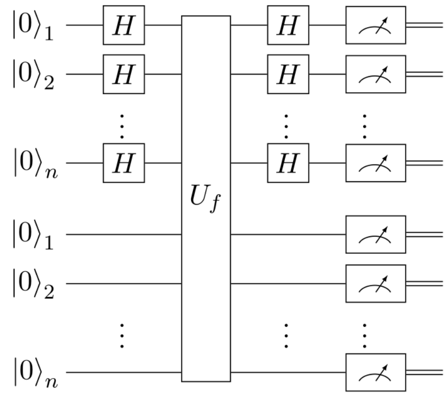


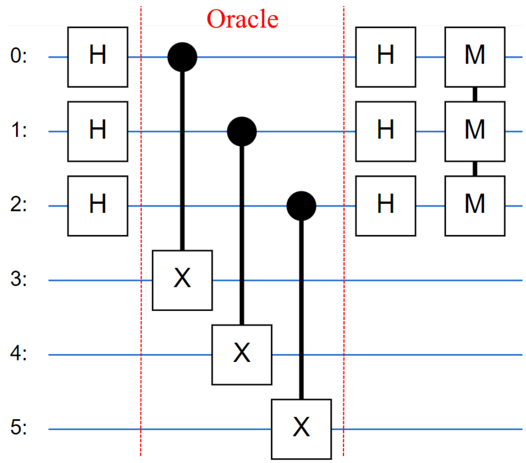
Figure. Simon's circuit.

Quantum state after measuring the lower register:

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

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

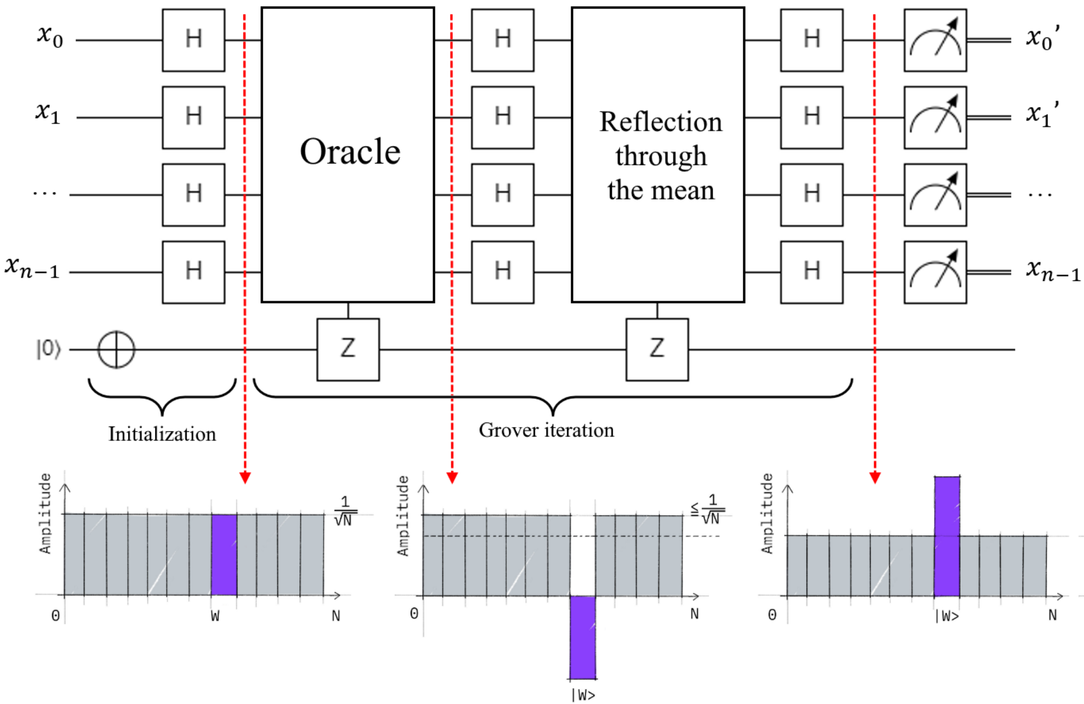
Implementation in Cirq



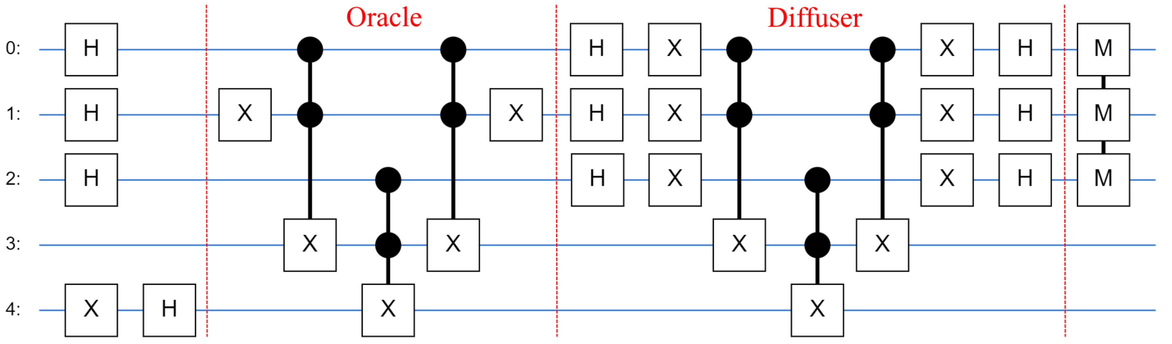
Part VI

Grover's algorithm

Grover's algorithm



Implementation in Cirq



Part VII

Quantum Fourier transform

Quantum Fourier transform

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

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

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

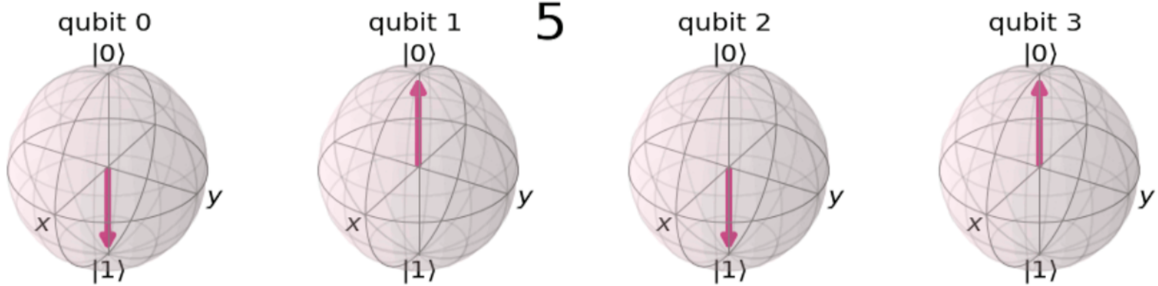
$$\text{QFT}\,|x\rangle = \frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}\prod_{k=1}^{2^n} e^{2\pi i x \frac{y_k}{2^k}}\,|y_1 y_2 \dots y_n\rangle$$

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

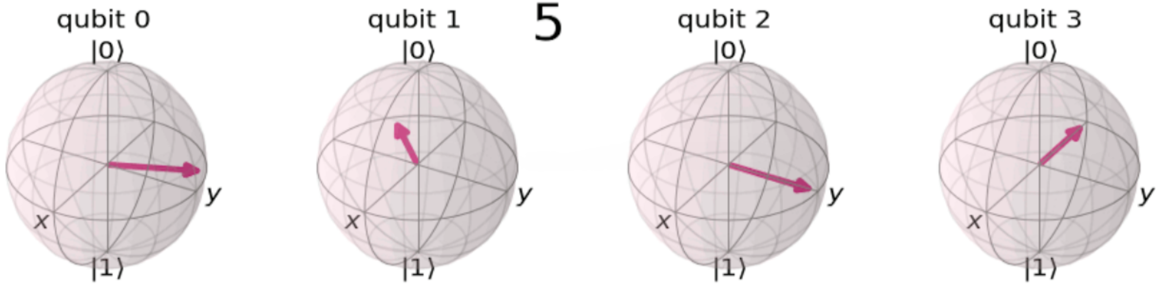
$$\text{QFT}\,|x\rangle = \frac{1}{\sqrt{2^n}}\Big(|0\rangle + e^{i\pi x}\,|1\rangle\Big) \otimes \Big(|0\rangle + e^{i\frac{\pi}{2}x}\,|1\rangle\Big) \otimes \Big(|0\rangle + e^{i\frac{\pi}{4}x}\,|1\rangle\Big) \otimes \cdots \cdots \otimes \Big(|0\rangle + e^{i\frac{\pi}{2^{n-1}}x}\,|1\rangle\Big)$$

Quantum Fourier transform

5

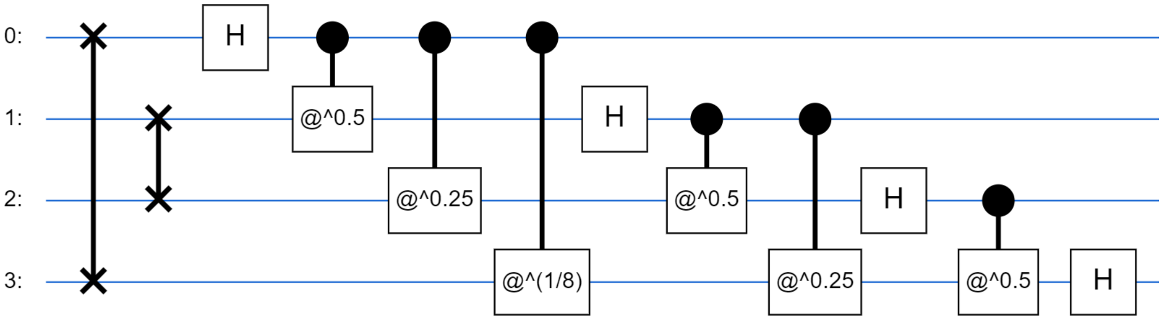


$\widetilde{5}$



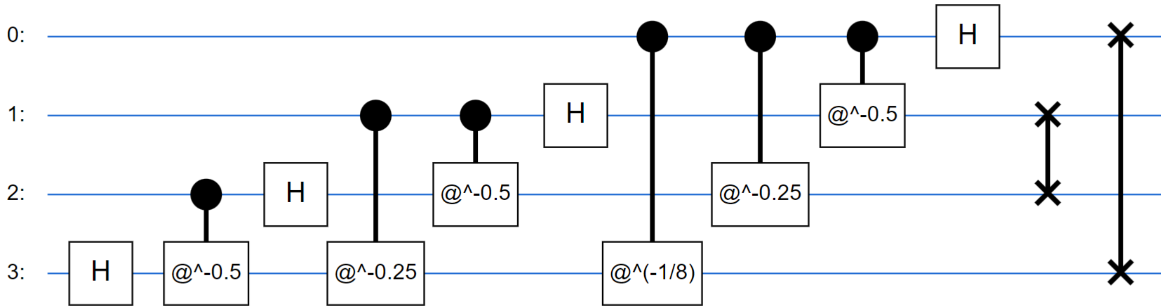
Implementation in Cirq

Direct QFT:



Implementation in Cirq

Inverse QFT:



Part VIII

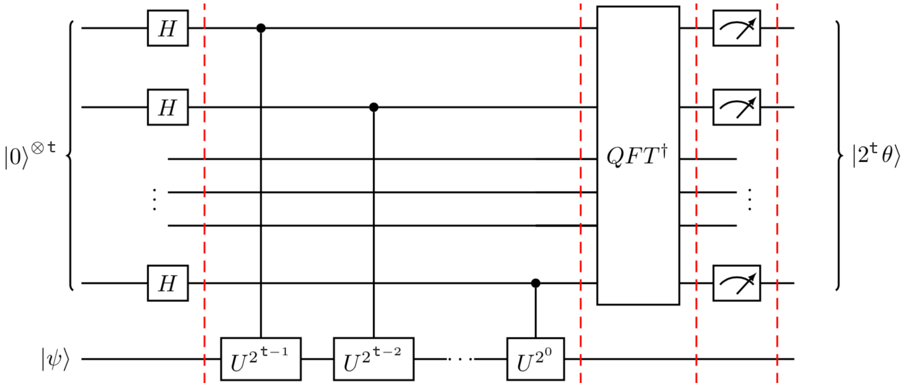
Quantum phase estimation

Quantum phase estimation

The problem statement:

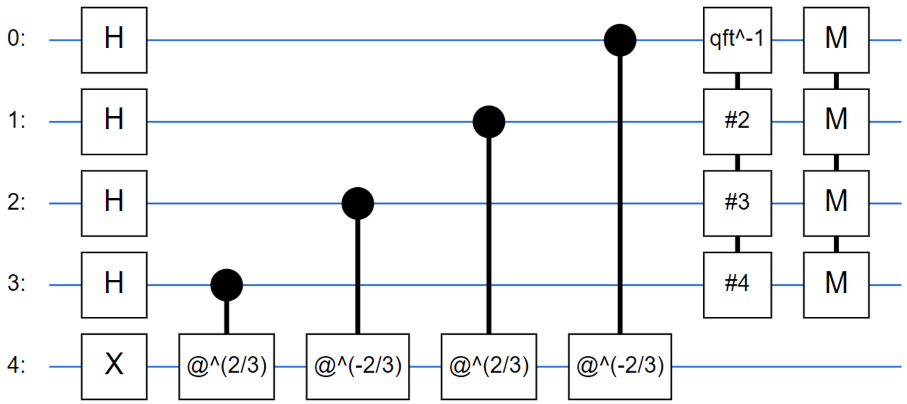
Estimate the phase of an eigenvalue $e^{2\pi i\theta}$ of a unitary operator U, provided with the corresponding eigenstate ψ:

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



$$|0\rangle^{\otimes t} \to \frac{1}{\sqrt{2^t}}\Big(|0\rangle+|1\rangle\Big)^{\otimes t} \to \frac{1}{\sqrt{2^t}}\Big(|0\rangle+e^{2\pi i\theta 2^{t-1}}|1\rangle\Big)\otimes\Big(|0\rangle+e^{2\pi i\theta 2^{t-2}}|1\rangle\Big)\otimes\cdots\otimes\Big(|0\rangle+e^{2\pi i\theta 2^{0}}|1\rangle\Big) = \mathrm{QFT}\left|2^t\theta\right\rangle$$

Implementation in Cirq



Part IX

Shor's algorithm

Shor's algorithm

The problem statement:

Find factors P, R of number N.

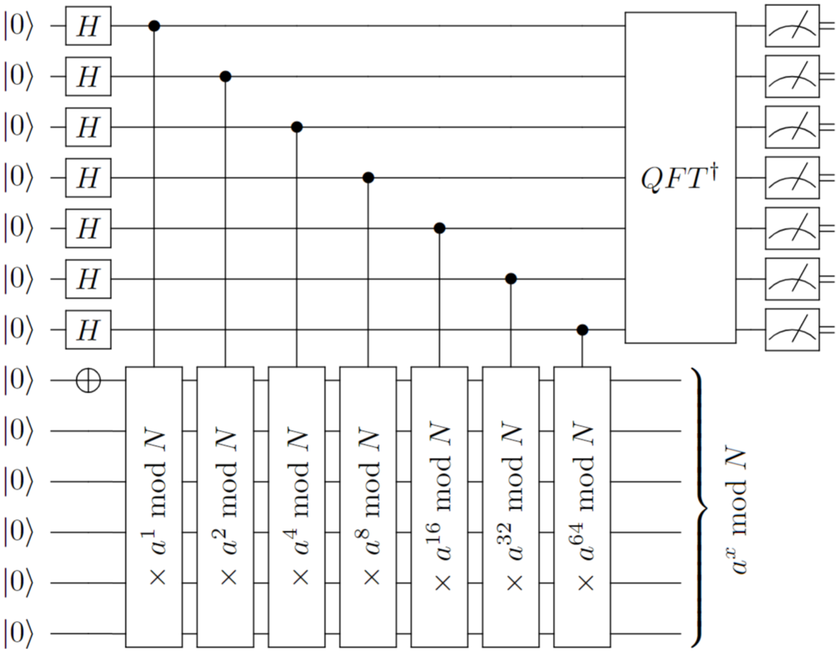
Shor's algorithm procedure:

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 $f(x) = a^x \bmod N$.
4. If r is odd then go back to step 1 and choose different a.
5. Otherwise, factors $P, R = \gcd(a^{r/2} \pm 1, N)$.

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.

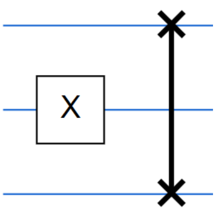
Shor's algorithm

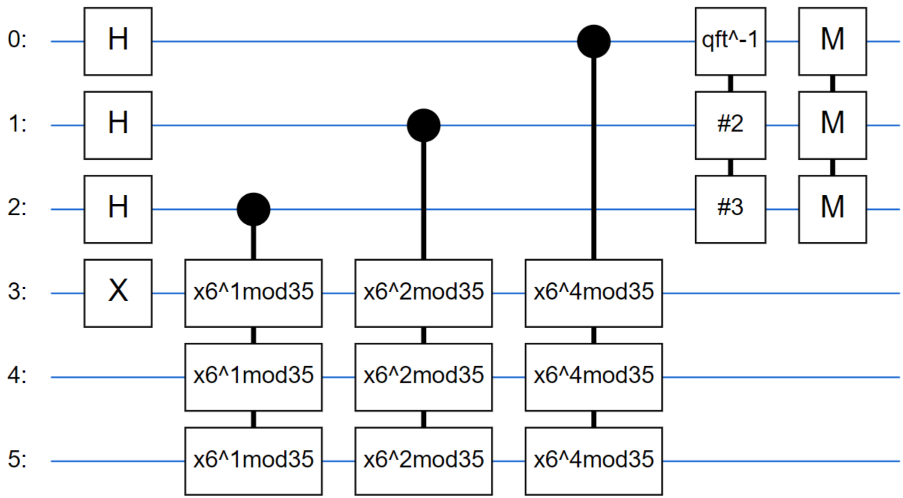
Period-finder cirquit:



Implementation in Cirq

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





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