Quantum Basics

Presenter: Changyeol Lee
Department of Computer Science, Yonsei University
Combinatorial Optimization Lab

Complex Number

Complex number. $z = a + bi$ where a and b are real numbers.

- $a = Re(z)$ is the *real part* of z
- $b = Im(z)$ is the *imaginary part* of z
- $z^* \coloneqq a - bi$ is the *conjugate* of z.
- $|z| = \sqrt{Re(z)^2 + Im(z)^2} = \sqrt{a^2 + b^2}$ is the *magnitude* of z.

Complex Number

Let z be a complex number i.e., $|z| = 1$.

Then $\boldsymbol{z = \cos\theta + i\sin\theta}$.

$$\frac{dz}{d\theta} = -\sin\theta + i\cos\theta$$

$$= i\cos\theta + i^2\sin\theta$$

$$= i(\cos\theta + i\sin\theta)$$

$$= iz \quad \Leftrightarrow \frac{dz}{z} = id\theta \quad \Leftrightarrow \int \frac{1}{z}dz = \int id\theta \quad \Leftrightarrow \ln z = i\theta + C$$

$$\Leftrightarrow z = e^{i\theta + C}$$

$z = 1$ when $\theta = 0$

$\therefore \boldsymbol{z = e^{i\theta}}$

Euler's Formula

$$e^{i\theta} = \cos\theta + i\sin\theta$$

for all real θ

Note. $\left|e^{i\theta}\right| = \sqrt{\cos^2\theta + \sin^2\theta} = 1.$

Qubits and Gates

Presented by Changyeol Lee

Qubit

The *Qubit* (short for *quantum bit*). $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
where α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$.

α and β are the (probability) amplitude for the state $|0\rangle$ and $|1\rangle$ respectively.

Let a $\coloneqq |\alpha|$ and $b \coloneqq |\beta|$.

Using Euler's formula, $\alpha = a \cdot e^{i\phi_1}$ and $\beta = b \cdot e^{i\phi_2}$ for some $\phi_1, \phi_2 \in \mathbb{R}$.

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} a \cdot e^{i\phi_1} \\ b \cdot e^{i\phi_2} \end{pmatrix}$$

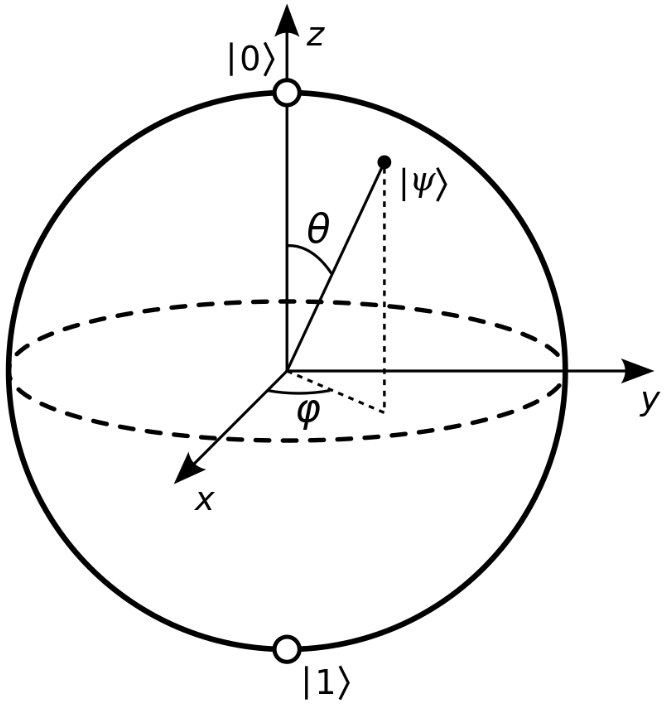
Multiply by the unit scalar $e^{i\phi}$ where $\phi \coloneqq (\phi_1 - \phi_2)/2$.

$$|\psi\rangle = \begin{pmatrix} a \cdot e^{i\phi} \\ b \cdot e^{-i\phi} \end{pmatrix}$$

Qubit

$a = \cos\frac{\theta}{2}$ and $b = \sin\frac{\theta}{2}$ for some θ since $a^2 + b^2 = 1$.

$$|\psi\rangle = \begin{pmatrix} \cos\frac{\theta}{2} \cdot e^{i\phi} \\ \sin\frac{\theta}{2} \cdot e^{-i\phi} \end{pmatrix}$$



Turns out to be…

$$\begin{pmatrix} 1 \\ \theta \\ \phi \end{pmatrix} \in \text{Bloch sphere} \leftrightarrow |\psi\rangle = \begin{pmatrix} \cos\frac{\theta}{2} \cdot e^{i\phi} \\ \sin\frac{\theta}{2} \cdot e^{-i\phi} \end{pmatrix}$$

Unitary matrix

Unitary Matrix. The matrix U is unitary if $UU^\dagger = U^\dagger U = I$ where $U^\dagger$ is the *conjugate transpose* of U.

- $U^\dagger \coloneqq U^{*T}$ is sometimes called Hermitian *conjugate matrix* or *adjoint matrix*.

Every quantum gate must be unitary.

Each unitary matrix is a possible quantum gate.

$$U_1(\lambda) = \begin{pmatrix} 1 & 0 \\ 0 & -e^{i\lambda} \end{pmatrix}$$

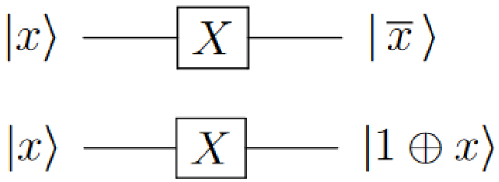
$$U_2(\lambda, \phi) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -e^{i\lambda} \\ e^{i\phi} & -e^{i(\lambda+\phi)} \end{pmatrix}$$

$$U_3(\lambda, \phi, \theta) = \begin{pmatrix} \cos\theta/2 & -e^{i\lambda}\sin\theta/2 \\ e^{i\phi}\sin\theta/2 & -e^{i(\lambda+\phi)}\cos\theta/2 \end{pmatrix}$$

One Qubit Gate

$X = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

- $\alpha|0\rangle + \beta|1\rangle \longrightarrow \boldsymbol{\beta}|0\rangle + \boldsymbol{\alpha}|1\rangle$
- "bit flip" operator



Apply only to the binary values.
For general states, extend linearly.

One Qubit Gate

$Z = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

- $\alpha|0\rangle + \beta|1\rangle \longrightarrow \boldsymbol{\alpha}|0\rangle + (\boldsymbol{-\beta})|1\rangle$
- “phase flip” operator

$P \text{ or } R_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$

- “phase shift” operator
- $Z = P_\pi$
- $S = \sqrt{Z} = P_{\pi/2} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$

One Qubit Gate

$Y = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$

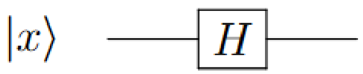
- $\alpha|0\rangle + \beta|1\rangle \longrightarrow (-i\boldsymbol{\beta})|0\rangle + \boldsymbol{i\alpha}|1\rangle \cong \boldsymbol{\beta}|0\rangle - \boldsymbol{\alpha}|1\rangle$

- “bit-and-phase flip” operator

One Qubit Gate

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- $\alpha|0\rangle + \beta|1\rangle \longrightarrow \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle$



$$\frac{|0\rangle + (-1)^x |1\rangle}{\sqrt{2}}$$

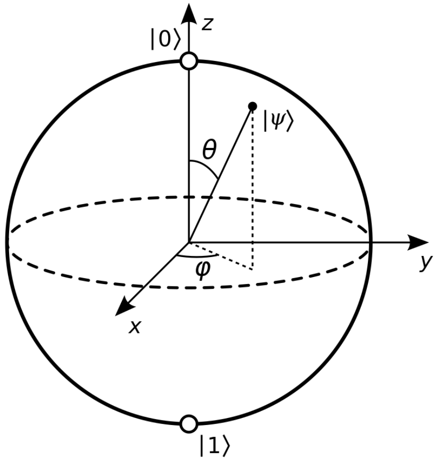
$$H : |0\rangle \longmapsto |0\rangle_x$$
$$H : |1\rangle \longmapsto |1\rangle_x$$

One Qubit Gate

$$R_A(\theta) = e^{-\frac{i\theta A}{2}} \text{ or } \exp\left(-\frac{i\theta A}{2}\right) = \cos(\theta/2)\, I - i\sin(\theta/2)\, A$$

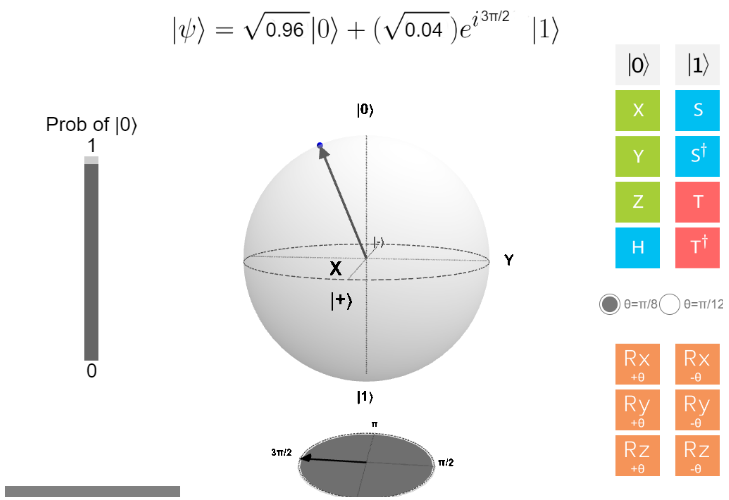
where $A \in \{X, Y, Z\}$

- rotation around A-axis



e.g.,

$$R_x(\theta) = \exp\left(-\frac{i\theta X}{2}\right) = \exp\left(-\frac{i\theta}{2}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) = \begin{pmatrix} \cos\theta/2 & -i\sin\theta/2 \\ -i\sin\theta/2 & \cos\theta/2 \end{pmatrix}$$



Multi Qubits

"Ket ψ_1 ψ_2" or "Ket ψ_1 (tensor) Ket ψ_2"

$$|\psi_1\psi_2\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} \otimes \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ \beta_1\beta_2 \end{pmatrix} = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle$$

Multi-Qubit Gate

$$A \otimes B = \begin{pmatrix} A_{00}\begin{pmatrix} B_{00} & B_{01} \\ B_{10} & B_{11} \end{pmatrix} & A_{01}\begin{pmatrix} B_{00} & B_{01} \\ B_{10} & B_{11} \end{pmatrix} \\ A_{01}\begin{pmatrix} B_{00} & B_{01} \\ B_{10} & B_{11} \end{pmatrix} & A_{11}\begin{pmatrix} B_{00} & B_{01} \\ B_{10} & B_{11} \end{pmatrix} \end{pmatrix}$$

$$A \otimes B \, |\psi_1 \psi_2\rangle = A|\psi_1\rangle \otimes B|\psi_2\rangle$$

Multi-Qubit Gate

Controlled-X (when control bit is q[0]). $CX = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

Controlled-H (when control bit is q[1]). $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1/\sqrt{2} & 0 & 1/\sqrt{2} \\ 0 & 0 & 1 & 0 \\ 0 & 1/\sqrt{2} & 0 & -1/\sqrt{2} \end{pmatrix}$

Swap. $\mathrm{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

Multi-Qubit Gate

Controlled-X (when control bit is q[0]). $CX = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

Controlled-H (when control bit is q[1]). $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1/\sqrt{2} & 0 & 1/\sqrt{2} \\ 0 & 0 & 1 & 0 \\ 0 & 1/\sqrt{2} & 0 & -1/\sqrt{2} \end{pmatrix}$

Swap. $\mathrm{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

Multi-Qubit Gate

$(H \otimes H \otimes \cdots \otimes H)|\psi\rangle^n = H^{\otimes n}|\psi\rangle^n$

$= H^{\otimes n}(a_0|0\rangle^n + a_1|1\rangle^n + \cdots + a_{2^n-1}|2^n - 1\rangle^n)$

$$H^{\otimes n}|x\rangle^n = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} (-1)^{x \odot y}|y\rangle^n$$

where $\odot$ is the mod-2 dot product, i.e.,

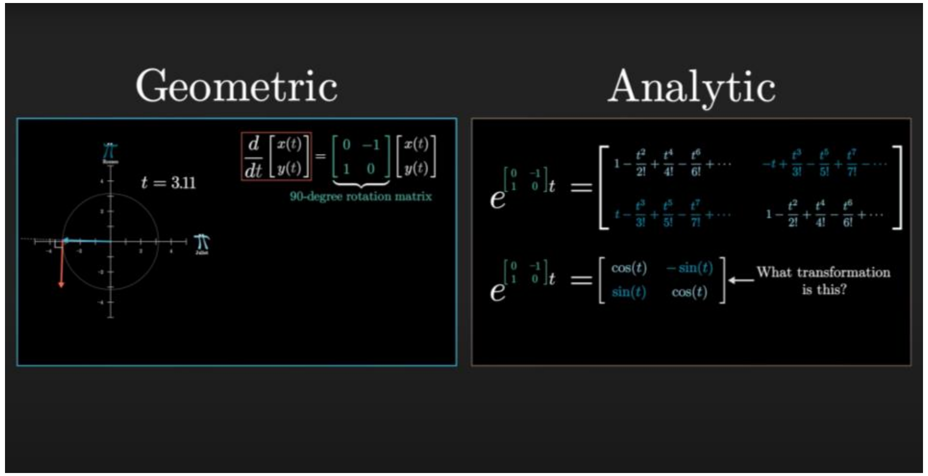
$$x \odot y = x_{n-1}y_{n-1} \oplus x_{n-2}y_{n-2} \oplus \cdots \oplus x_0 y_0$$

Useful References

Michael Locef. A Course in Quantum Computing.

https://lapastillaroja.net/wp-content/uploads/2016/09/Intro_to_QC_Vol_1_Loceff.pdf

3Blue1Brown. How (and why) to raise e to the power of a matrix.



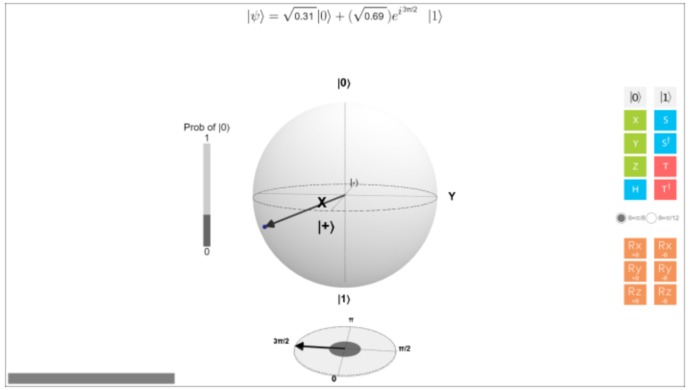
https://youtu.be/O85OWBJ2ayo?si=bNf0Jq-G-zo0Hc2X

Qiskit. Summary of Quantum Operations.

https://qiskit.org/documentation/tutorials/circuits/3_summary_of_quantum_operations.html

javafxpert. Grokking the Bloch Sphere.

https://javafxpert.github.io/grok-bloch/



Quantum Oracle

Presented by Changyeol Lee

Quantum Oracle

Given $f:\{0,1\}^n \to \{0,1\}^m$ (or $f:\mathbb{Z}_{2^n} \to \mathbb{Z}_{2^m}$), the **oracle $\boldsymbol{U_f}$** is the following:

$$|\boldsymbol{x}\rangle^{\boldsymbol{n}}|\boldsymbol{y}\rangle^{\boldsymbol{m}} \xrightarrow{\boldsymbol{U_f}} |\boldsymbol{x}\rangle^{\boldsymbol{n}}|\boldsymbol{f}(\boldsymbol{x}) \oplus \boldsymbol{y}\rangle^{\boldsymbol{m}}$$

where bit-wise mod-2 sum operator, i.e., $|f(x) \oplus y\rangle^m = |f(\mathrm{x})_{m-1} \oplus y_{m-1}\rangle \cdots |f(\mathrm{x})_0 \oplus y_0\rangle$.

E.g., $|01 \oplus 11\rangle = |10\rangle$

U_f is unitary and thus it is a valid quantum gate.

Bernstein-Vazirani

Presented by Changyeol Lee

Bernstein-Vazirani Problem

Given an unknown unary function $f: \{0,1\}^n \to \{0,1\}$

that are known to be an n (binary) digit constant a

such that $f(x) = a \odot x$ for all $x \in \{0,1\}^n$,

find a in one query of U_f.

With less than n queries, it is forced to guess at least one coordinate of a.

-> wrong with prob. at least 0.5

Classically, need linear queries.

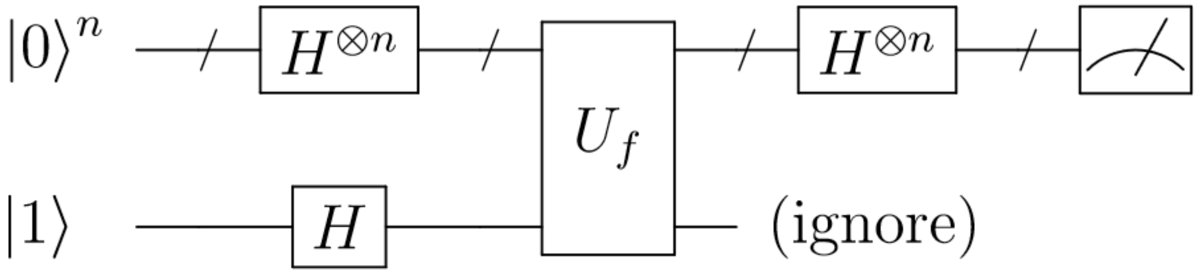
Bernstein-Vazirani Problem

Given an unknown unary function $f\colon \{0,1\}^n \to \{0,1\}$

that are known to be an n (binary) digit constant a

such that $f(x) = a \odot x$ for all $x \in \{0,1\}^n$,

find a in one query of U_f.

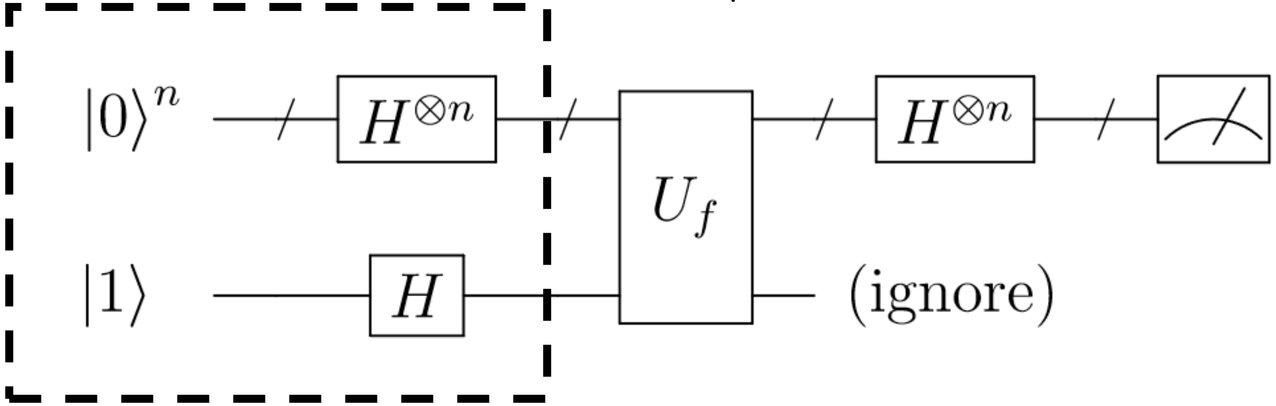


Analysis

$$H^{\otimes n}|x\rangle^n = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} (-1)^{x\odot y}|y\rangle^n$$

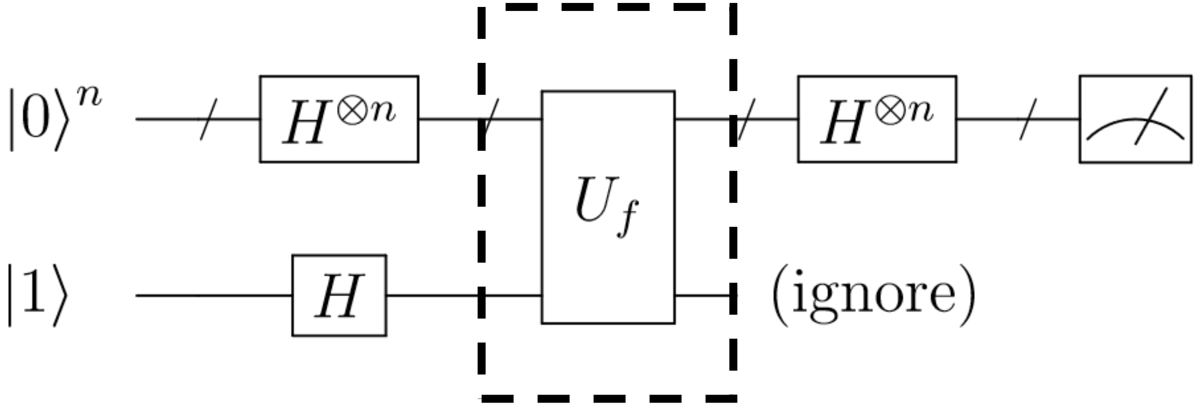
$$H^{\otimes n}|0\rangle^n = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} (-1)^{0\odot y}|y\rangle^n = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} |y\rangle^n$$

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



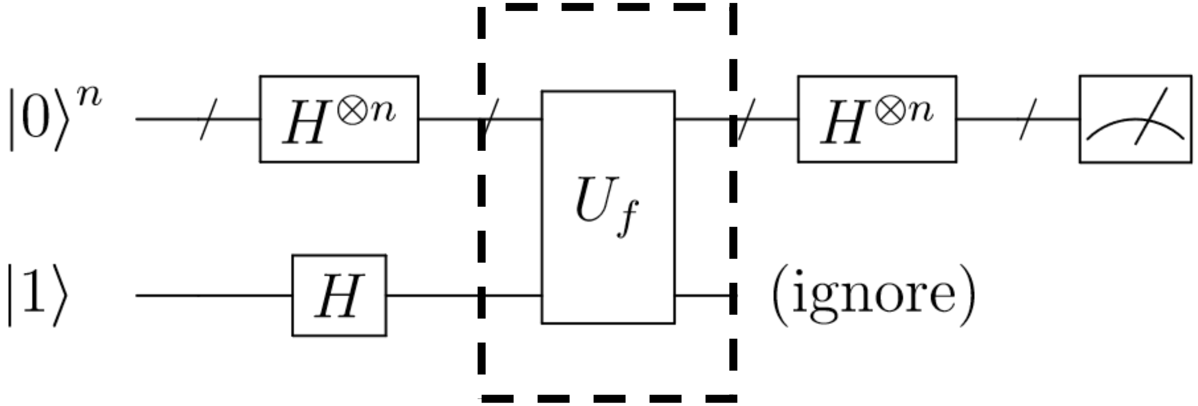
Analysis

$$U_f\left(\left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} |y\rangle^n \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$



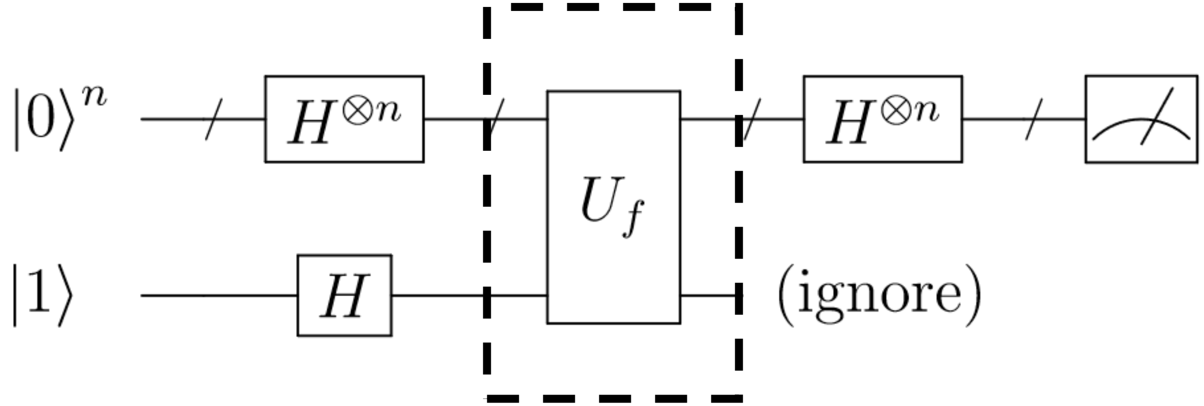
Analysis

$$U_f\left(\left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} |y\rangle^n \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} U_f\left(|y\rangle^n \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$



Analysis

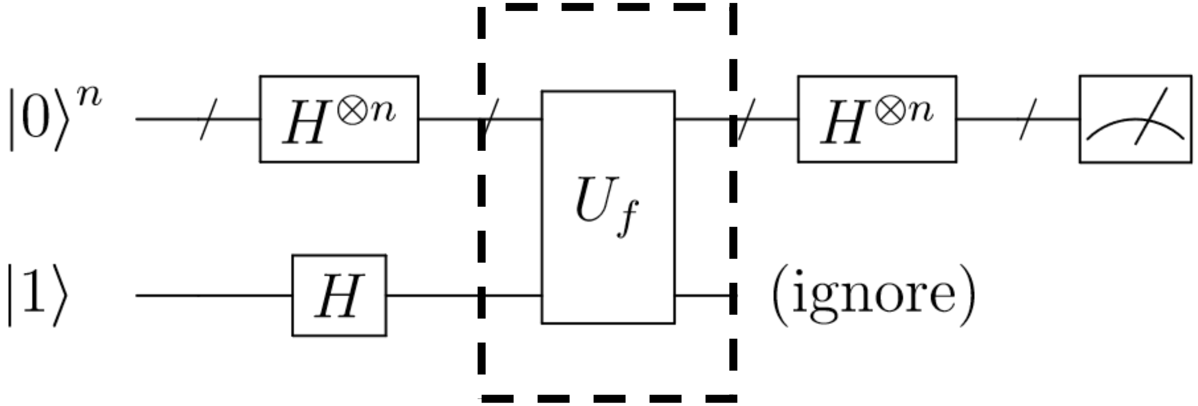
$$U_f\left(\left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} |y\rangle^n \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} U_f\left(|y\rangle^n \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} |y\rangle^n \otimes \frac{|f(y)\rangle - |\neg f(y)\rangle}{\sqrt{2}}$$



$$|y\rangle^n \otimes \frac{|f(y)\rangle - |\neg f(y)\rangle}{\sqrt{2}} =$$

Analysis

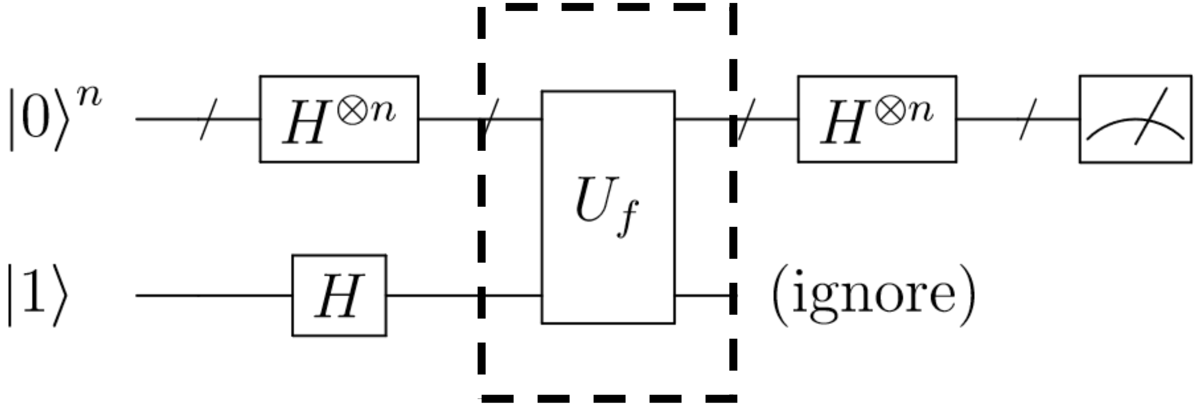
$$U_f\left(\left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} |y\rangle^n \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} U_f\left(|y\rangle^n \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} |y\rangle^n \otimes \frac{|f(y)\rangle - |\neg f(y)\rangle}{\sqrt{2}}$$



$$|y\rangle^n \otimes \frac{|f(y)\rangle - |\neg f(y)\rangle}{\sqrt{2}} = \begin{cases} |y\rangle^n \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}, & f(y) = 0 \\ |y\rangle^n \otimes \frac{|1\rangle - |0\rangle}{\sqrt{2}}, & f(y) = 1 \end{cases}$$

Analysis

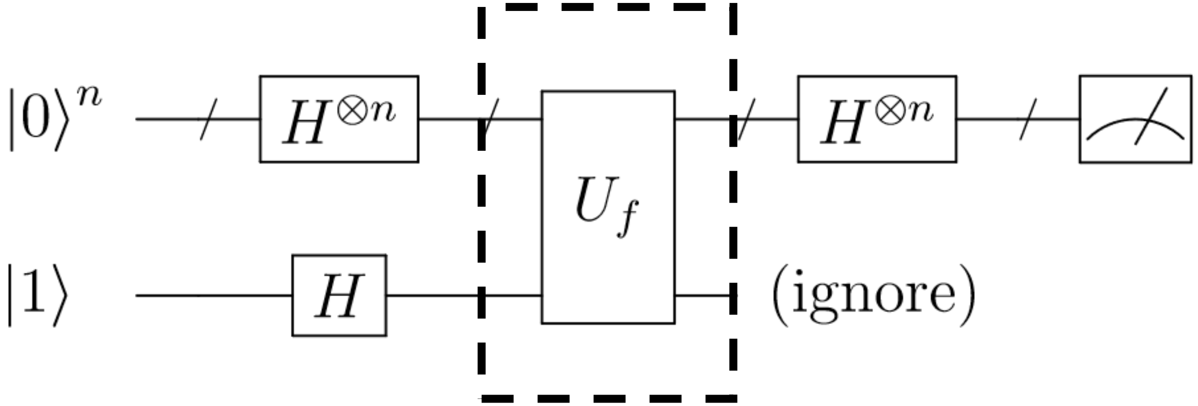
$$U_f\left(\left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} |y\rangle^n \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} U_f\left(|y\rangle^n \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} |y\rangle^n \otimes \frac{|f(y)\rangle - |\neg f(y)\rangle}{\sqrt{2}}$$



$$|y\rangle^n \otimes \frac{|f(y)\rangle - |\neg f(y)\rangle}{\sqrt{2}} = (-1)^{f(y)}|y\rangle^n \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Analysis

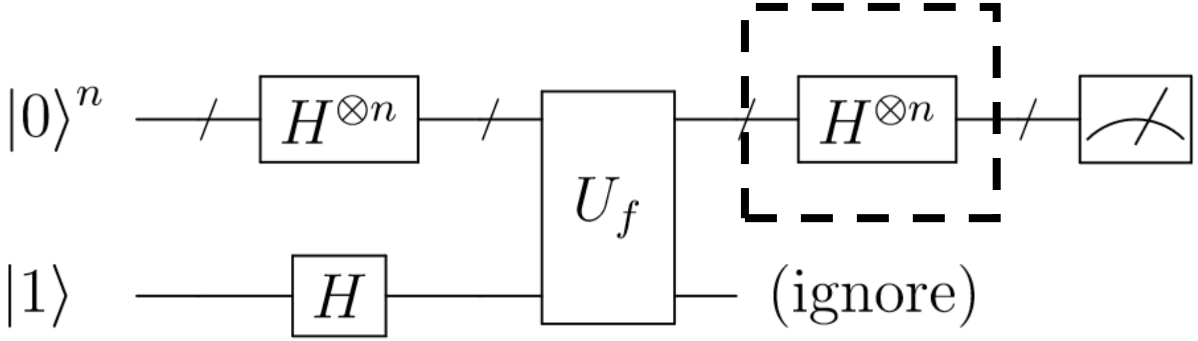
$$U_f\left(\left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} |y\rangle^n \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} U_f\left(|y\rangle^n \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} |y\rangle^n \otimes \frac{|f(y)\rangle - |\neg f(y)\rangle}{\sqrt{2}}$$



$$|y\rangle^n \otimes \frac{|f(y)\rangle - |\neg f(y)\rangle}{\sqrt{2}} = (-1)^{a \odot y} |y\rangle^n \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Analysis

$$H^{\otimes n}\left(\left(\frac{1}{\sqrt{2}}\right)^{n}\sum_{y=0}^{2^n-1}(-1)^{a\odot y}|y\rangle^{n}\right)$$

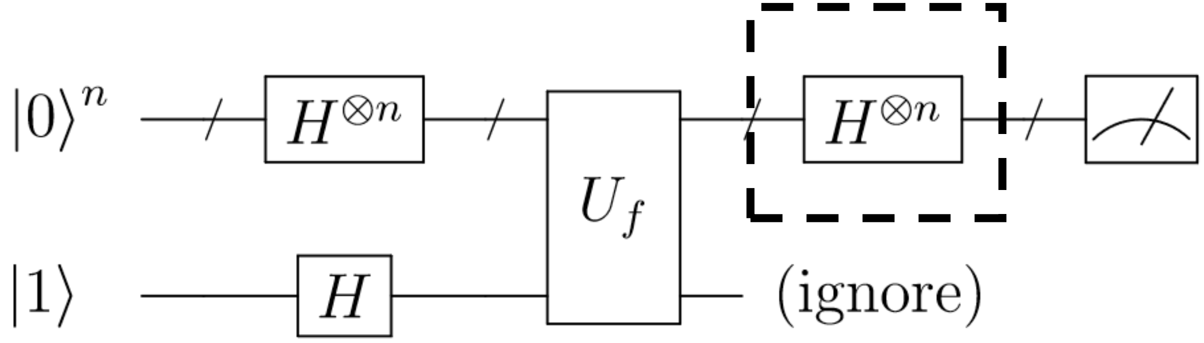


$$|y\rangle^{n}\otimes\frac{|f(y)\rangle-|\neg f(y)\rangle}{\sqrt{2}} = (-1)^{a\odot y}|y\rangle^{n}\otimes\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

Analysis

$$H^{\otimes n}|y\rangle^n = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{z=0}^{2^n-1} (-1)^{y\odot z}|z\rangle^n$$

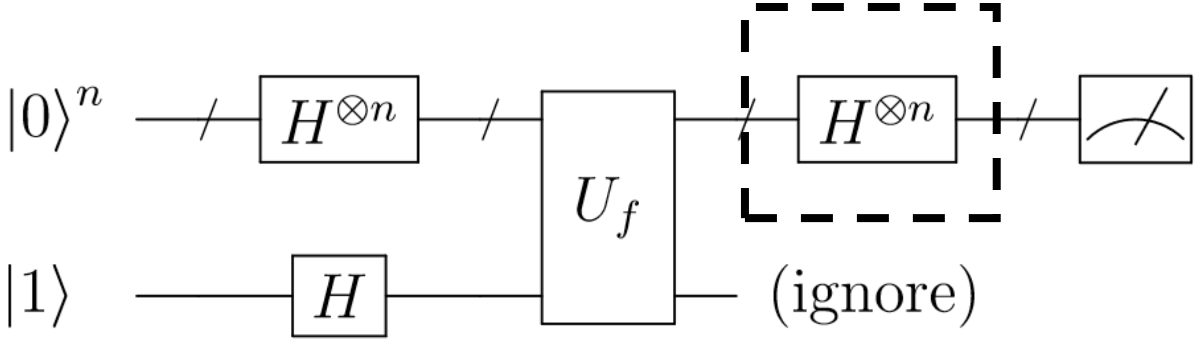
$$H^{\otimes n}\left(\left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} (-1)^{a\odot y}|y\rangle^n\right) = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} H^{\otimes n}\left((-1)^{a\odot y}|y\rangle^n\right)$$



Analysis

$$H^{\otimes n}|y\rangle^n = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{z=0}^{2^n-1} (-1)^{y\odot z}|z\rangle^n$$

$$H^{\otimes n}\left(\left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} (-1)^{a\odot y}|y\rangle^n\right) = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} H^{\otimes n}\left((-1)^{a\odot y}|y\rangle^n\right) = \frac{1}{2^n}\sum_{y=0}^{2^n-1}(-1)^{a\odot y}\sum_{z=0}^{2^n-1}(-1)^{y\odot z}|z\rangle^n$$

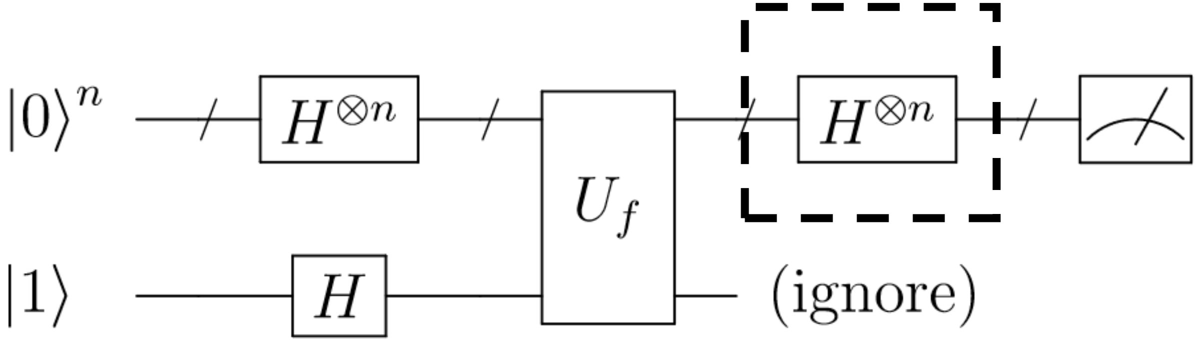


Analysis

$$H^{\otimes n}|y\rangle^n = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{z=0}^{2^n-1} (-1)^{y\odot z}|z\rangle^n$$

$$H^{\otimes n}\left(\left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} (-1)^{a\odot y}|y\rangle^n\right) = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} H^{\otimes n}\left((-1)^{a\odot y}|y\rangle^n\right) = \frac{1}{2^n}\sum_{z=0}^{2^n-1}\sum_{y=0}^{2^n-1}(-1)^{a\odot y}(-1)^{y\odot z}|z\rangle^n$$

$G(z)$



Analysis

$$H^{\otimes n}|y\rangle^n = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{z=0}^{2^n-1} (-1)^{y\odot z}|z\rangle^n$$

$$H^{\otimes n}\left(\left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} (-1)^{a\odot y}|y\rangle^n\right) = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} H^{\otimes n}\left((-1)^{a\odot y}|y\rangle^n\right) = \frac{1}{2^n}\sum_{z=0}^{2^n-1}\underbrace{\sum_{y=0}^{2^n-1}(-1)^{a\odot y}(-1)^{y\odot z}}_{G(z)}|z\rangle^n$$

Consider when $z = a$.

$$G(a) = \sum_{y=0}^{2^n-1} (-1)^{a\odot y}(-1)^{y\odot a}$$

Analysis

$$H^{\otimes n}|y\rangle^n = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{z=0}^{2^n-1} (-1)^{y \odot z} |z\rangle^n$$

$$H^{\otimes n}\left(\left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} (-1)^{a \odot y} |y\rangle^n\right) = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} H^{\otimes n}\left((-1)^{a \odot y} |y\rangle^n\right) = \frac{1}{2^n} \sum_{z=0}^{2^n-1} \underbrace{\sum_{y=0}^{2^n-1} (-1)^{a \odot y} (-1)^{y \odot z}}_{G(z)} |z\rangle^n$$

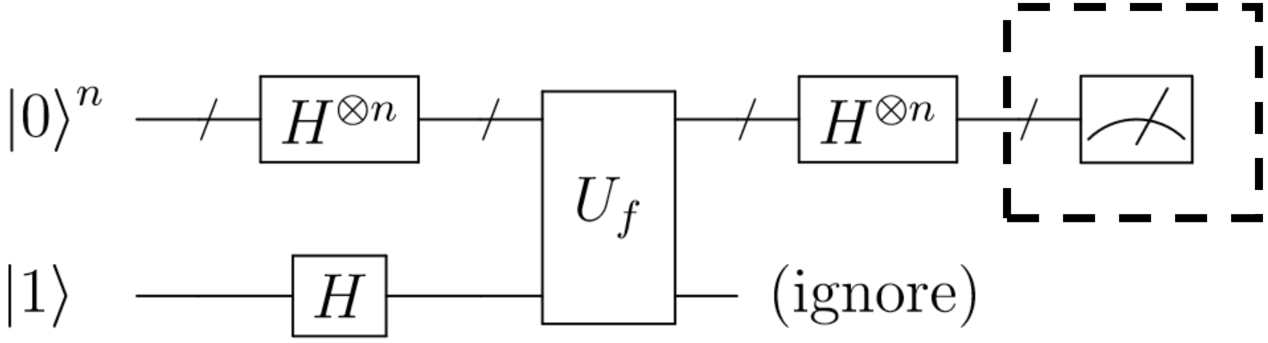
Consider when $z = a$.

$$G(a) = \sum_{y=0}^{2^n-1} (-1)^{a \odot y} (-1)^{y \odot a} = \sum_{y=0}^{2^n-1} 1 = 2^n,$$

which means that the amplitude of $|a\rangle$ is 1.

Analysis

Observe a with probability 1.



Grover's Algorithm

Presented by Changyeol Lee

Problem

Given a function $f(\mathrm{x})\colon \{0,1\}^n \rightarrow \{0,1\}$, find an n-bit target string x^* such that $f(\mathrm{x}^*) = 1$

(where #targets is known).

Let $N = 2^n$.

Requires $O(N)$ function calls in the classical model.

Grover's Algorithm. Requires $\Theta(\sqrt{N})$ calls to the quantum oracle.

Grover operator G

Defn (Uniform superposition state).

$$|\psi\rangle := \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle^n$$

$$|\psi\rangle\langle\psi| = \frac{1}{N} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 1 & 1 & \cdots & 1 \\ 1 & 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \cdots & 1 \end{pmatrix}$$

Defn (Grover operator).

$$G := \big((2|\psi\rangle\langle\psi| - I_N) \otimes I_2\big) U_f$$

$$I_N = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$2|\psi\rangle\langle\psi| - I_N$ on an arbitrary state $|\phi\rangle^n = \sum_i a_i |i\rangle^n$

$$(2|\psi\rangle\langle\psi| - I_N)|\phi\rangle^n = \sum_i \left(2\frac{a_0 + \cdots + a_{N-1}}{N} - a_i\right)|i\rangle^n$$

Grover's Algorithm

Step 1. Perform state initialization

- (n qubits) $|00\cdots0\rangle \longrightarrow |\psi\rangle$

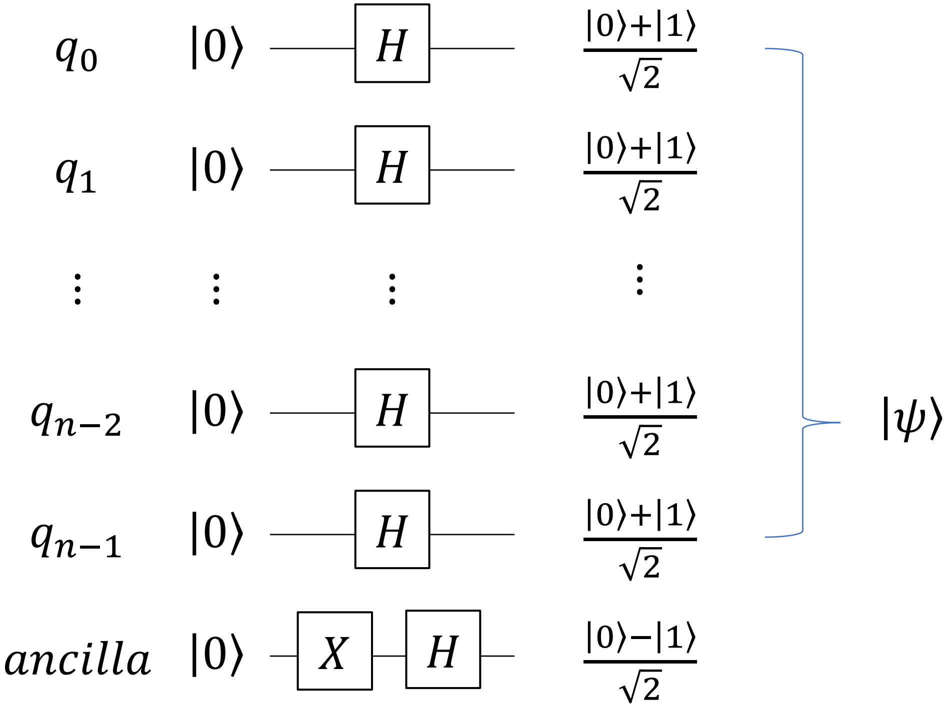
- (ancillary qubit) $|0\rangle \longrightarrow \frac{|0\rangle-|1\rangle}{\sqrt{2}}$

Step 2. Apply Grover operator $\left\lfloor\frac{\pi\sqrt{N}}{4}\right\rfloor$ times

Step 3. Perform measurement on all qubit (except the ancillary qubit)

Grover's Algorithm

Step 1. Initialization



$$|\psi\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Grover's Algorithm

Step 2. Apply $G \coloneqq \big((2|\psi\rangle\langle\psi| - I_N) \otimes I_2\big)U_f$

$|\mathrm{x}\rangle^n|q\rangle \longrightarrow |\mathrm{x}\rangle^n|f(\mathrm{x}) \oplus q\rangle$

$$U_f\left(\frac{1}{\sqrt{N}}(|00\cdots00\rangle + |00\cdots01\rangle + \cdots + |\mathbf{x}^*\rangle + \cdots + |11\cdots11\rangle) \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$$= \frac{1}{\sqrt{N}}(|00\cdots00\rangle + |00\cdots01\rangle + \cdots + (-\mathbf{1})|\mathrm{x}^*\rangle + \cdots + |11\cdots11\rangle) \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Grover's Algorithm

Step 2. Apply $G := \left((2|\psi\rangle\langle\psi| - I_N) \otimes I_2\right)U_f$

$$(2|\psi\rangle\langle\psi| - I_N)|\phi\rangle^n = \sum_i \left(\frac{2}{N}(a_0 + \cdots + a_{N-1}) - a_i\right)|i\rangle^n$$

$$(2|\psi\rangle\langle\psi| - I_N)\left(\frac{1}{\sqrt{N}}(|00\cdots00\rangle + |00\cdots01\rangle + \cdots + (-1)|x^*\rangle + \cdots + |11\cdots11\rangle)\right)$$

$$= \frac{1}{\sqrt{N}}\left(\frac{N-4}{N}|00\cdots00\rangle + \cdots + \frac{3N-4}{N}|x^*\rangle + \cdots + \frac{N-4}{N}|11\cdots11\rangle\right)$$

amplified

Grover's Algorithm

Step 2. Apply $G \coloneqq ((2|\psi\rangle\langle\psi| - I_N) \otimes I_2)U_f$ again

$$|\mathrm{x}\rangle^n|q\rangle \longrightarrow |\mathrm{x}\rangle^n|f(\mathrm{x}) \oplus q\rangle$$

$$U_f\left(\frac{1}{\sqrt{N}}\left(\frac{N-4}{N}|00\cdots00\rangle + \cdots + \frac{3N-4}{N}|\mathrm{x}^*\rangle + \cdots + \frac{N-4}{N}|11\cdots11\rangle\right) \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$$= \frac{1}{\sqrt{N}}\left(\frac{N-4}{N}|00\cdots00\rangle + \cdots + (-1)\frac{3N-4}{N}|\mathrm{x}^*\rangle + \cdots + \frac{N-4}{N}|11\cdots11\rangle\right) \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

flipped

Grover's Algorithm

Step 2. Apply $G := \left((2|\psi\rangle\langle\psi| - I_N) \otimes I_2\right)U_f$ again

$$(2|\psi\rangle\langle\psi| - I_N)|\phi\rangle^n = \sum_i \left(\frac{2}{N}(a_0 + \cdots + a_{N-1}) - a_i\right)|i\rangle^n$$

$$(2|\psi\rangle\langle\psi| - I_N)\left(\frac{1}{\sqrt{N}}\left(\frac{N-4}{N}|00\cdots00\rangle + \cdots + (-1)\frac{3N-4}{N}|\mathrm{x}^*\rangle + \cdots + \frac{N-4}{N}|11\cdots11\rangle\right)\right)$$

$$= \frac{1}{\sqrt{N}}\left(\frac{N^2-12N+16}{N^2}|00\cdots00\rangle + \cdots + \frac{5N^2-20N+16}{N^2}|\mathrm{x}^*\rangle + \cdots + \frac{N^2-12N+16}{N^2}|11\cdots11\rangle\right)$$

more amplified

Grover's Algorithm

Step 2. Apply G **fixed amount**

$$\text{(informally)} \quad \frac{1}{\sqrt{N}}\left(\epsilon|00\cdots00\rangle + \cdots + \underbrace{\left(\sqrt{N}-\epsilon'\right)}_{\text{amplified a lot}}|\mathrm{x}^*\rangle + \cdots + \epsilon|11\cdots11\rangle\right)$$

for some small ϵ, ϵ'.

Grover’s Algorithm

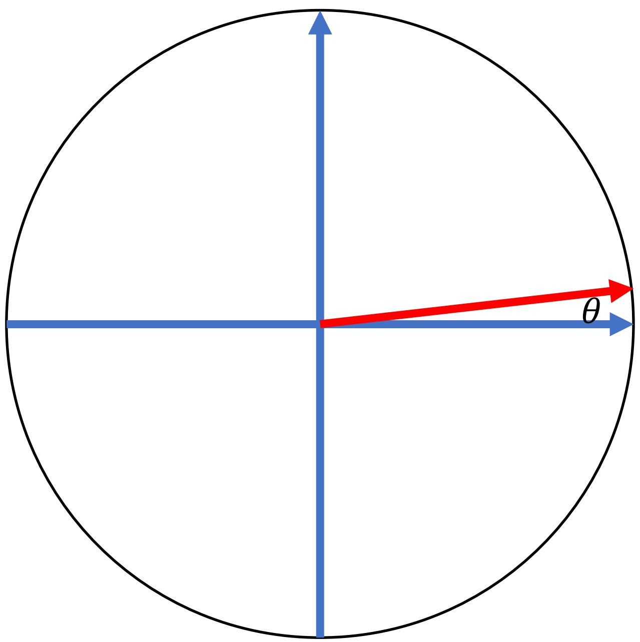
Step 3. Measurement

$$\text{(informally)} \quad \frac{1}{\sqrt{N}}\left(\epsilon|00\cdots00\rangle+\cdots+\left(\sqrt{N}-\epsilon'\right)|\mathrm{x}^*\rangle+\cdots+\epsilon|11\cdots11\rangle\right)$$

Obtain $|x^*\rangle$ with probability close to 1.

Geometric Analysis

Why applying Grover operator (exactly) $\left\lceil \frac{\pi\sqrt{N}}{4} \right\rceil$ times?



Let $|\omega\rangle = \frac{1}{\sqrt{N-1}}(\sum_i |i\rangle^n - |x^*\rangle)$

Note. $|\omega\rangle$ and $|x^*\rangle$ are orthonormal.

Note. After the step 1, the state is

$$\frac{1}{\sqrt{N}}(|00\cdots 00\rangle + |00\cdots 01\rangle + |00\cdots 10\rangle + \cdots + |11\cdots 1\rangle)$$

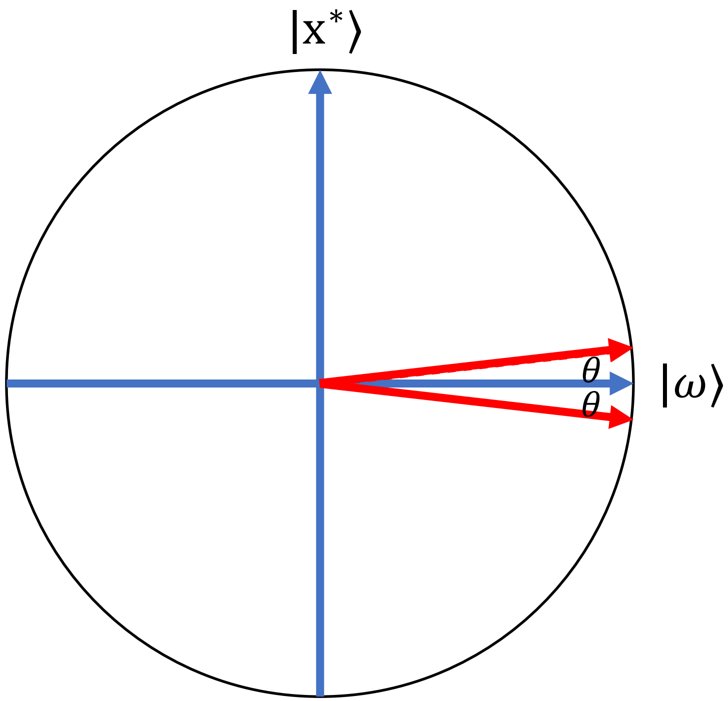
$$= \frac{\sqrt{N-1}}{\sqrt{N}}|\omega\rangle + \frac{1}{\sqrt{N}}|x^*\rangle$$

$$= \cos\theta\,|\omega\rangle + \sin\theta\,|x^*\rangle$$

Geometric Analysis

What happens we apply U_f?

$$\cos\theta\,|\omega\rangle + \sin\theta\,|\mathrm{x}^*\rangle \longrightarrow \cos\theta\,|\omega\rangle - \sin\theta\,|\mathrm{x}^*\rangle$$



Applying U_f =Reflection about $|\omega\rangle$

Geometric Analysis

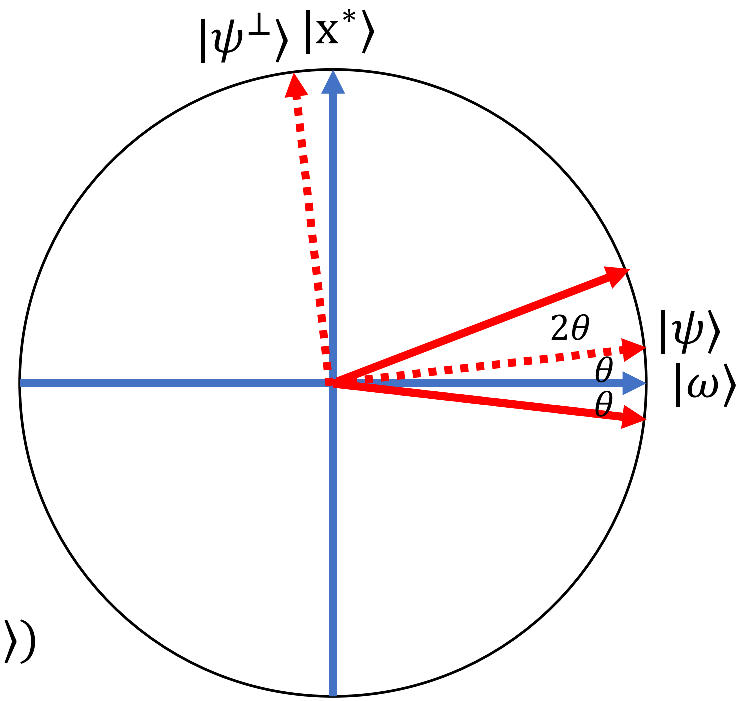
What happens we apply $(2|\psi\rangle\langle\psi| - I_N)$?

Any state $|\phi\rangle$ of this plane can be decomposed into

$$|\phi\rangle = \alpha|\psi\rangle + \beta|\psi^{\perp}\rangle$$

Then,

$$(2|\psi\rangle\langle\psi| - I_N)|\phi\rangle$$
$$= 2|\psi\rangle\langle\psi|(\alpha|\psi\rangle + \beta|\psi^{\perp}\rangle) - (\alpha|\psi\rangle + \beta|\psi^{\perp}\rangle)$$
$$= 2\alpha|\psi\rangle\langle\psi||\psi\rangle + 2\beta|\psi\rangle\langle\psi||\psi^{\perp}\rangle - (\alpha|\psi\rangle + \beta|\psi^{\perp}\rangle)$$
$$= 2\alpha|\psi\rangle - (\alpha|\psi\rangle + \beta|\psi^{\perp}\rangle)$$
$$= \boldsymbol{\alpha|\psi\rangle - \beta|\psi^{\perp}\rangle}$$

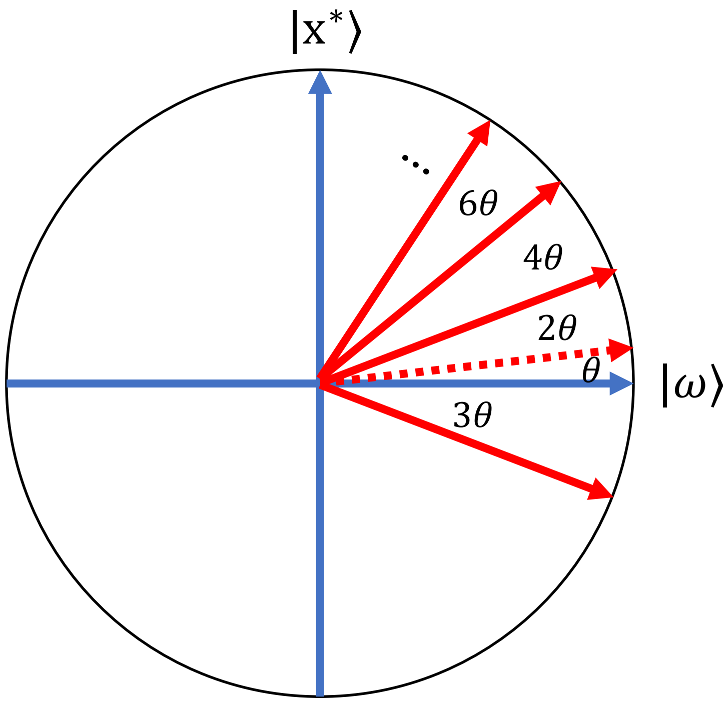


Applying $(2|\psi\rangle\langle\psi| - I_N)$ = Reflection about $|\psi\rangle$

Geometric Analysis

After first iteration,

$$\cos\theta\,|\omega\rangle + \sin\theta\,|\mathrm{x}^*\rangle \longrightarrow \cos 3\theta\,|\omega\rangle + \sin 3\theta\,|\mathrm{x}^*\rangle$$



After each iteration,

$$\cos 5\theta\,|\omega\rangle + \sin 5\theta\,|\mathrm{x}^*\rangle$$

$$\cos 7\theta\,|\omega\rangle + \sin 7\theta\,|\mathrm{x}^*\rangle$$

$$\vdots$$

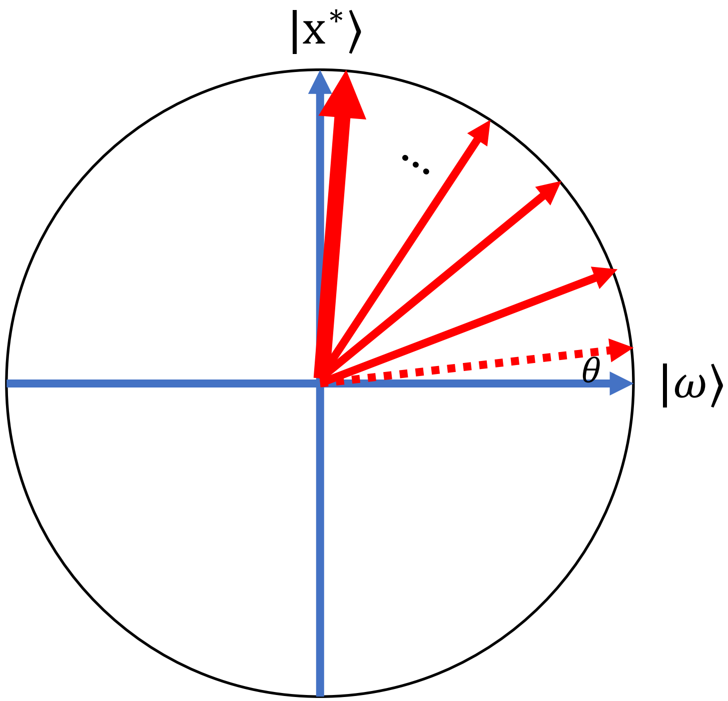
After applying k times,

$$\cos(\theta + 2k\theta)\,|\omega\rangle + \sin(\theta + 2k\theta)\,|\mathrm{x}^*\rangle$$

Geometric Analysis

Recall $\frac{\sqrt{N-1}}{\sqrt{N}}|\omega\rangle + \frac{1}{\sqrt{N}}|\mathrm{x}^*\rangle = \cos\theta\,|\omega\rangle + \sin\theta\,|\mathrm{x}^*\rangle$.

- $\theta = \arccos\sqrt{\frac{N-1}{N}}$



Find k such that $\frac{\pi}{2} \sim (2k+1)\arccos\sqrt{\frac{N-1}{N}}$

$$k_{optimal} = \frac{\pi}{4}\sqrt{N} - \frac{1}{2} - O\left(\sqrt{1/N}\right)$$

Quantum Fourier Transform

Presented by Changyeol Lee

DFT

$\mathcal{DFT}: \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$

$$\frac{1}{\sqrt{N}}\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \cdots & \omega^{(N-1)(N-1)} \end{bmatrix}$$

where $N = 2^n$ and $\omega^N = 1$.

Note. $\mathcal{DFT}$ is unitary.

$$\mathcal{DFT}(\boldsymbol{c})_x = \frac{1}{\sqrt{N}}\sum_{y=0}^{N-1} \omega^{xy} c_y$$

QFT

$\mathcal{QFT}: H_{(n)} \to H_{(n)}$ or (n-qubit) → (n-qubit)

Let $|\psi\rangle^n \coloneqq \sum_{x=0}^{N-1} c_x |x\rangle^n$.

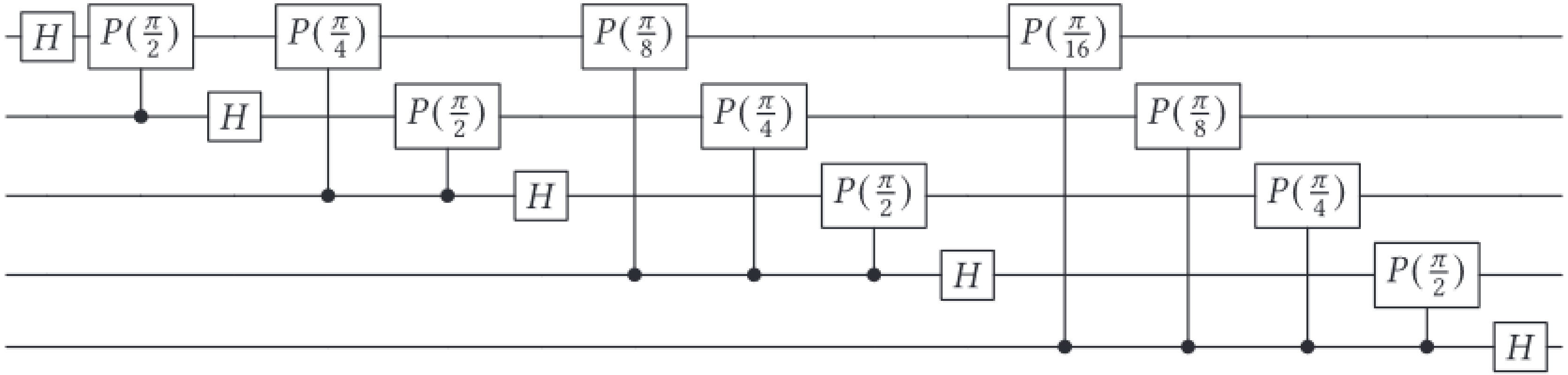
$$\mathcal{QFT}(|\psi\rangle^n) = \mathcal{QFT}\left(\sum_{x=0}^{N-1} c_x |x\rangle^n\right) = \sum_{x=0}^{N-1} \mathcal{DFT}(\boldsymbol{c})_x |x\rangle^n$$

QFT

$\mathcal{QFT}: H_{(n)} \to H_{(n)}$ or (n-qubit) → (n-qubit)

Let $|\psi\rangle^n \coloneqq \sum_{x=0}^{N-1} c_x |x\rangle^n$.

$$\mathcal{QFT}(|\psi\rangle^n) = \mathcal{QFT}\left(\sum_{x=0}^{N-1} c_x |x\rangle^n\right) = \sum_{x=0}^{N-1} \mathcal{DFT}(\boldsymbol{c})_x |x\rangle^n = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \omega^{xy} c_y \, |x\rangle^n$$

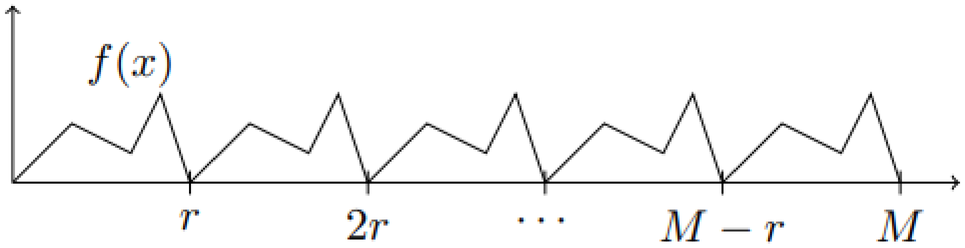


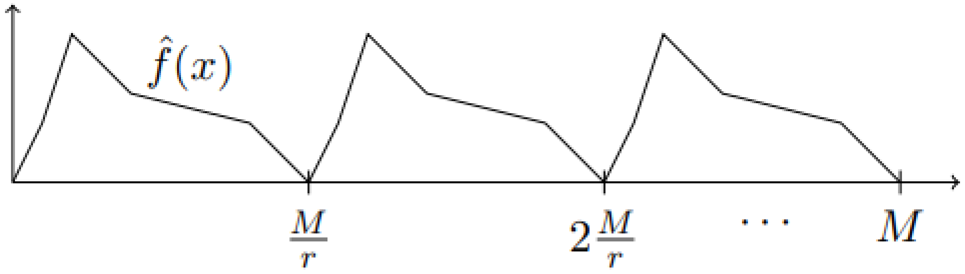
when $n = 5$

Period / Frequency

Suppose f is periodic with period r (or frequency M/r).

Then $\hat{f}$ (the Fourier transform of f) is periodic with period M/r (or frequency r).





Shor’s Periodicity Problem

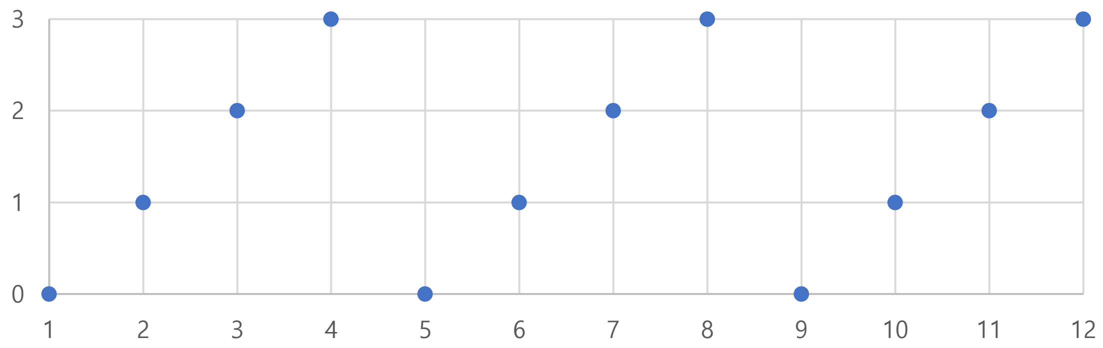
Presented by Changyeol Lee

Periodic injective

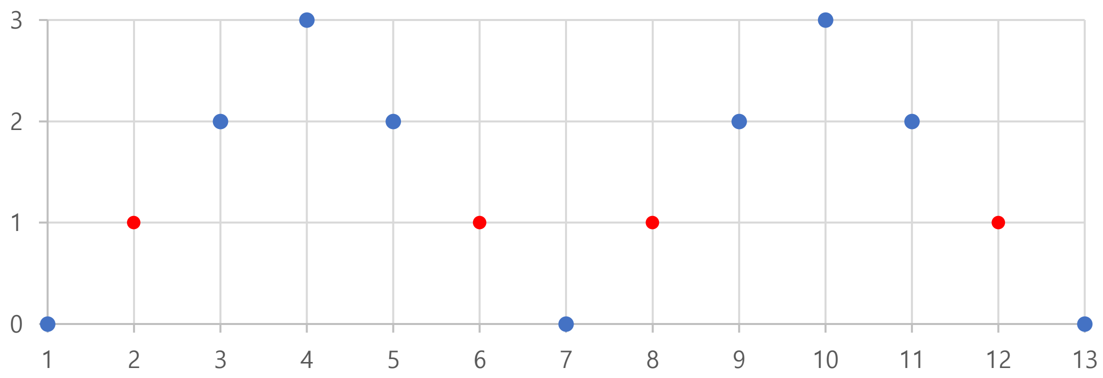
A function $f: \mathbb{Z}_M \to S$ where $S \subset \mathbb{Z}_M$ is called **periodic injective**

if there exists an integer $a \in \mathbb{Z}_m$ (called period)

such that for all $x \neq y$, we have $f(x) = f(y) \Leftrightarrow y = x + ka$ for some integer k.



periodic injective



periodic but not injective

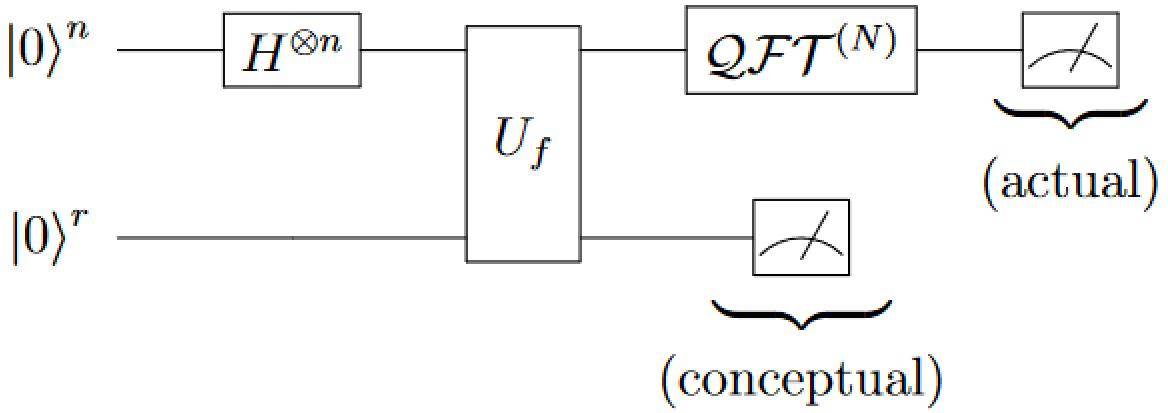
Problem

Let $f: \mathbb{Z}_M \to \mathbb{Z}$ be periodic injective. Find a. (Assume $a < M/2$.)

Let n be an integer such that $2^{n-1} < M^2 \leq 2^n$.

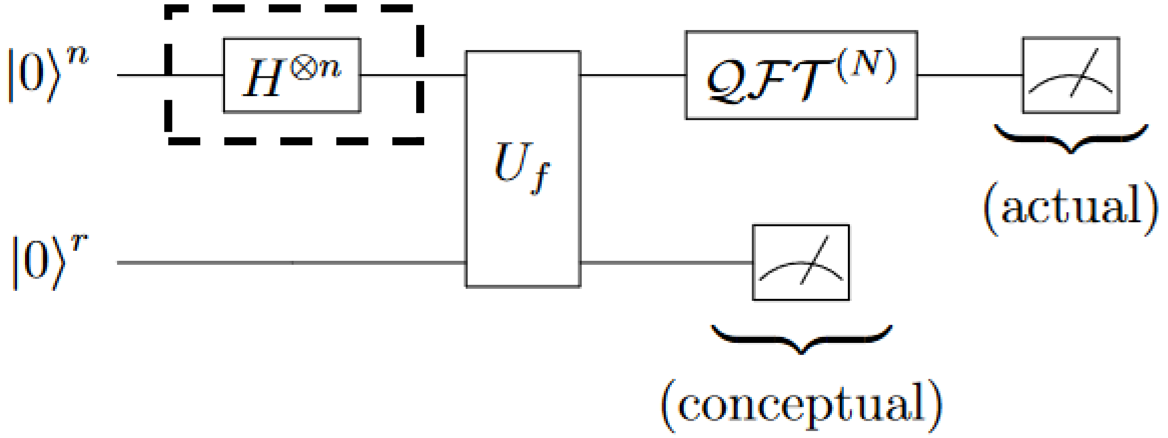
WLOG, assume that range of f is a subset of $\mathbb{Z}_{2^r}$ for some r

Let $f: \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^r}$ be periodic injective. Find a.



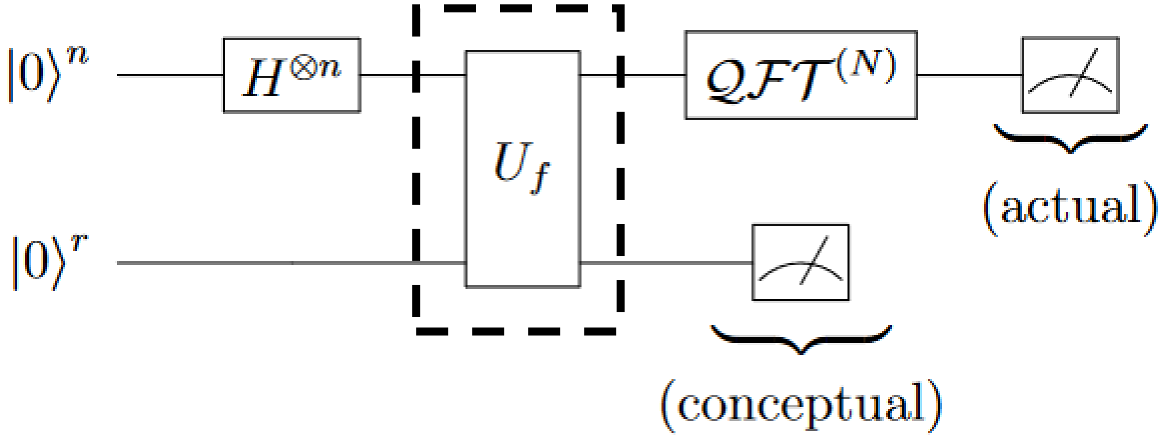
Analysis

$$H^{\otimes n}|0\rangle^n = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} (-1)^{0\odot y}|y\rangle^n = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} |y\rangle^n$$



Analysis

$$U_f\left(\left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} |y\rangle^n \otimes |0\rangle^r\right) = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} U_f(|y\rangle^n \otimes |0\rangle^r) = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} |y\rangle^n \otimes |f(y)\rangle^r$$



Analysis

Let $m \coloneqq \lfloor N/a \rfloor$. Let k be an integer s.t. $N-1 = am + k$.

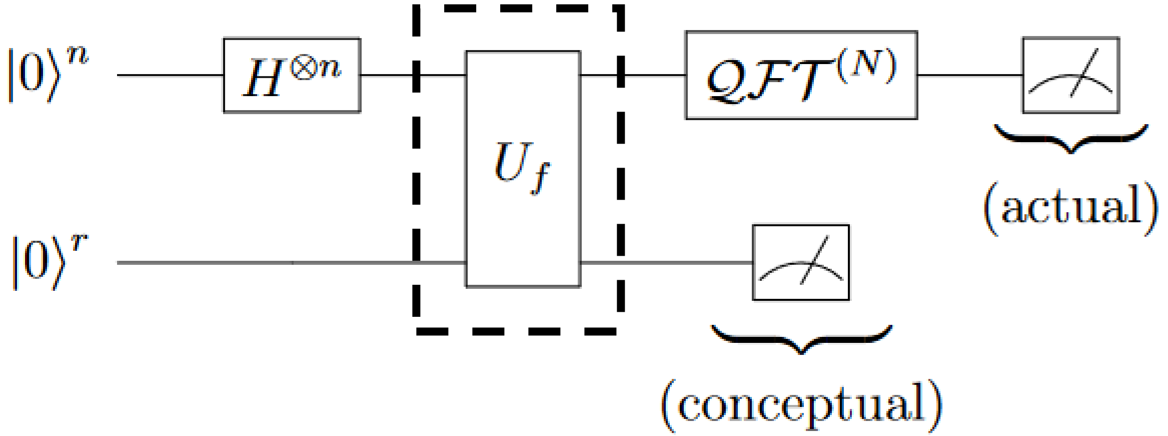
$$
\begin{aligned}
&|0\rangle^n \otimes |f(0)\rangle^r && + |1\rangle^n \otimes |f(1)\rangle^r && + \cdots\cdots + |a-1\rangle^n \otimes |f(a-1)\rangle^r + \\
&|a\rangle^n \otimes |f(0)\rangle^r && + |a+1\rangle^n \otimes |f(1)\rangle^r && + \cdots\cdots + |2a-1\rangle^n \otimes |f(a-1)\rangle^r + \\
& && && \cdots \\
&|(m-1)a\rangle^n \otimes |f(0)\rangle^r && + |(m-1)a+1\rangle^n \otimes |f(1)\rangle^r && + \cdots\cdots + |(m-1)a-1\rangle^n \otimes |f(a-1)\rangle^r + \\
&|ma\rangle^n \otimes |f(0)\rangle^r && + |ma+1\rangle^n \otimes |f(1)\rangle^r && + \cdots + |ma+k\rangle^n \otimes |f(k)\rangle^r
\end{aligned}
$$

$$
\sum_{y=0}^{2^n-1} |y\rangle^n \otimes |f(y)\rangle^r = \sum_{y=0}^{a-1} \left(\mathbf{1}_{y \le k} |y+ma\rangle^n + \sum_{i=0}^{m-1} |y+ia\rangle^n \right) \otimes |f(y)\rangle^r
$$

Analysis

$$U_f\left(\left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} |y\rangle^n \otimes |0\rangle^r\right) = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} U_f(|y\rangle^n \otimes |0\rangle^r) = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{2^n-1} |y\rangle^n \otimes |f(y)\rangle^r$$

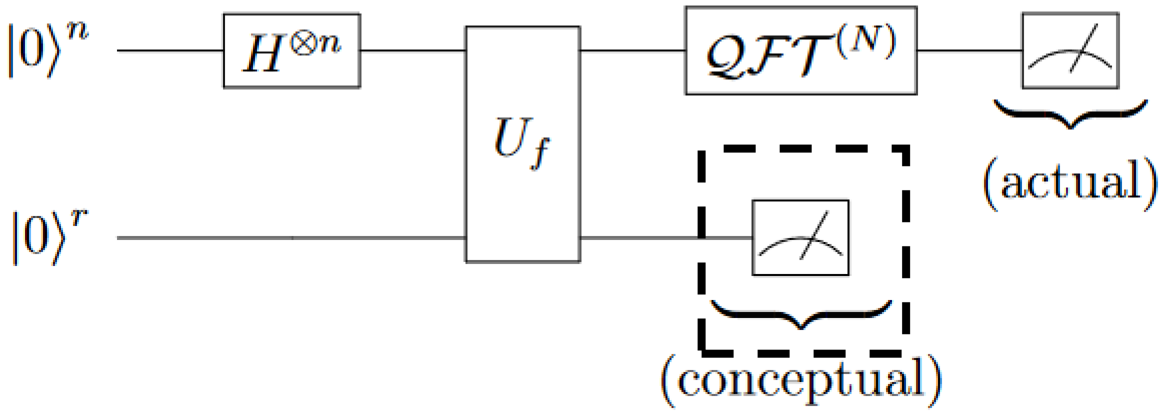
$$= \left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{a-1} \left(\mathbf{1}_{y\le k}|y+ma\rangle^n + \sum_{i=0}^{m-1} |y+ia\rangle^n\right) \otimes |f(y)\rangle^r$$



Analysis

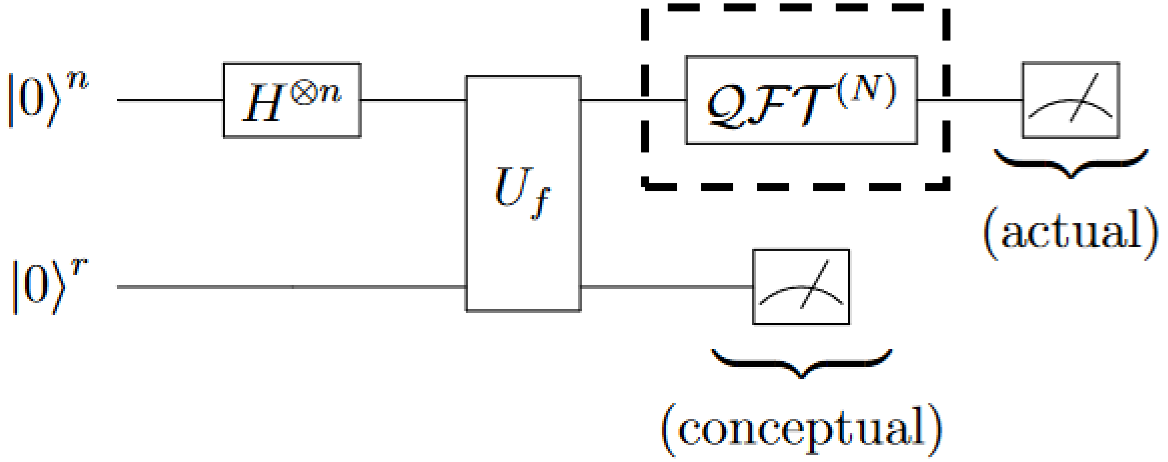
$$\left(\frac{1}{\sqrt{2}}\right)^n \sum_{y=0}^{a-1} \left(\mathbf{1}_{y \le k} |y + ma\rangle^n + \sum_{i=0}^{m-1} |y + ia\rangle^n \right) \otimes |f(y)\rangle^r$$

$|f(y)\rangle^r$ collapses to some y_0 with probability m/N or $(m+1)/N$.



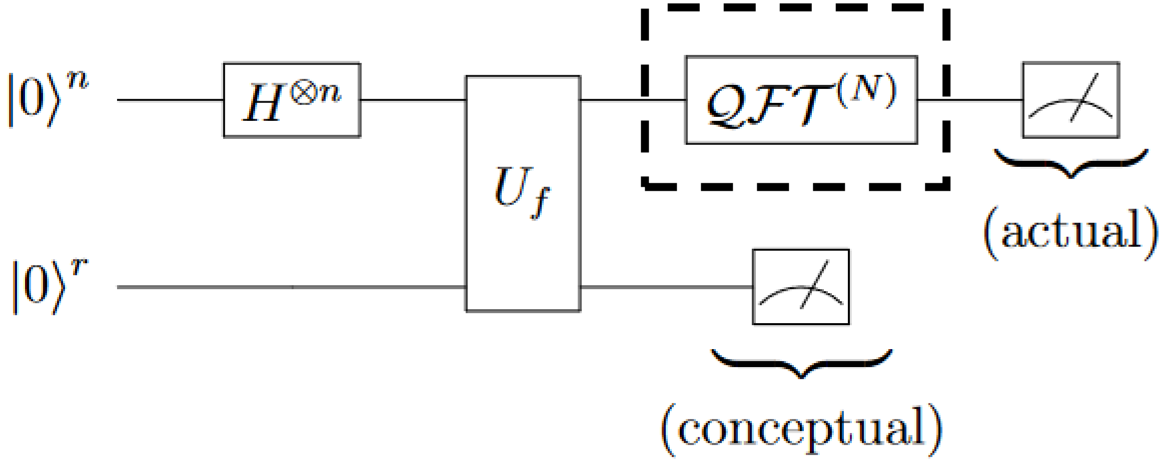
Analysis

$$\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}|y_0 + ia\rangle^n$$



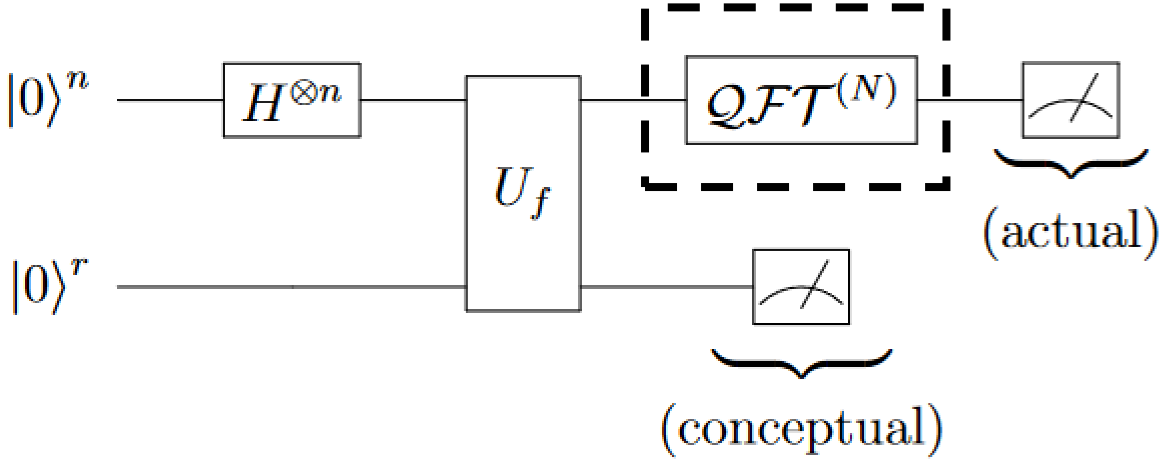
Analysis

$$\mathcal{QFT}\left(\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}|y_0+ia\rangle^n\right)$$



Analysis

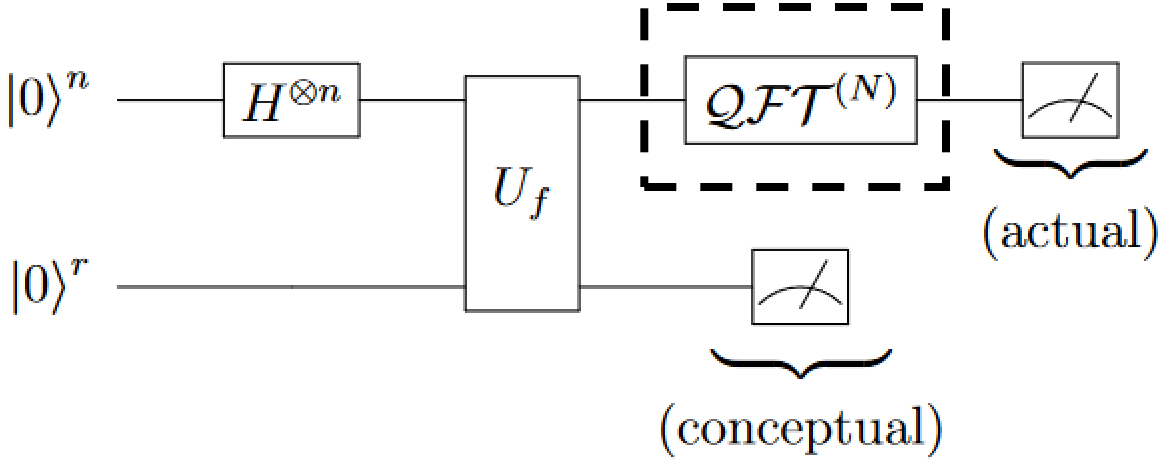
$$\mathcal{QFT}\left(\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}|y_0+ia\rangle^n\right)=\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}\mathcal{QFT}|y_0+ia\rangle^n$$



Analysis

$$\mathcal{QFT}\left(\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}|y_0+ia\rangle^n\right)=\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}\mathcal{QFT}|y_0+ia\rangle^n$$

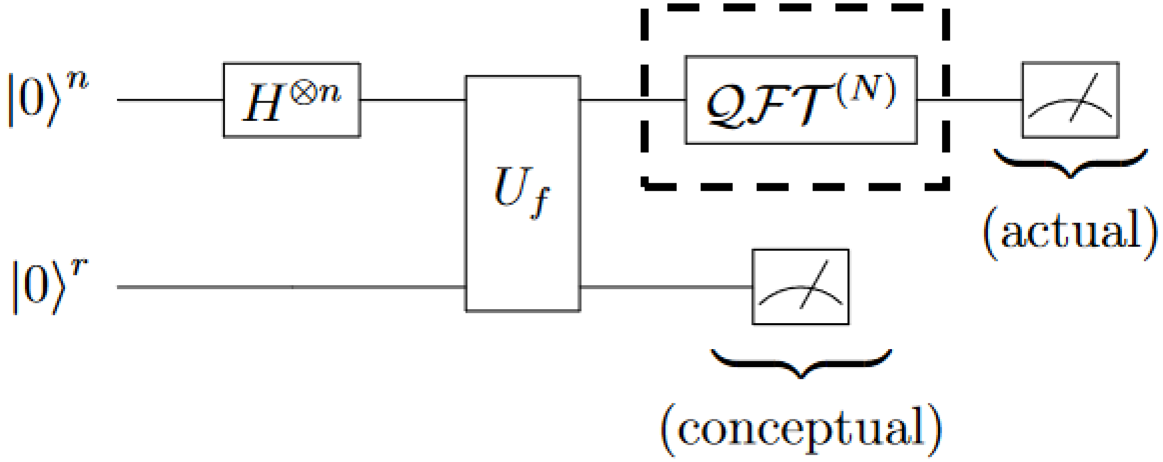
$$\mathcal{QFT}|y_0+ia\rangle^n=\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\omega^{(y_0+ia)x}\,|x\rangle^n=\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\omega^{y_0x}\omega^{iax}\,|x\rangle^n$$



Analysis

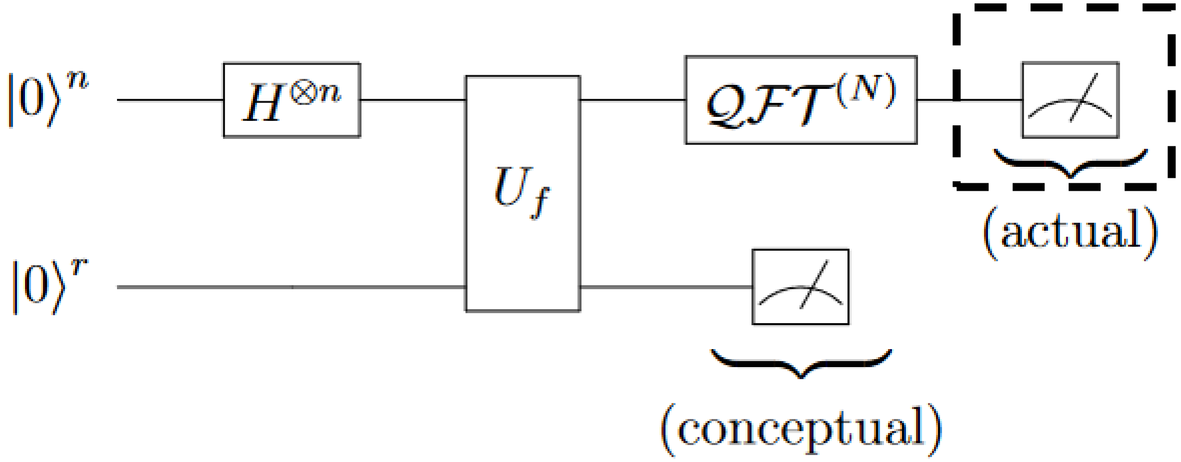
$$\mathcal{QFT}\left(\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}|y_0+ia\rangle^n\right)=\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}\mathcal{QFT}|y_0+ia\rangle^n=\frac{1}{\sqrt{m'N}}\sum_{x=0}^{N-1}\omega^{y_0x}\left(\sum_{i=0}^{m'-1}\omega^{iax}\right)|x\rangle^n$$

$$\mathcal{QFT}|y_0+ia\rangle^n=\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\omega^{(y_0+ia)x}\,|x\rangle^n=\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\omega^{y_0x}\omega^{iax}\,|x\rangle^n$$



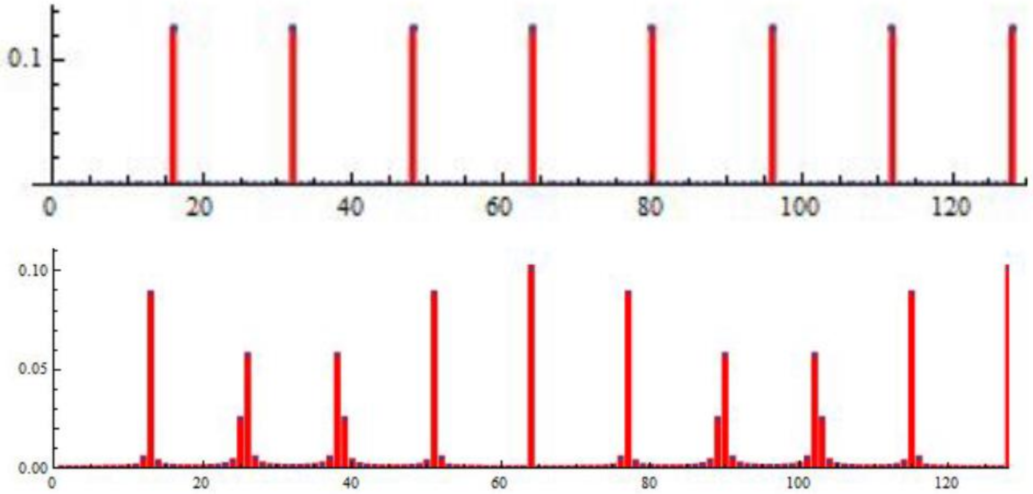
Analysis

$$\mathcal{QFT}\left(\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}|y_0+ia\rangle^n\right)=\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}\mathcal{QFT}|y_0+ia\rangle^n=\frac{1}{\sqrt{m'N}}\sum_{x=0}^{N-1}\omega^{y_0x}\left(\sum_{i=0}^{m'-1}\omega^{iax}\right)|x\rangle^n$$



Analysis

$$\mathcal{QFT}\left(\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}|y_0+ia\rangle^n\right)=\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}\mathcal{QFT}|y_0+ia\rangle^n=\frac{1}{\sqrt{m'N}}\sum_{x=0}^{N-1}\omega^{y_0x}\left(\sum_{i=0}^{m'-1}\omega^{iax}\right)|x\rangle^n$$



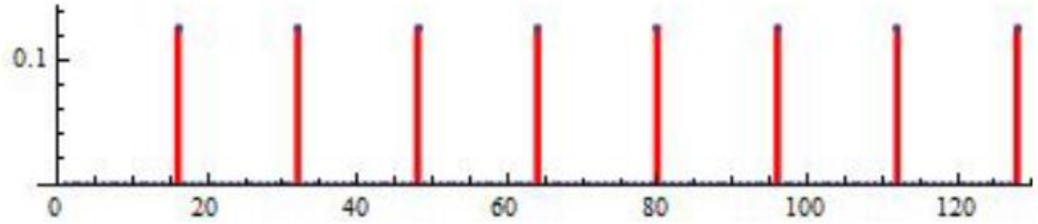
spectrum of
period 8
with domain 128

spectrum of
period 10
with domain 128

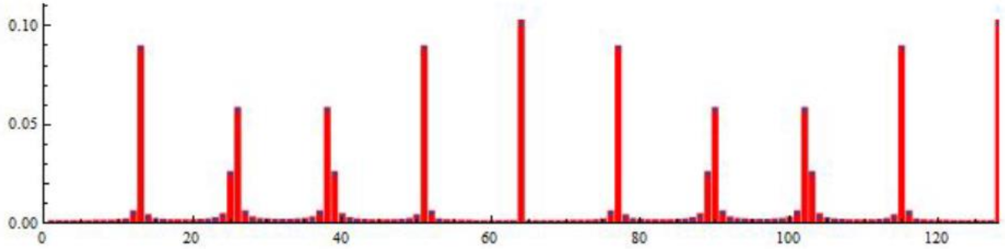
Analysis

$$\mathcal{QFT}\left(\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}|y_0+ia\rangle^n\right)=\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}\mathcal{QFT}|y_0+ia\rangle^n=\frac{1}{\sqrt{m'N}}\sum_{x=0}^{N-1}\omega^{y_0x}\left(\sum_{i=0}^{m'-1}\omega^{iax}\right)|x\rangle^n$$

Claim. Some x's are highly likely to be measured!



spectrum of
period 8
with domain 128



spectrum of
period 10
with domain 128

Analysis

$$\mathcal{QFT}\left(\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}|y_0+ia\rangle^n\right)=\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}\mathcal{QFT}|y_0+ia\rangle^n=\frac{1}{\sqrt{m'N}}\sum_{x=0}^{N-1}\omega^{y_0x}\left(\sum_{i=0}^{m'-1}\omega^{iax}\right)|x\rangle^n$$

Claim. "Some" x's are highly likely to be measured!

Consider $x_0, x_1, \cdots, x_{a-1}$ where $x_c a \in \left[cN-\frac{a}{2}, cN+\frac{a}{2}\right)$ for all $c=0,\cdots,a-1$.

(Note. $x_c a < aN$ and thus any x_c is a candidate of the measurement.)

e.g., if $N=32, a=3$, $x_0=0, x_1=11, x_2=21$

Analysis

$$\mathcal{QFT}\left(\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}|y_0+ia\rangle^n\right)=\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}\mathcal{QFT}|y_0+ia\rangle^n=\frac{1}{\sqrt{m'N}}\sum_{x=0}^{N-1}\omega^{y_0x}\left(\sum_{i=0}^{m'-1}\omega^{iax}\right)|x\rangle^n$$

Claim. Some x's are "highly likely" to be measured!

$$\Pr(x\text{ is measured})=\frac{1}{m'N}|\omega^{y_0x}|^2\left|\sum_{i=0}^{m'-1}\omega^{iax}\right|^2=\frac{1}{m'N}\left|\sum_{i=0}^{m'-1}\omega^{iax}\right|^2\quad(\text{since }|\omega|=1)$$

Let $\mu\coloneqq\omega^{ax}$.

$$\sum_{i=0}^{m'-1}\mu^i=\frac{\mu^{m'}-1}{\mu-1}=\frac{\omega^{axm'}-1}{\omega^{ax}-1}=\frac{e^{i\theta_x m'}-1}{e^{i\theta_x}-1}$$

where θ_x is the angle of ω^{ax}.

Analysis

$$\mathcal{QFT}\left(\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}|y_0+ia\rangle^n\right)=\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}\mathcal{QFT}|y_0+ia\rangle^n=\frac{1}{\sqrt{m'N}}\sum_{x=0}^{N-1}\omega^{y_0x}\left(\sum_{i=0}^{m'-1}\omega^{iax}\right)|x\rangle^n$$

Claim. Some x's are "highly likely" to be measured!

$$\Pr(x\text{ is measured})=\frac{1}{m'N}\left|\frac{e^{i\theta_x m'}-1}{e^{i\theta_x}-1}\right|^2$$

- $\frac{2\theta}{\pi}\le\left|e^{i\theta}-1\right|=2\left|\sin\frac{\theta}{2}\right|\le|\theta|$

Analysis

$$\mathcal{QFT}\left(\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}|y_0+ia\rangle^n\right)=\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}\mathcal{QFT}|y_0+ia\rangle^n=\frac{1}{\sqrt{m'N}}\sum_{x=0}^{N-1}\omega^{y_0x}\left(\sum_{i=0}^{m'-1}\omega^{iax}\right)|x\rangle^n$$

Claim. Some x's are "highly likely" to be measured!

$$\Pr(\text{some } x_c \text{ is measured}) > 0.405$$

assuming $a \ll M$.

Analysis

$$\mathcal{QFT}\left(\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}|y_0+ia\rangle^n\right)=\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}\mathcal{QFT}|y_0+ia\rangle^n=\frac{1}{\sqrt{m'N}}\sum_{x=0}^{N-1}\omega^{y_0x}\left(\sum_{i=0}^{m'-1}\omega^{iax}\right)|x\rangle^n$$

One of $x_0, x_1, \cdots, x_{a-1}$ where $cN-\frac{a}{2}\le x_c a< cN+\frac{a}{2}$ is highly likely to be measured.

Claim. x_c/N is uniquely close to c/a.

$$cN-\frac{a}{2}\le x_c a< cN+\frac{a}{2} \iff -\frac{a}{2}\le x_c a-cN<\frac{a}{2} \iff -\frac{1}{2N}\le\frac{x_c}{N}-\frac{c}{a}<\frac{1}{2N} \iff 2\left|\frac{x_c}{N}-\frac{c}{a}\right|<\frac{1}{N}$$

$$2\left|\frac{x_c}{N}-\frac{c}{a}\right|<\frac{1}{M^2}\ \ (M^2\le N)\ \text{ and }\ \frac{1}{M^2}\le\left|\frac{c+1}{a}-\frac{c}{a}\right|\ \ (M^2\le N)$$

Therefore, x_c/N is uniquely close to c/a.

Analysis

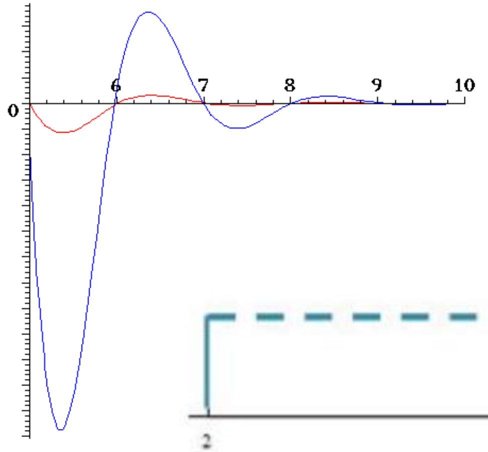
$$QFT\left(\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}|y_0+ia\rangle^n\right)=\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}QFT|y_0+ia\rangle^n=\frac{1}{\sqrt{m'N}}\sum_{x=0}^{N-1}\omega^{y_0x}\left(\sum_{i=0}^{m'-1}\omega^{iax}\right)|x\rangle^n$$

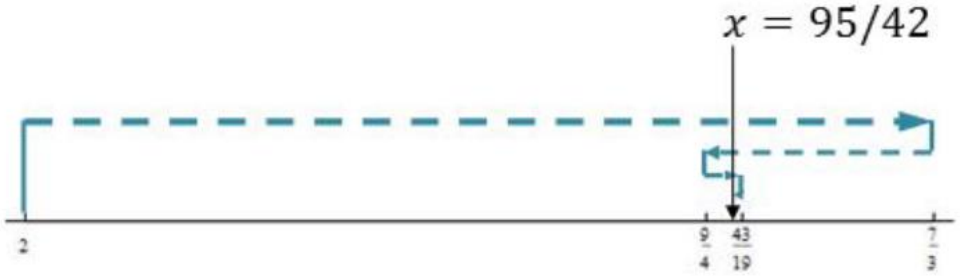
One of $x_0, x_1, \cdots, x_{a-1}$ where $cN-\frac{a}{2}\le x_c a<cN+\frac{a}{2}$ is highly likely to be measured.

x_c/N is uniquely close to c/a.

How to compute c/a from x_c?

- By continued fraction algorithm (CFA).
- Starting from close point n_0/d_0, compute $\{n_k/d_k\}$
- Can be done in $O(\log^3 N)$





Analysis

$$\mathcal{QFT}\left(\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}|y_0+ia\rangle^n\right)=\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}\mathcal{QFT}|y_0+ia\rangle^n=\frac{1}{\sqrt{m'N}}\sum_{x=0}^{N-1}\omega^{y_0x}\left(\sum_{i=0}^{m'-1}\omega^{iax}\right)|x\rangle^n$$

One of $x_0, x_1, \cdots, x_{a-1}$ where $cN-\frac{a}{2}\le x_c a < cN+\frac{a}{2}$ is highly likely to be measured.

x_c/N is uniquely close to c/a.

Find n/d which is equal to c/a by CFA.

So... what is the value of a*?*

No guarantee that c corresponding to y_c is coprime to a.

Therefore, not necessarily $n=c$ and $d=a$.

Claim. One of $x_0, x_1, \cdots, x_{a-1}$ whose index is coprime to a is highly likely to be measured!

Analysis

$$\mathcal{QFT}\left(\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}|y_0+ia\rangle^n\right)=\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}\mathcal{QFT}|y_0+ia\rangle^n=\frac{1}{\sqrt{m'N}}\sum_{x=0}^{N-1}\omega^{y_0x}\left(\sum_{i=0}^{m'-1}\omega^{iax}\right)|x\rangle^n$$

One of $x_0, x_1, \cdots, x_{a-1}$ where $cN-\frac{a}{2}\le x_c a < cN+\frac{a}{2}$ is highly likely to be measured.

x_c/N is uniquely close to c/a.

Find n/d which is equal to c/a by CFA.

Claim 1. $\Pr(x_c \text{ measured}) \approx \Pr(x_{c'} \text{ measured})$.

Claim 2. $\Pr(c \text{ coprime to } a) \ge \zeta(2) > 0.6$ where $c \sim \text{Uni}[0, a-1]$.

Analysis

$$\mathcal{QFT}\left(\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}|y_0+ia\rangle^n\right)=\frac{1}{\sqrt{m'}}\sum_{i=0}^{m'-1}\mathcal{QFT}|y_0+ia\rangle^n=\frac{1}{\sqrt{m'N}}\sum_{x=0}^{N-1}\omega^{y_0x}\left(\sum_{i=0}^{m'-1}\omega^{iax}\right)|x\rangle^n$$

One of $x_0, x_1, \cdots, x_{a-1}$ where $cN-\frac{a}{2}\le x_c a< cN+\frac{a}{2}$ **and $\boldsymbol{c}$ is coprime to $\boldsymbol{a}$** is highly likely to be measured.

x_c/N is uniquely close to c/a.

Find n/d which is equal to c/a by CFA.

d is the period!

Thank You

Presented by Changyeol Lee