Basic Quantum Computing Algorithms and Their Implementation in Cirq

Jiří Tomčala

IT4Innovations,
VŠB - Technical University of Ostrava

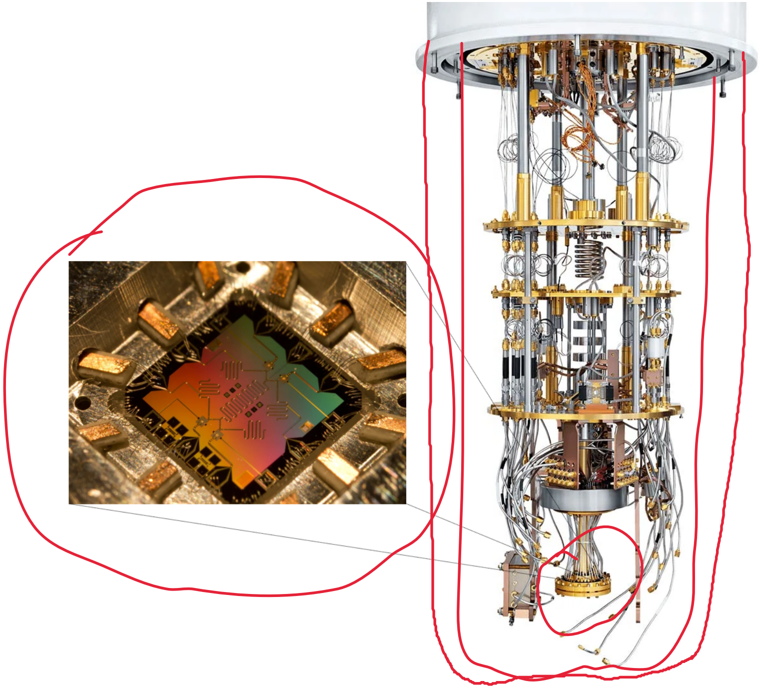
5 – 6 September 2023

Part I

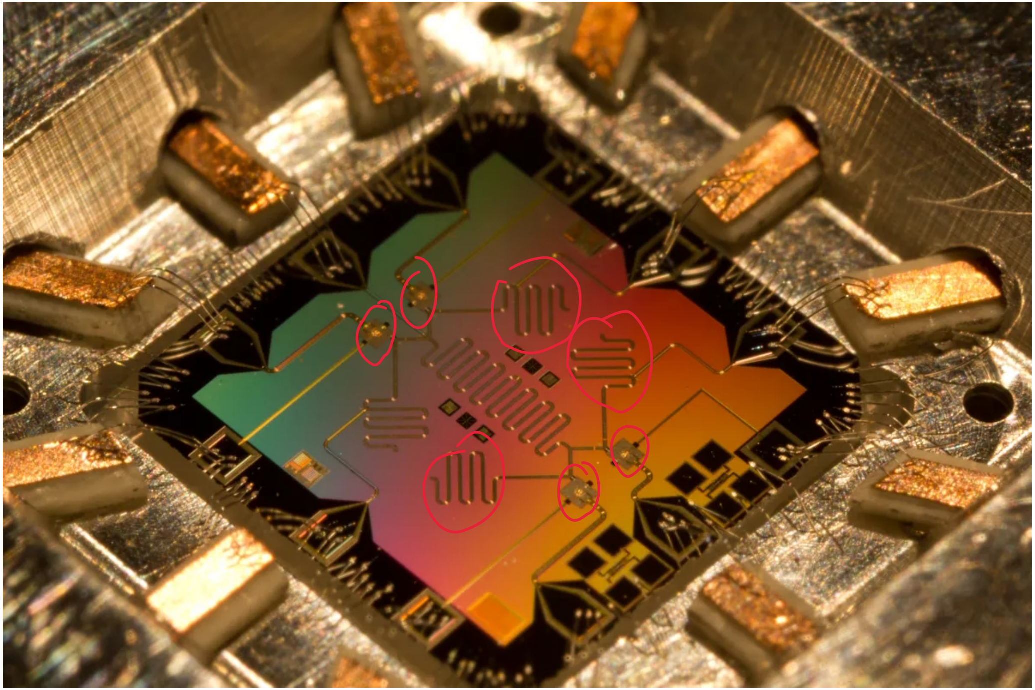
Introduction to Quantum Computing

Hardware

Superconducting technology:

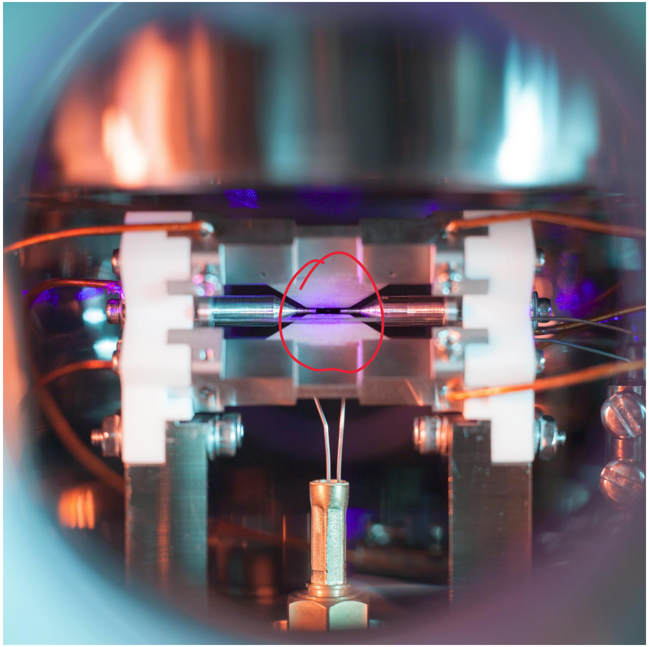


Hardware

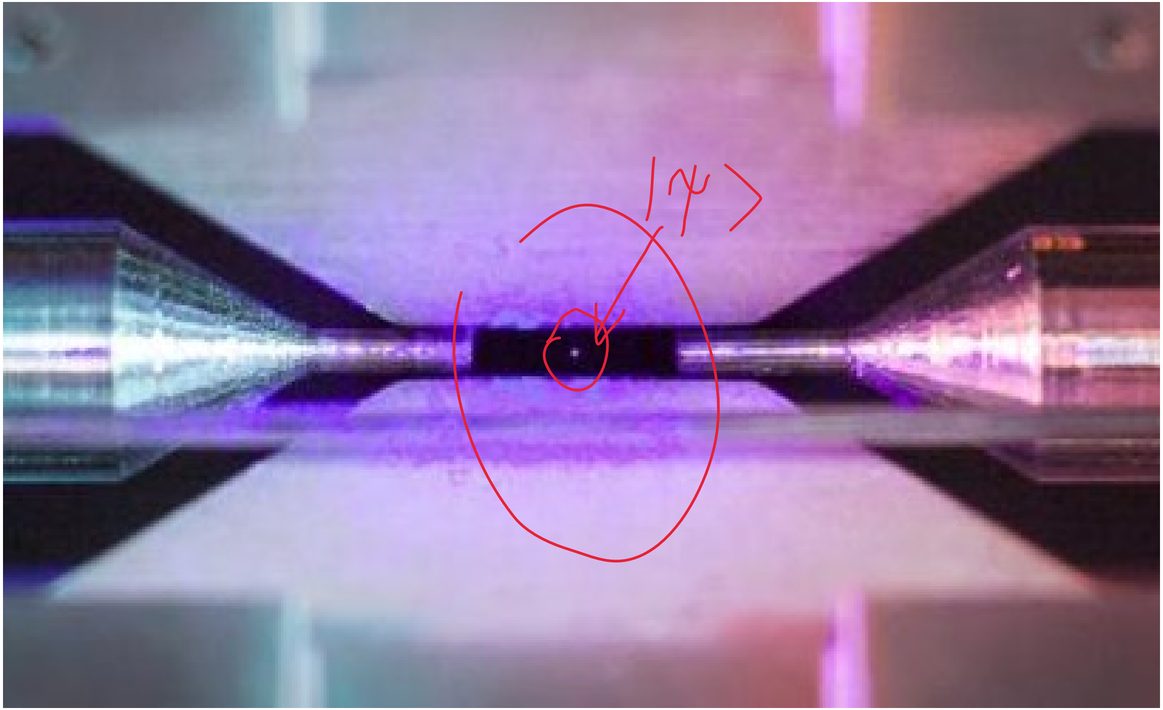


Hardware

Trapped-ion technology:



Hardware



Qubit

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

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

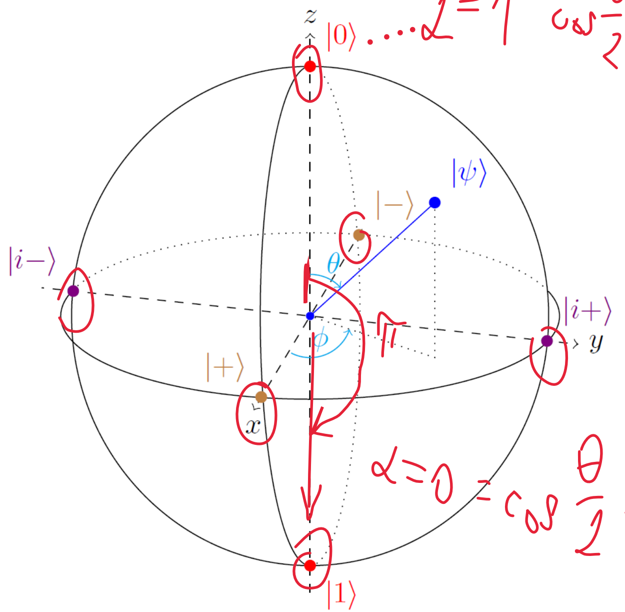
α, β ... AMPLITUDES

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

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

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

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



$|0\rangle$ .... $\alpha \doteq 1$ $\quad \cos\frac{\theta}{2} \doteq 1$

π

$\alpha = 0 = \cos\frac{\theta}{2} \doteq \cos$

Figure. Bloch sphere.

Qubit

QUBIT IS IN EQUAL SUPERPOSITION OF 0 & 1

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

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

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

$$|+\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle = \cos\frac{\pi/2}{2}\,|0\rangle + \sin\frac{\pi/2}{2}\,|1\rangle$$

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

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

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

$$\theta = \frac{\pi}{2}$$

$$\cos\frac{\pi}{4} = \frac{1}{\sqrt{2}}$$

$$\Pr(0) = |\alpha|^2 = \frac{1}{2}$$

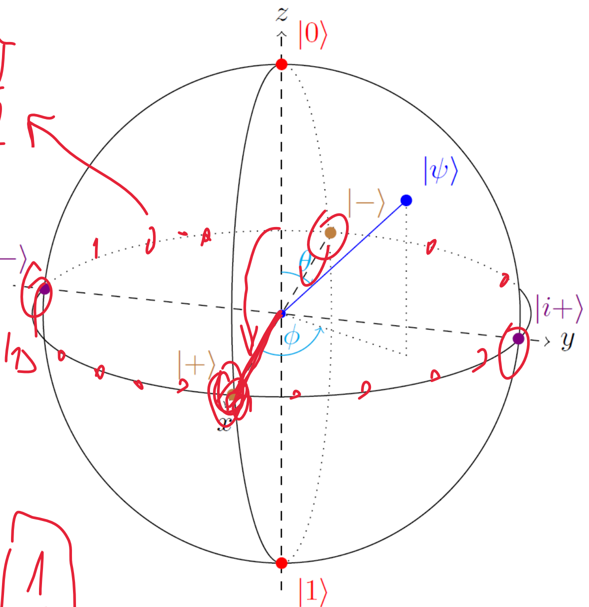


Figure. Bloch sphere.

1-QUBIT QUANTUM GATES

H HADAMARD GATE

$HH = I$

$|+\rangle$

$|0\rangle - \boxed{H} - \boxed{H} - |0\rangle$

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

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

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

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

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

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

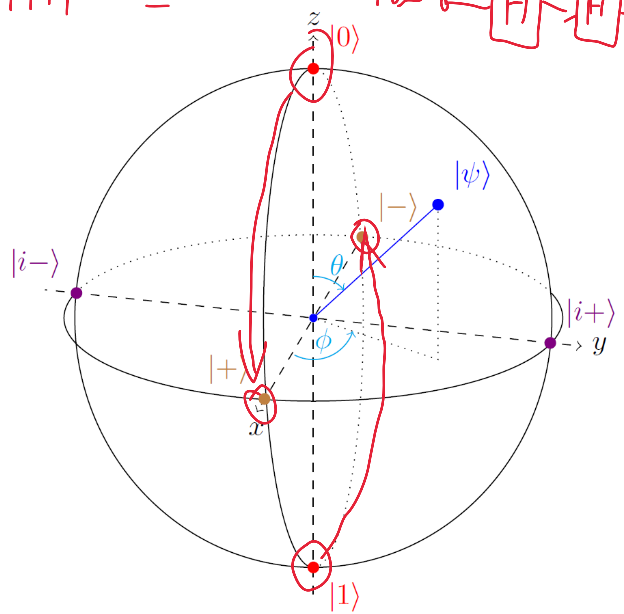


Figure. Bloch sphere.

1-QUBIT QUANTUM GATES

P ... PHASE GATE

$P(\pi) = Z$

$\lambda = \pi \Rightarrow Z$

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

$P(-\frac{\pi}{2}) = S^\dagger$

$P(\frac{\pi}{4}) = T$

$P(-\frac{\pi}{4}) = T^\dagger$

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

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

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

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

$Z\,|+\rangle = |-\rangle \quad Z\,|-\rangle = |+\rangle \quad S\,|+\rangle = |i+\rangle$

$Z|i-\rangle = S|S\,|i-\rangle = T|T|T|T\,|i-\rangle = |i+\rangle$

$P(\pi) = Z = \boxed{SS} = P(\frac{\pi}{2})\,P(\frac{\pi}{2})$

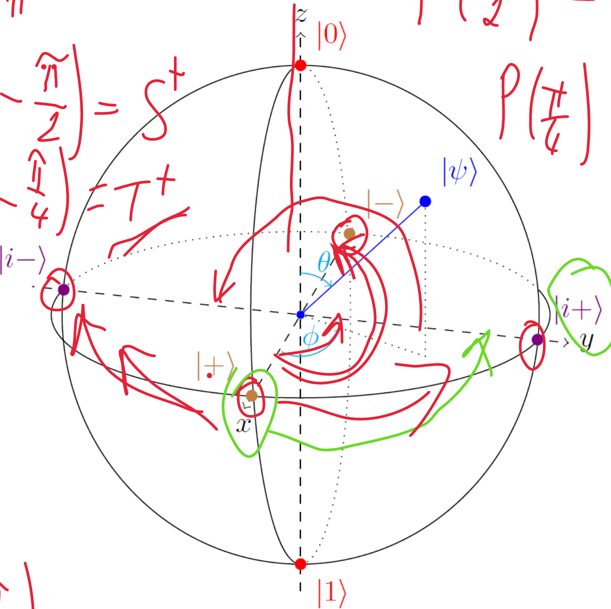
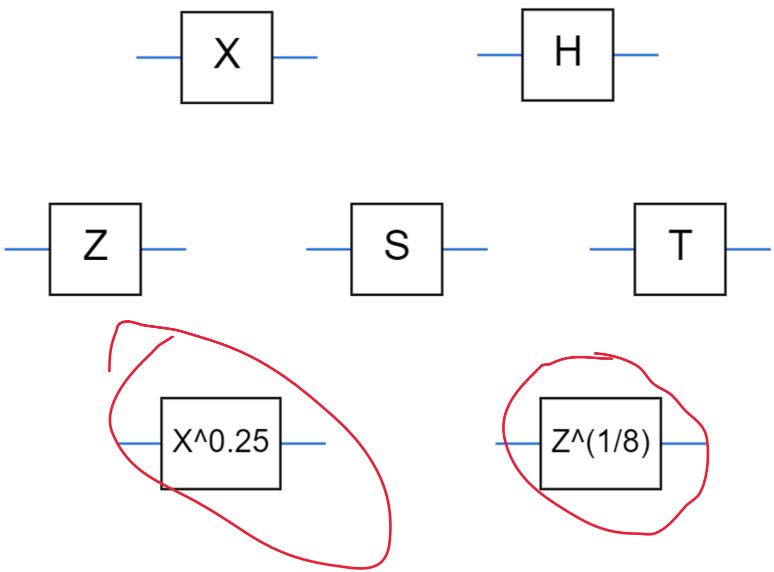


Figure. Bloch sphere.

Implementation in Cirq



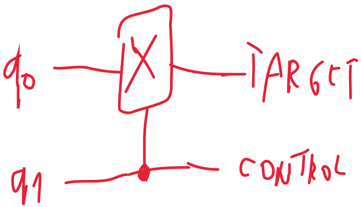
2-QUBIT QUANTUM GATES

$|\psi\rangle = |q_1 q_0\rangle$

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

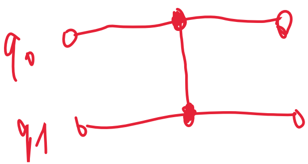
$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

$q_1\ q_0$	CNOT (CX)
0 0	0 0
0 1	0 1
1 0	1 1
1 1	1 0

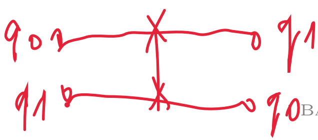


$$CX|\psi\rangle = \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}\begin{bmatrix}\alpha_{00}\\ \alpha_{01}\\ \alpha_{10}\\ \alpha_{11}\end{bmatrix} = \begin{bmatrix}\alpha_{00}\\ \alpha_{01}\\ \alpha_{11}\\ \alpha_{10}\end{bmatrix}$$

(CNOT)

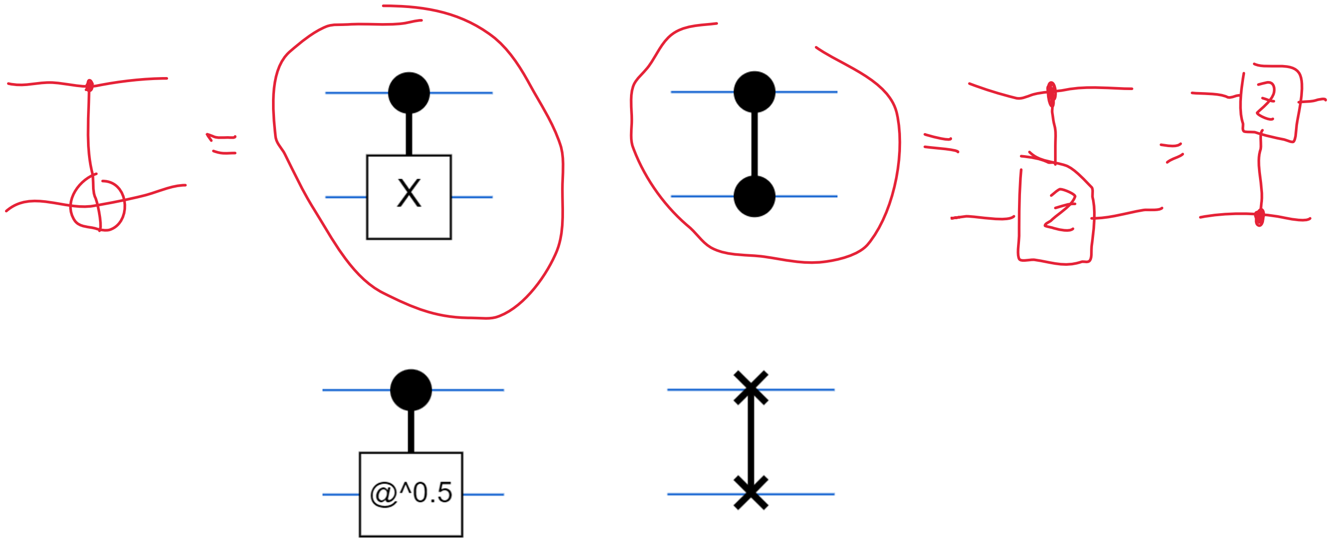


$$CP(\lambda)|\psi\rangle = \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&e^{i\lambda}\end{bmatrix}\begin{bmatrix}\alpha_{00}\\ \alpha_{01}\\ \alpha_{10}\\ \alpha_{11}\end{bmatrix} = \begin{bmatrix}\alpha_{00}\\ \alpha_{01}\\ \alpha_{10}\\ e^{i\lambda}\alpha_{11}\end{bmatrix}$$

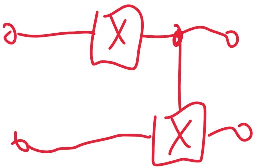


$$SWAP|\psi\rangle = \begin{bmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{bmatrix}\begin{bmatrix}\alpha_{00}\\ \alpha_{01}\\ \alpha_{10}\\ \alpha_{11}\end{bmatrix} = \begin{bmatrix}\alpha_{00}\\ \alpha_{10}\\ \alpha_{01}\\ \alpha_{11}\end{bmatrix}$$

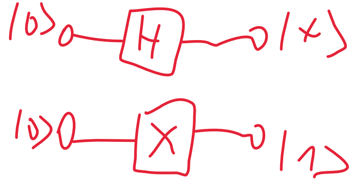
Implementation in Cirq



$|00\rangle$



$|11\rangle = |1\rangle \otimes |1\rangle$

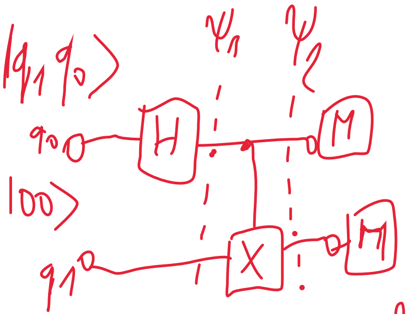


$|+\rangle \otimes |1\rangle$

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

Part II

Quantum entanglement



$$\psi_1 = |0+\rangle = |0\rangle \otimes |+\rangle = |0\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) =$$

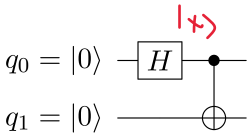
$$= \underbrace{\frac{1}{\sqrt{2}}|\overset{q_1 q_0}{00}\rangle + \frac{1}{\sqrt{2}}|\overset{q_1 q_0}{01}\rangle}$$

$$\psi_2 = CNOT|\psi_1\rangle = \boxed{\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle} \neq \psi_{q_0} \otimes \psi_{q_1}$$

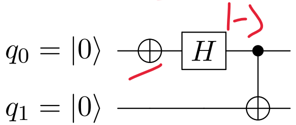
$M|q_0\rangle = 0 \Rightarrow M|q_1\rangle = 0$

$M|q_0\rangle = 1 \Rightarrow M|q_1\rangle = 1$

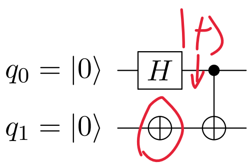
Bell states



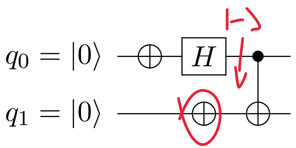
$$|\psi_e\rangle = CX|H\,|00\rangle = CX\left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|01\rangle\right) = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle = |\Phi^+\rangle$$



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



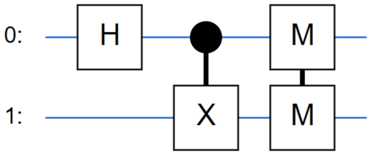
$$|\psi_e\rangle = CX|H\,|00\rangle = CX\left(\frac{1}{\sqrt{2}}|10\rangle + \frac{1}{\sqrt{2}}|11\rangle\right) = \boxed{\frac{1}{\sqrt{2}}|10\rangle + \frac{1}{\sqrt{2}}|01\rangle} = |\Psi^+\rangle$$



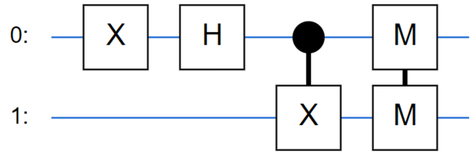
$$|\psi_e\rangle = CX|H\,|00\rangle = CX\left(\frac{1}{\sqrt{2}}|10\rangle - \frac{1}{\sqrt{2}}|11\rangle\right) = \boxed{\frac{1}{\sqrt{2}}|10\rangle - \frac{1}{\sqrt{2}}|01\rangle} = -|\Psi^-\rangle$$

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

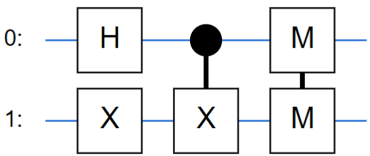
Implementation in Cirq



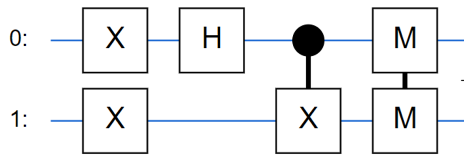
$|\Phi^{+}\rangle$



$|\Phi^{-}\rangle$



$|\Psi^{+}\rangle$

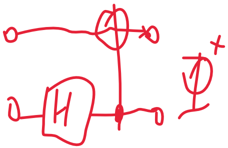


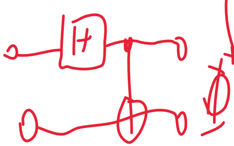
$-|\Psi^{-}\rangle$

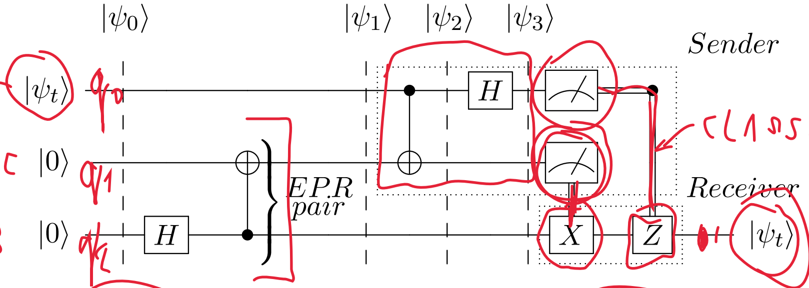
Part III

Quantum teleportation

EPR pair EINSTEIN - PODOLSKY - ROSEN pair = Bell state







$= \alpha_t|0\rangle + \beta_t|1\rangle$

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

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

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

$$|\psi_3\rangle = \frac{1}{2}|00\rangle \otimes (\alpha_t|0\rangle + \beta_t|1\rangle) + \frac{1}{2}|01\rangle \otimes (\alpha_t|1\rangle + \beta_t|0\rangle) +$$
$$+ \frac{1}{2}|10\rangle \otimes (\alpha_t|0\rangle - \beta_t|1\rangle) + \frac{1}{2}|11\rangle \otimes (\alpha_t|1\rangle - \beta_t|0\rangle) =$$
$$= \frac{1}{2}|00\rangle \otimes |\psi_t\rangle + \frac{1}{2}|01\rangle \otimes |\overline{\psi_t}\rangle + \frac{1}{2}|10\rangle \otimes \left|\psi_t^\dagger\right\rangle + \frac{1}{2}|11\rangle \otimes \left|\overline{\psi_t^\dagger}\right\rangle$$

$\alpha_t|1\rangle + \beta_t|0\rangle$

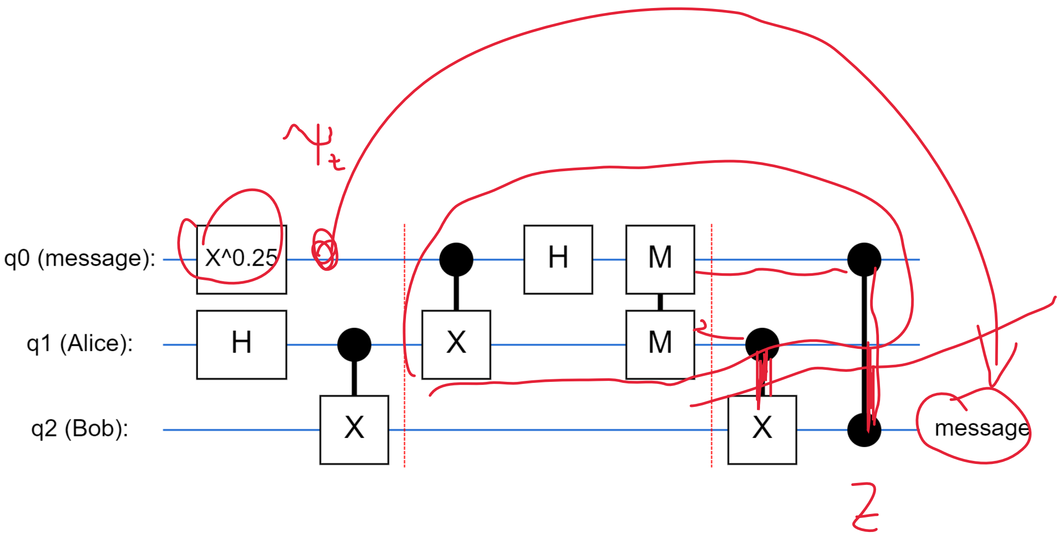
$\alpha_t|0\rangle + \beta_t|1\rangle$

$X \to \psi_t$

$XZ \to \psi_t$

$\psi_t \leftarrow Z$

Implementation in Cirq



Part IV

Bernstein-Vazirani + Deutch-Jozsa algorithm

Bernstein-Vazirani algorithm

$\frac{1}{\sqrt{2^3}}\left(|000\rangle + |001\rangle + |010\rangle + \quad + |111\rangle\right)$

ORACLE

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

$f(x)=0$ $\quad f(x)=1$

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

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

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

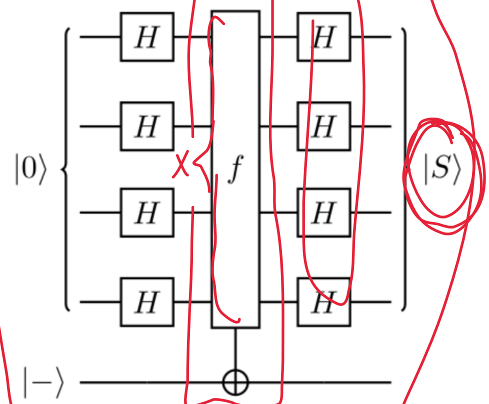
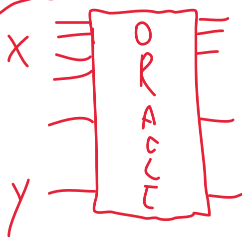


Figure. Bernstein-Vazirani circuit.



$(-1)^0 + (-1)^1 + \quad 1-1$

$y\oplus f(x) = y\oplus(x\cdot s)$

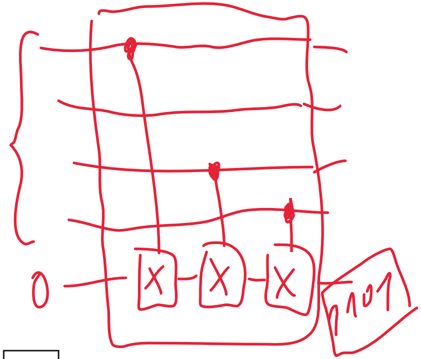
x	$x\cdot s$
001	1
010	0
100	1

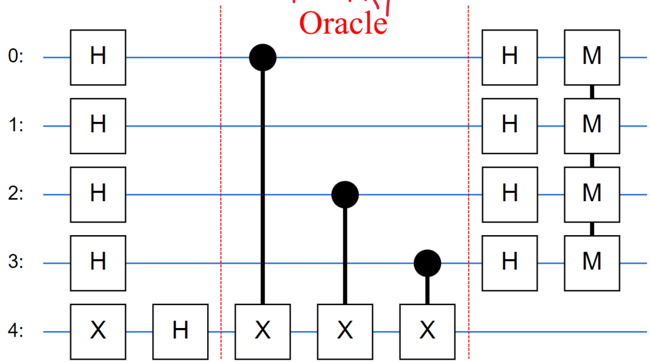
$\} \; s = 101$ $\quad$ 3 times

Implementation in Cirq

$x = \begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{matrix}$

4x TRY





$|-\rangle$

$1101 = 13$

$f(x) = x \cdot s =$

$= x_0 s_0 \oplus x_1 s_1 \oplus x_2 s_2 \oplus x_3 s_3$

Deutch-Jozsa algorithm

$f(x)$ $\left(2^{n-1}+1\right)$ TRIES

x	C	B	B	B
000	0	0	0	0
001	0	1	0	0
010	0	0	1	0
011	0	1	1	0
100	0	0	0	1
		1	0	1
			1	1
			1	1

The problem statement: Decide whether the implemented function f is constant or balanced.

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

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

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

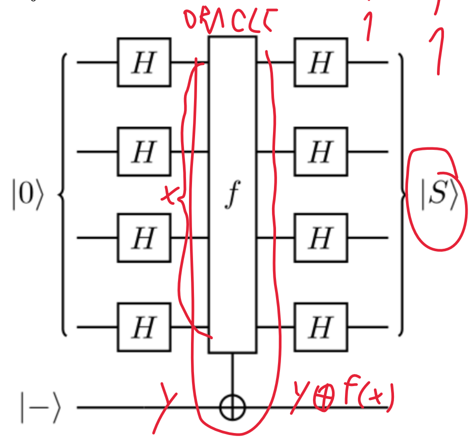


Figure. Deutch-Jozsa circuit.

$|y\rangle = |0\rangle^{\otimes n} \to (-1)^0 + (-1)^0 + (-1)^0 + \dots + (-1)^0 = 1+1+1+\dots 1 = 2^n$

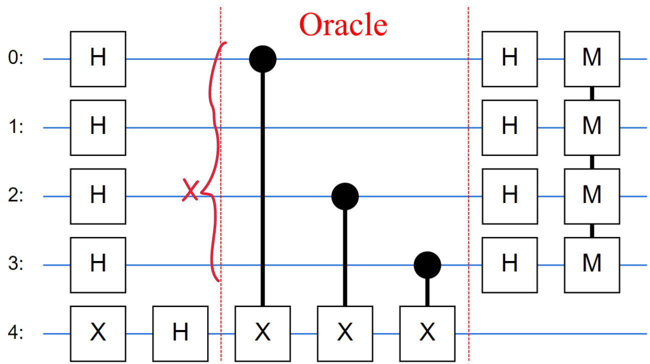
$\to (-1)^0 + (-1)^1 + (-1)^0 + (-1)^1 + \dots = 1-1+1-1\dots = 0$

Implementation in Cirq

$n = 4$

$2^3 + 1 = 9$ TRIES

x	f(x)
0000	0
0001	1
0010	0
0011	1
0100	1
0101	



NOT PERIOD

x	$f(x)$
000	111
001	110
010	101
011	100
100	011

$$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$$

2^n TRIES

Part V

Simon's algorithm

x	$f(x)$
000	000
001	000
010	000
011	000
100	100
101	100
110	100
	100

Simon's algorithm

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

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

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

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

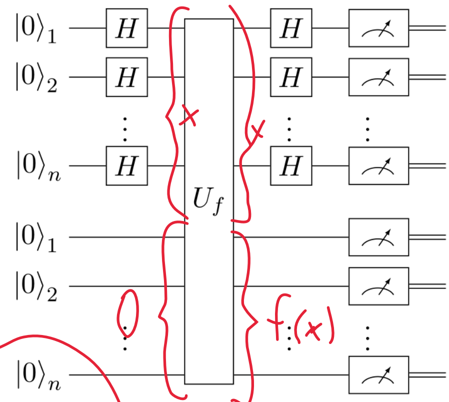


Figure. Simon's circuit.

Quantum state after measuring the lower register:

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

$(-1)^0+(-1)^0+(-1)^0+(-1)^0=4$

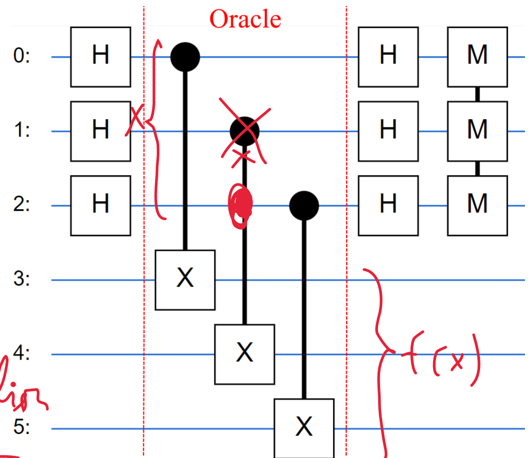
Implementation in Cirq

$n = 10$

$2^{10} = 1024$

$n = 20$

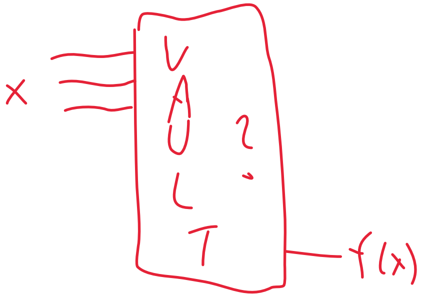
$2^{20} = 1024^2 \sim 1$ milion



q 2 1 0	f(x)	f_2
000	000	000
001	001	001
010	010	000
011	011	001
100	100	
101	101	
110	110	
111	111	

$f(x) = x$

w ... secret code



$f(w) = 1$

$f(x \neq w) = 0$

Part VI

Grover's algorithm

	x	$f(x)$
	000	0
	001	0
	010	0
w	101	1
	111	

$2^n - 1$

Grover's algorithm

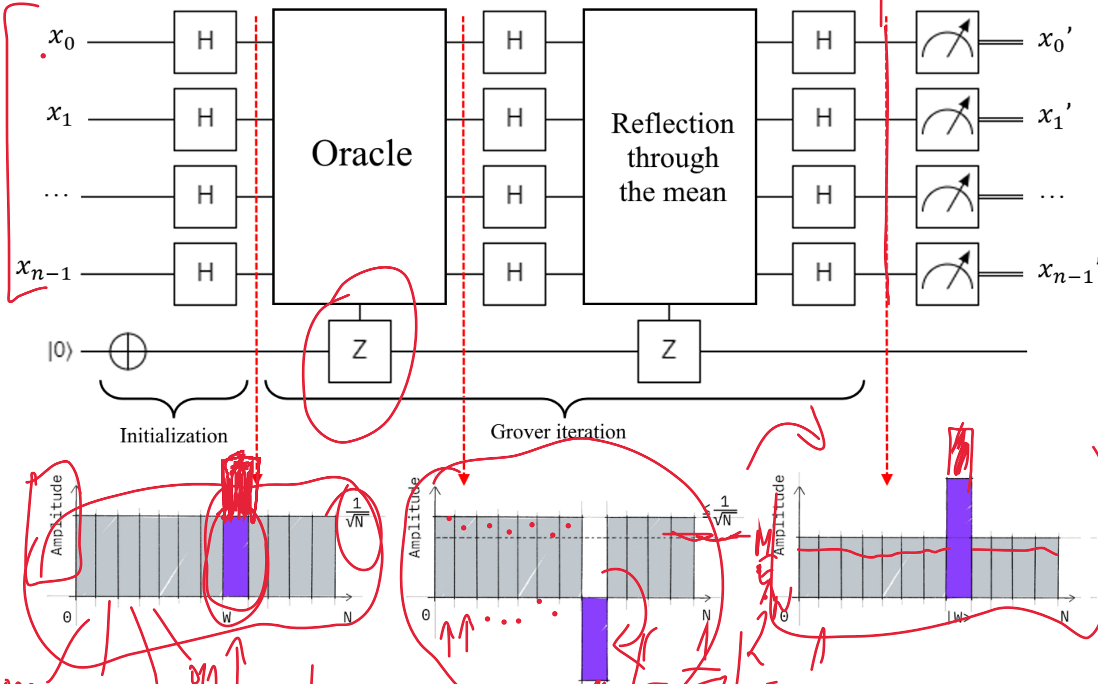
$|0\rangle - |D\rangle - |0\rangle - |D\rangle$

1 ITERATION

DIFFUSER

2it

x



$\frac{1}{N} = \left|\frac{1}{\sqrt{N}}\right|$

000 001 010 011

$x = \left|-\frac{1}{\sqrt{N}}\right| = \frac{1}{N}$

k=1 SECRET CODE

Implementation in Cirq

TOFFOLI GATE

x_0	x_1	f
0	0	–
0	1	–
1	0	–
1	1	X

$\#it = \left\lfloor \frac{\pi}{4 \cdot \arcsin\sqrt{\frac{k}{N}}} \right\rfloor$

CCNOT

CCCNOT

ORACLE – D

m=3

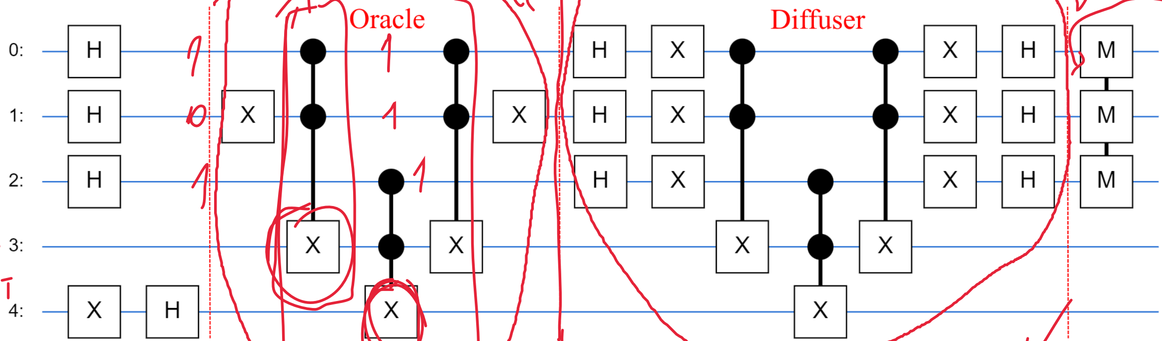
x

ANCILLA QBIT

PHASE QBIT

ORACLE

D



$m/$ H | O – D | O – D | M

1

2

ITERATIONS

Part VII

Quantum Fourier transform

Quantum Fourier transform

INVERSE DISCRETE FT

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

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

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

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

n ... no qubits

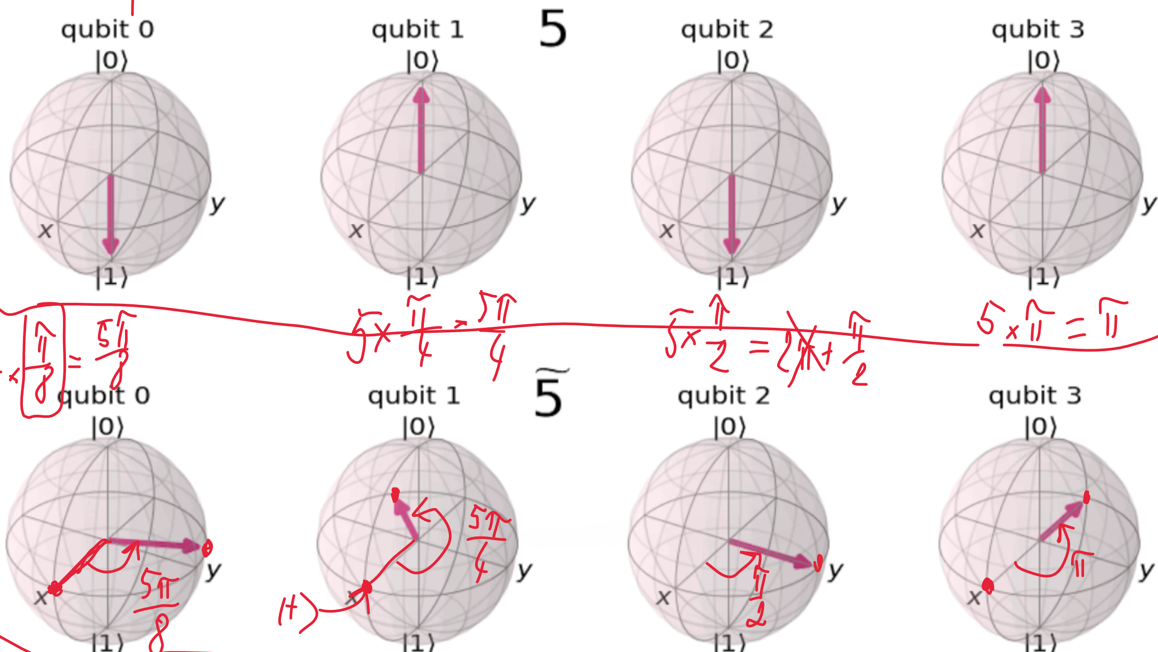
$$\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots$$

$$\text{QFT}\,|x\rangle = \frac{1}{\sqrt{2^n}}\underbrace{\left(|0\rangle + e^{i\pi x}\,|1\rangle\right)}_{q_{n-1}} \otimes \underbrace{\left(|0\rangle + e^{i\frac{\pi}{2}x}\,|1\rangle\right)}_{q_{n-2}} \otimes \underbrace{\left(|0\rangle + e^{i\frac{\pi}{4}x}\,|1\rangle\right)}_{q_{n-3}} \otimes \cdots\cdots \otimes \underbrace{\left(|0\rangle + e^{i\frac{\pi}{2^{n-1}}x}\,|1\rangle\right)}_{q_0}$$

$q_3\, q_2\, q_1\, q_0 = 0101 = 5$

Quantum Fourier transform

1 0 1 0

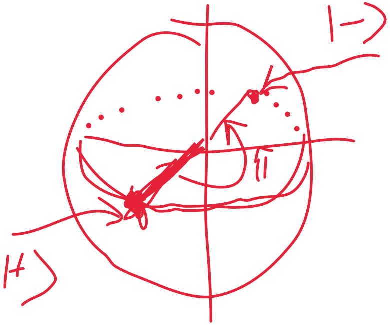


$5 \times \boxed{\frac{\pi}{8}} = \frac{5\pi}{8}$ $\quad 5 \times \frac{\pi}{4} = \frac{5\pi}{4}$ $\quad 5 \times \frac{\pi}{2} = \cancel{2\pi} + \frac{\pi}{2}$ $\quad 5 \times \pi = \pi$

$QFT|5\rangle$

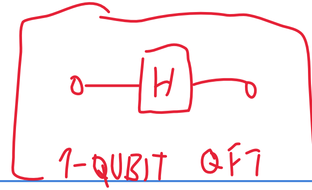
$\frac{5\pi}{8}$ $\quad |+\rangle$ $\quad \frac{5\pi}{4}$ $\quad \frac{\pi}{2}$ $\quad \pi$

Implementation in Cirq



$H|0\rangle \to |+\rangle$

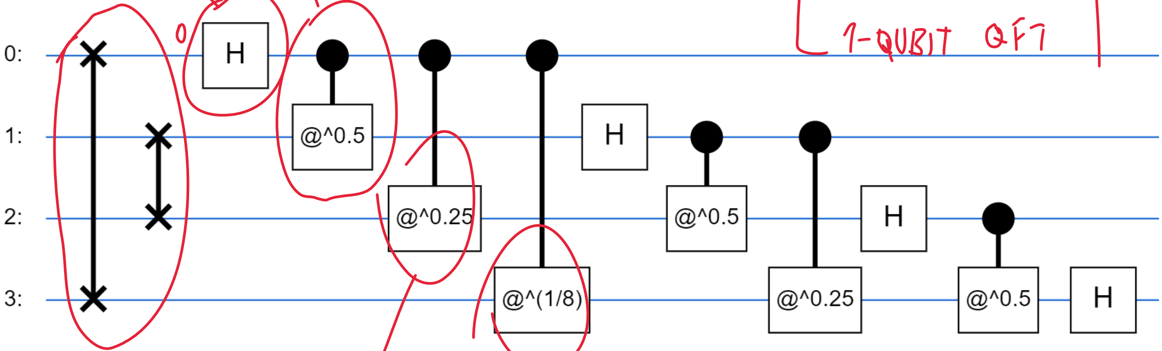
$H|1\rangle \to |-\rangle$



π

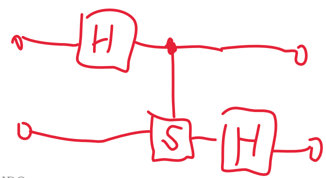
$\frac{\pi}{2}$

Direct QFT:

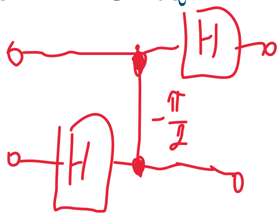


$\frac{\pi}{4}$

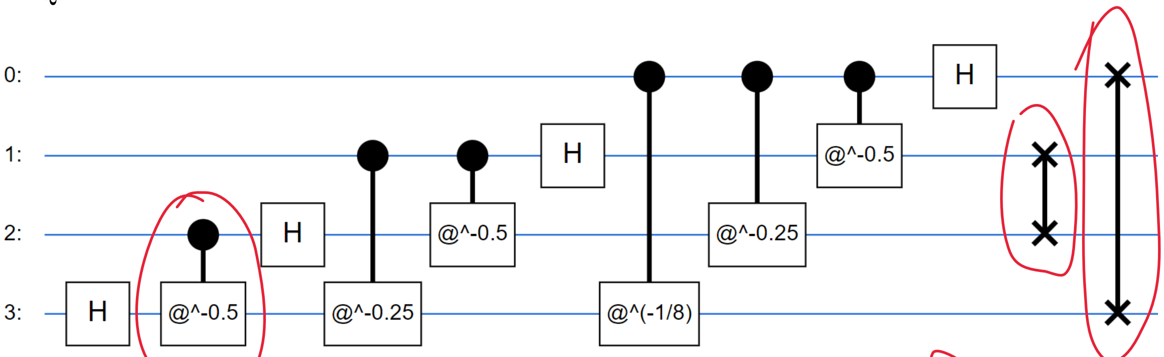
$\frac{\pi}{8}$

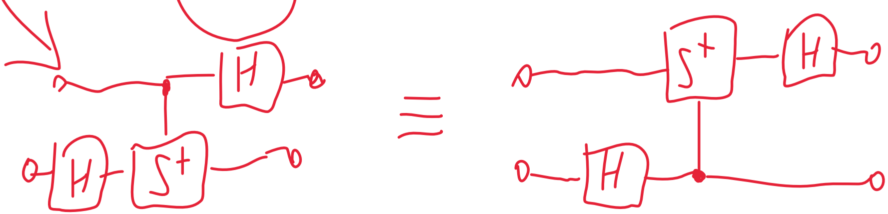


Implementation in Cirq



Inverse QFT:





$$S^{+}\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&\boxed{e^{-i\frac{\pi}{2}}}\end{bmatrix}\begin{bmatrix}\alpha_0\\\alpha_1\\\alpha_2\\\alpha_3\end{bmatrix}=\begin{bmatrix}\alpha_0\\\alpha_1\\\alpha_2\\e^{-i\frac{\pi}{2}}\alpha_3\end{bmatrix}$$

Part VIII

Quantum phase estimation

Quantum phase estimation

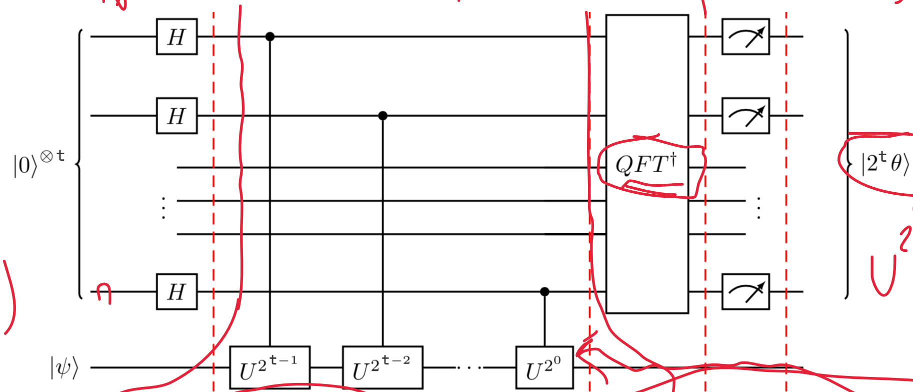
$\Pr(|0\rangle) = |e^{2\pi i\theta}\alpha|^2 = |e^{2\pi i\theta}|^2 |\alpha|^2 = |\alpha|^2$

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:

$e^{2\pi i\theta}(\alpha|0\rangle + \beta|1\rangle)$

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



$U^{2^0} U^{2^0} = e^{2\pi i\theta 2^0 + 2\pi i\theta 2^0} = e^{2\pi i\theta 2^1}$

$U^{2^0} = (e^{2\pi i\theta})^{2^0} = e^{2\pi i\theta 2^0}$

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

$\frac{1}{\sqrt{2^t}}(|0\rangle+|1\rangle)\otimes(|0\rangle+|1\rangle)\otimes(|0\rangle+|1\rangle)\ldots(|0\rangle+|1\rangle)$

Implementation in Cirq

$t=7 \quad 2^7 = 128$

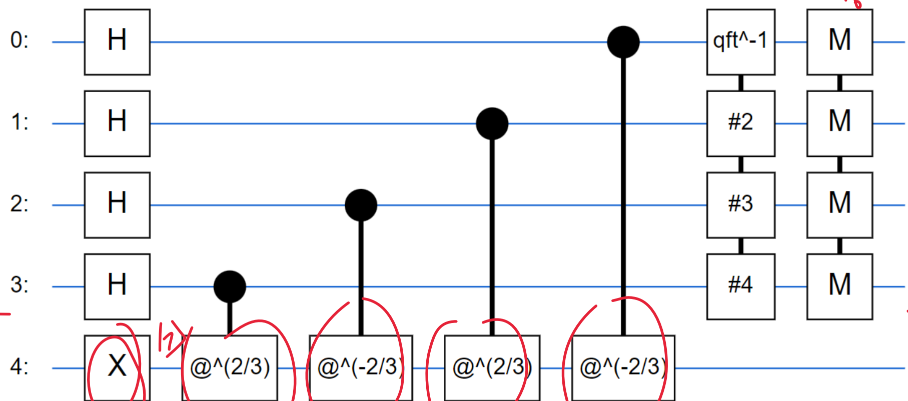
$\theta \cong \frac{11}{128} 2\pi \cong 0{,}156\,\pi \cong \frac{\pi}{7}$

$t=4$

$2^t \theta = 5 \cdot 2\pi = 16\,\theta \qquad \theta \simeq \frac{5}{16} 2\pi \approx \frac{2}{3}\pi$

$2^t \theta = 1 \cdot 2\pi = 16\,\theta \Rightarrow \theta \simeq \frac{2\pi}{16} = \frac{\pi}{8} \sim \frac{\pi}{7}$

$\theta = \frac{2}{16} 2\pi = \frac{1}{4}\pi$



ψ $|1\rangle$

$2^t \theta = 16\,\theta$

$\theta = \frac{2}{3}\pi$

$2^0 \theta = \frac{2}{3}\pi \qquad 2^1 \theta = \frac{4}{3}\pi = -\frac{2}{3}\pi \qquad 2^2 \theta = \frac{8}{3}\pi = \frac{2}{3}\pi \qquad \ldots$

Part IX

FACTORING

Shor's algorithm

Shor's algorithm

$N = P \times R$

gcd GREATEST COMMON DIVISOR

The problem statement:

Find factors P, R of number N.

Shor's algorithm procedure:

$U : a \bmod N$

1. Pick a random integer number a such that: $1 < a < N$.
2. If $\boxed{\gcd(a, N) \neq 1}$ then $\boxed{P = a}$ 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 $P, R = \gcd(a^{r/2} \pm 1, N)$.

$g(y) = (y a) \bmod N$

$g(g(y)) = (y a^2) \bmod N$

x-times

$f(x) = g(g(g(\dots g(1)\dots))) = a^x \bmod N$

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.

$$U^x = U^{(2^3 x_3 + 2^2 x_2 + 2^1 x_1 + 2^0 x_0)} = U^{2^3 x_3} U^{2^2 x_2} U^{2^1 x_1} U^{2^0 x_0}$$

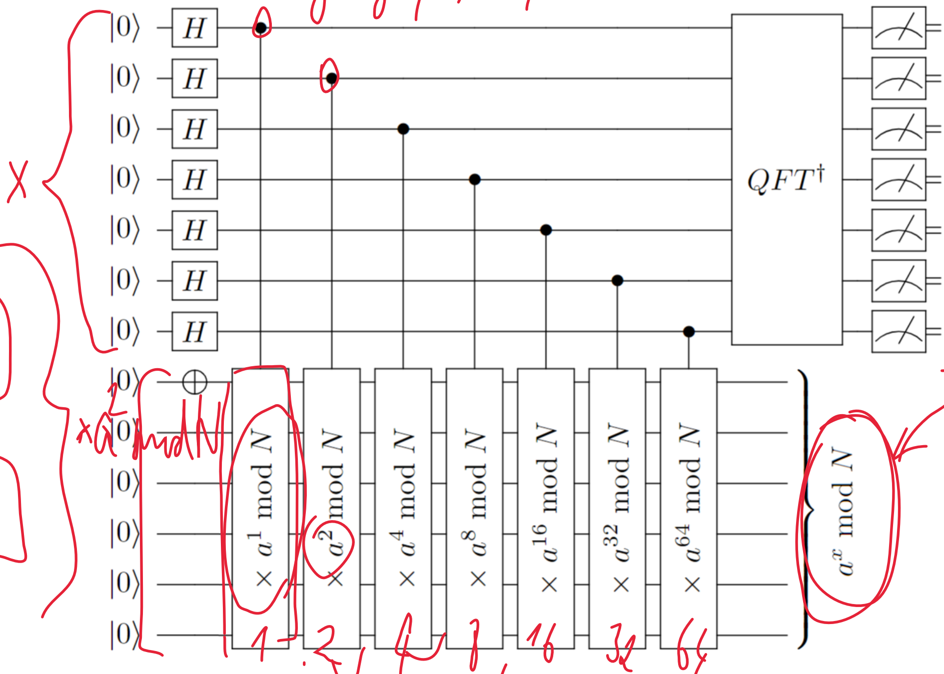
$$|x\rangle = |x_3 x_2 x_1 x_0\rangle = 2^3 x_3 + 2^2 x_2 + 2^1 x_1 + 2^0 x_0 = x$$

Shor's algorithm

$g(y) = (y \cdot a) \bmod N$

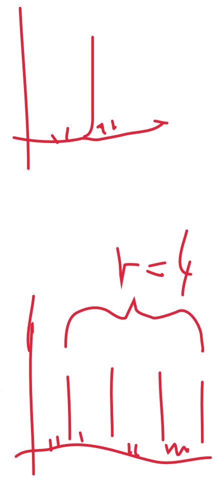
$g(g(y)) = (y\, a^2) \bmod N$

Period-finder circuit:



$\times a^1 \bmod N$

$\times a^1 \bmod N$



$g(1) = 6$ $\boxed{a=6 \quad r=2}$ $g(1) = (1 \times 6) \bmod 35 = 6$ $\times 6^2 \bmod 35$

Implementation in Cirq

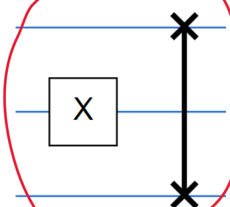
$g(6) = 1$ $p_1, R = \gcd(6^1 \pm 1, 35)$ $g(g(1)) = g(6) = 1$ $g(g(y))$

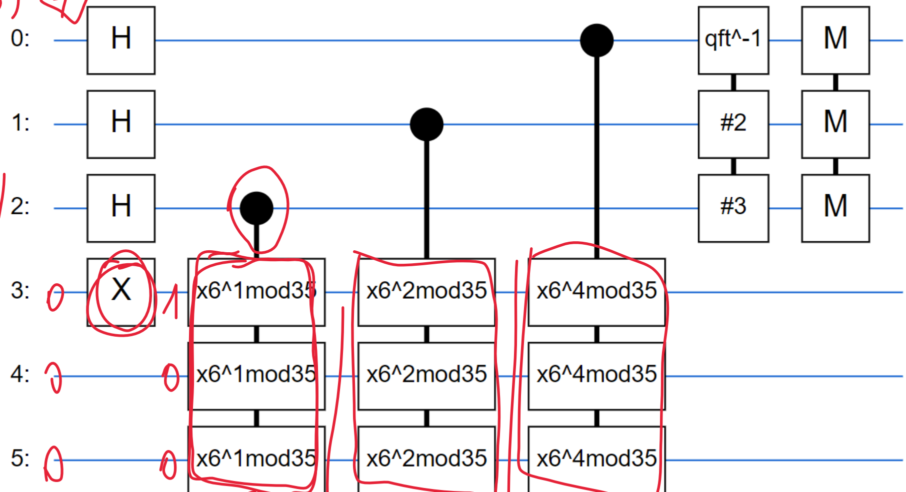
$\gcd(5, 35) = 5$ $g(g(6)) = 6$ $36 \bmod 35 = 1$

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 $f(x) = 6^x \bmod 35$:

$\gcd(7, 35) = 7$

$g(y) = \times 6 \bmod 35$





$\boxed{6}$ 0 1 1 → 1 0 0 $\boxed{1}$

6, 1 6, 1 6, 1