# Chapter 2 Quantum Algorithms for Quantum Computation

## 2.1 Deutsch-Jozsa algorithm

### 2.1.1 Basics

D. Deutsch and R. Jozsa, Proc. R. Soc. London A 439, 553 (1992)

Alice — inquiry → Bob

$x \in [0, 2^n - 1]$ ← reply — $f(x) = \begin{cases} 0 \\ 1 \end{cases}$

type 1 : all zeros or all ones
type 2 : half zeros and half ones

<u>$n$ = 2 bit D-J problem: Boolean function</u>

| $x$ | $x_1$ | $x_2$ | $f_c$ | $\overline{f_c}$ | $f_{x_1}$ | $\overline{f_{x_1}}$ | $f_{x_2}$ | $\overline{f_{x_2}}$ | $f_{x_1 \oplus x_2}$ | $\overline{f_{x_1 \oplus x_2}}$ |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 |
| 2 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 |
| 3 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 |
| | | | type 1 | | type 2 | | | | | |

Question : How many inquiries must Alice make before she finds whether $f(x)$ is type 1 or type 2?

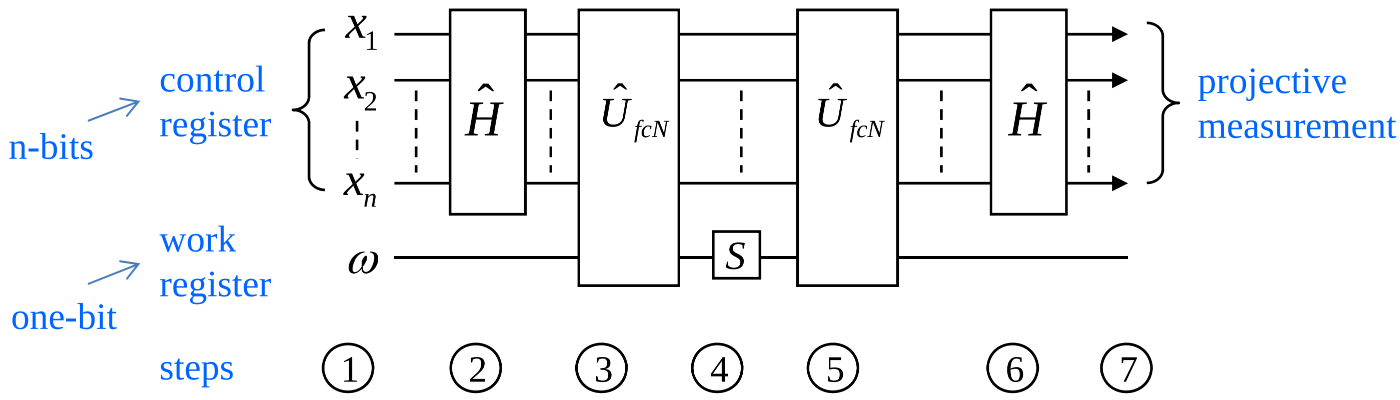
⇩

Classical solution : $2^{n-1} + 1$ (worst case)

$n = 1 \longrightarrow$ 2 inquiries
$n = 10 \longrightarrow$ 513 inquires
$n = 20 \longrightarrow$ 524.289 inquires
$n = 30 \longrightarrow$ $\sim 10^9$ inquires
$n = 40 \longrightarrow$ $\sim 10^{12}$ inquires

(exponential scaling)

## Quantum solution : 1 (just one inquiry)




**Step 1: Initialization**

$$|x=0\rangle = |0\rangle_1 |0\rangle_2 \cdots\cdots |0\rangle_n$$

$$|\omega=0\rangle = |0\rangle_\omega$$

**Step 2: Walsh-Hadamard transform**

$$\hat{H}_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{matrix} |0\rangle_L \\ |1\rangle_L \end{matrix}$$

base state
(logical state)

$$\hat{H}|x=0\rangle = \left(\hat{H}_2|0\rangle_1\right)\otimes\left(\hat{H}_2|0\rangle_2\right)\otimes\cdots\cdots\otimes\left(\hat{H}_2|0\rangle_n\right)$$ : bit-wise Hadamard transform

$$= \frac{1}{\sqrt{2}}\left(|0\rangle_1+|1\rangle_1\right)\otimes\frac{1}{\sqrt{2}}\left(|0\rangle_2+|1\rangle_2\right)\otimes\cdots\cdots\otimes\frac{1}{\sqrt{2}}\left(|0\rangle_n+|1\rangle_n\right)$$

$$= \frac{1}{\sqrt{2^n}}\left[\left(\underbrace{|0\rangle_1|0\rangle_2\cdots|0\rangle_n}_{|x=0\rangle} + \underbrace{|0\rangle_1|0\rangle_2\cdots|1\rangle_n}_{|x=1\rangle} + \cdots + \underbrace{|1\rangle_1|1\rangle_2\cdots|1\rangle_n}_{|x=2^n-1\rangle}\right)\right]$$

In general,

$$\hat{H}|x_1\rangle_1|x_2\rangle_2\cdots\cdots|x_n\rangle_n = \frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{x\cdot y}|y_1\rangle_1|y_2\rangle_2\cdots\cdots|y_n\rangle_n$$

$$x\cdot y = x_1y_1 + x_2y_2 + \cdots\cdots + x_ny_n$$

only if $x_i$=1 and $y_i$=1, a minus sign applies.

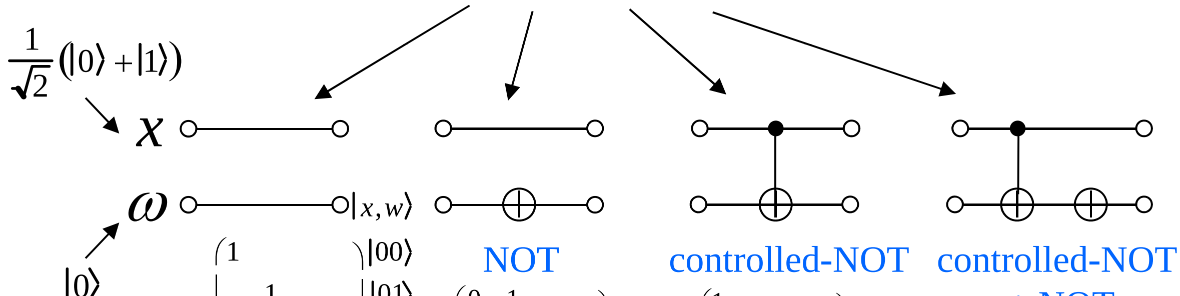
## Step 3: *f*-controlled-NOT gate

$$\hat{U}_{fcN}\left(\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_c\right)\otimes|0\rangle_\omega = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_c|f(x)\rangle_\omega$$

simultaneous calculation of *f(x)* for all *x* values.

$n$ = 1 qubit

| $x$ | $f_c$ | $\overline{f}_c$ | $f_x$ | $\overline{f}_x$ |
|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 1 |
| 1 | 0 | 1 | 1 | 0 |



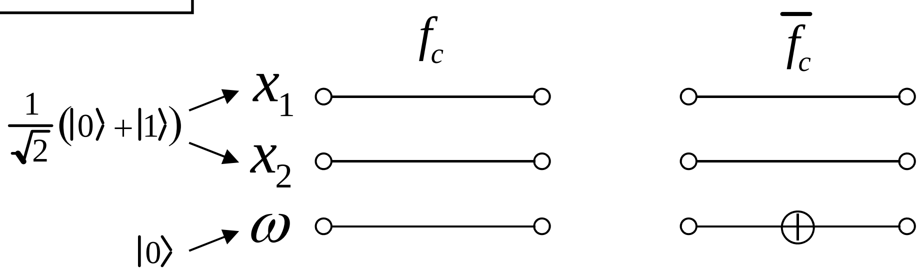

$$I = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}\begin{matrix}|00\rangle\\|01\rangle\\|10\rangle\\|11\rangle\end{matrix}$$

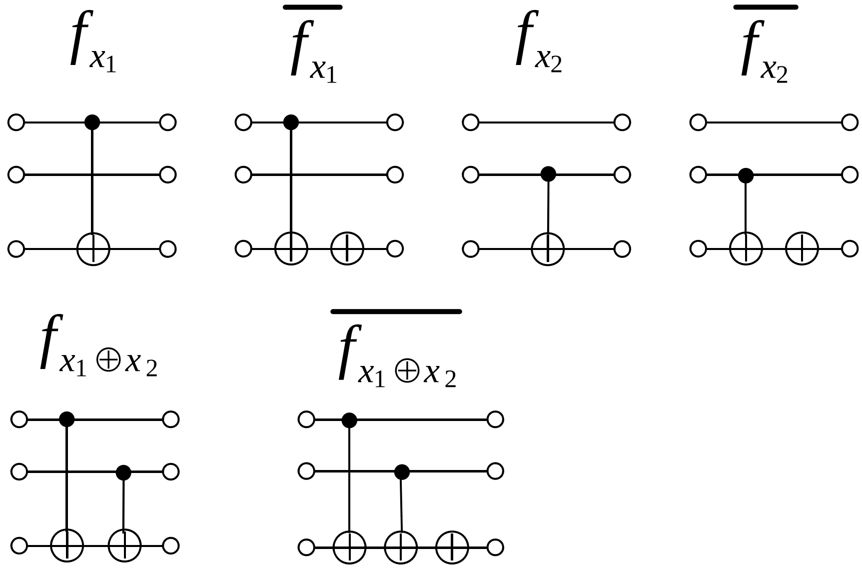
NOT: $\begin{pmatrix} 0 & 1 & & \\ 1 & 0 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{pmatrix}$

controlled-NOT: $\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{pmatrix}$

controlled-NOT + NOT: $\begin{pmatrix} 0 & 1 & & \\ 1 & 0 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}$

$n$ = 2 qubit






## Step 4: Phase shifter

$$\hat{E}\left[\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_c|f(x)\rangle_\omega\right]=\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}e^{i\pi f(x)}|x\rangle_c|f(x)\rangle_\omega$$

$$\hat{E}=\begin{pmatrix}1 & 0\\ 0 & e^{i\pi}\end{pmatrix}\begin{matrix}|0\rangle_\omega\\ |1\rangle_\omega\end{matrix}$$

The phase modulation imposed on the work register is now shared by the control register.

## Step 5: f-controlled-NOT gate

$$\hat{U}_{fcN}\left[\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}e^{i\pi f(x)}|x\rangle_c|f(x)\rangle_\omega\right]=\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}e^{i\pi f(x)}|x\rangle_c|0\rangle_\omega$$

The work register is now decoupled from the control register.

$$|f(x)\oplus f(x)\rangle_\omega$$

## Step 6: Walsh-Hadamard transform

$$\hat{H}\left[\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}e^{i\pi f(x)}|x\rangle_c\right]=\frac{1}{2^n}\sum_{y\in\{0,1\}^n}\sum_{x\in\{0,1\}^n}e^{i\pi[f(x)+x\cdot y]}|y\rangle_c$$

$$\Downarrow$$

probability amplitude for $|y=0\rangle=|0\rangle_1|0\rangle_2\cdots|0\rangle_n$

$$\frac{1}{2^n}\sum_{x\in\{0,1\}^n}e^{i\pi f(x)}=\begin{cases}\pm 1 & \text{for type 1}\\ 0 & \text{for type 2}\end{cases}$$

## Step 7: Projective measurement

If the measurement results for $n$-qubit control registers are $|0\rangle_1|0\rangle_2\cdots|0\rangle_n$, we can conclude $f(x)$ is type 1. If the measurement result is one of the other $(2^n - 1)$ states, we conclude $f(x)$ is type 2.

## 2.1.2 Interpretation of D-J algorithm as a quantum interferometer

(2) $$|0\rangle_c|0\rangle_\omega \xrightarrow{\hat{H}} \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle_c|0\rangle_\omega$$ $\boxed{\text{linear superposition}}$

Simultaneous inquiries of $2^n$ different input values $|x\rangle_c$

$\Rightarrow$ quantum parallelism

(3) $$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle_c|0\rangle_\omega \xrightarrow{\hat{U}_{fcN}} \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle_c|f(x)\rangle_\omega$$ $\boxed{\text{entanglement}}$

Simultaneous calculation of $f(x)$ for all input values $|x\rangle_c$ , but a simple projective measurement for the work resister provides only one bit of information, which does not provide a desired result.

(4) $$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle_c|f(x)\rangle_\omega \xrightarrow{\hat{S}} \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}e^{i\pi f(x)}|x\rangle_c|f(x)\rangle_\omega$$

$\boxed{\text{nonlocal phase modulation}}$

The calculation result $f(x)$ is transferred to the phase of the control register state via the nonlocality & nonseparability of an entangled state.

(5) $$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1} e^{i\pi f(x)}|x\rangle_c |f(x)\rangle_\omega \xrightarrow{\hat{U}_{fcN}} \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1} e^{i\pi f(x)}|x\rangle_c |0\rangle_\omega$$

quantum erasure ⟹ $c$ and $\omega$ are disentangled

As a preparation of the next step of quantum interference, we need to erase the which-path information $|f(x)\rangle_\omega$ stored in the work register.

(6) $$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1} e^{i\pi f(x)}|x\rangle_c \xrightarrow{\hat{H}} \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1} e^{i\pi[f(x)+x\cdot y]}|y\rangle_c$$

quantum interference

The probability amplitudes $\frac{1}{\sqrt{2^n}}e^{i\pi f(x)}$ for all states $|x\rangle_c$ now interfere with each other in the probability amplitude of the output states $|y\rangle_c$ .

(7) $$\left|{}_c\langle 0|\frac{1}{2^n}\sum_y\sum_x e^{i\pi[f(x)+x\cdot y]}|y\rangle_c\right|^2 = \left|\frac{1}{2^n}\sum_x e^{i\pi f(x)}\right|^2$$

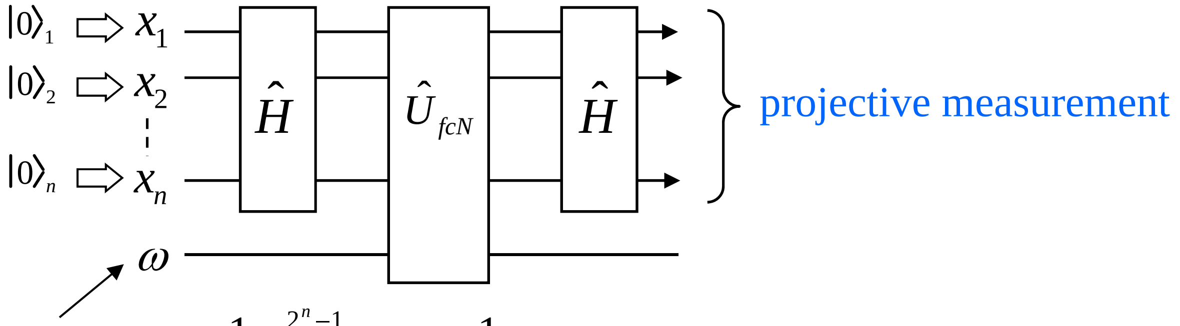
$$= \begin{cases} 1 & \text{: type 1} \\ 0 & \text{: type 2} \end{cases}$$

⇓

Projective measurement

deterministic answer

## 2.1.3 Modified Deutsch-Jozsa algorithm




$$\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \qquad \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle_c \otimes \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)_\omega$$

$$\xrightarrow{\hat{U}_{fcN}} \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle_c \otimes \frac{1}{\sqrt{2}}\left(|0\oplus f(x)\rangle - |1\oplus f(x)\rangle\right)_\omega$$

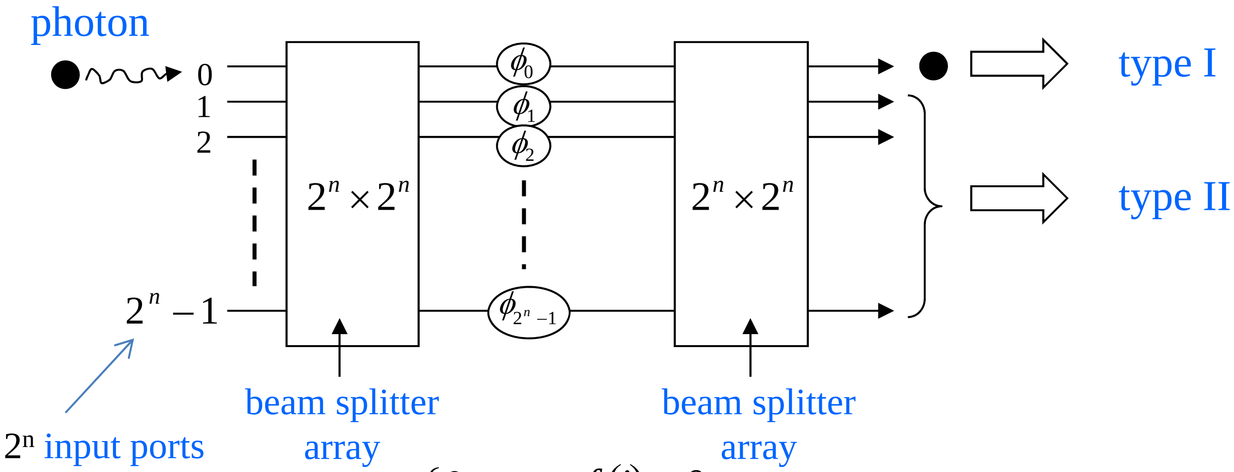
$$= \underbrace{\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1} e^{i\pi f(x)}|x\rangle_c}_{\text{ready to interfere!}} \otimes \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)_\omega$$

The work register is already disentangled.

$$\xrightarrow{\hat{H}} \underbrace{\frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1} e^{i\pi[f(x)+x\cdot y]}|y\rangle_c}_{\text{desired interference pattern}} \otimes \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)_\omega$$

This is an example of quantum interference without quantum erasure step, as was discussed in Chapter 1.

## 2.1.4 A single photon linear optics interferometer for implementing D-J algorithm




$$\phi_i = \begin{cases} 0 & \text{if } f(i) = 0 \\ \pi & \text{if } f(i) = 1 \end{cases}$$

We have to pay a penalty if a single particle linear optics interferometer is used instead of a multi-particle nonlinear interferometer.

The penalty is the exponential increase in spatial resources such as beam splitters, phase shifters and detectors.

$\Downarrow$

A quantum computer is a multi-particle nonlinear interferometer, in which an essential resource of quantum computation, entanglement, realizes the non-local correlations among localized qubits.

$\Downarrow$

A coherent computer (Chapter 4) is another kind of nonlinear interferometer, in which the non-local correlations are realized not by entanglement but by the non-local wave nature of particles.

## 2.2 Grover's data search algorithm

L. K. Grover, PRL 79, 325 (1997)

$$\underset{\text{Alice}}{x \in [0, 2^n - 1]} \underset{\text{reply}}{\overset{\text{inquiry}}{\rightleftarrows}} \underset{\text{Bob}}{f(x) = \begin{cases} 1 & \text{for } x = \tau \text{ (target)} \\ 0 & \text{for } x \neq \tau \text{ (non-target)} \end{cases}}$$

How many inquires must Alice make before she will find $x = \tau$ ?

$\Downarrow$

classical solution: $2^n$ (worst case) $2^{n-1}$ (on average)

quantum solution: $\sqrt{2^n}$ (still exponential but big improvement)

### 2.2.1. Heuristic picture

- inversion operator

$$\hat{I}_x = \begin{pmatrix} 1 & & & & & & 0 \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & -1 & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ 0 & & & & & & 1 \end{pmatrix} = \hat{I} - 2|x\rangle\langle x|, \qquad |x\rangle\langle x| = \begin{pmatrix} 0 & & & & & & 0 \\ & \ddots & & & & & \\ & & 0 & & & & \\ & & & 1 & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ 0 & & & & & & 0 \end{pmatrix}$$

*xx* term

$\Rightarrow$ invert the probability amplitude of a specific basis state $|x\rangle$

- unitary operator $\hat{U}\,|\gamma\rangle = \cdots\cdots + U_{\tau\gamma}\,|\tau\rangle + \cdots\cdots$

initial state target state

$$|U_{\tau\gamma}|^2 \ll 1 \longrightarrow \langle\gamma|\hat{U}^{-1}|\tau\rangle \approx 0$$

(nearly orthogonal but not exactly)

- rotation operator $\hat{Q} = -\hat{I}_\gamma \hat{U}^{-1} \hat{I}_\tau \hat{U}$

$$\hat{Q}\,|\gamma\rangle = -\left(\hat{I} - 2|\gamma\rangle\langle\gamma|\right)\hat{U}^{-1}\left(\hat{I} - 2|\tau\rangle\langle\tau|\right)\hat{U}\,|\gamma\rangle$$

$$=-\big(\hat I-2|\gamma\rangle\underbrace{\langle\gamma|\big)\underbrace{\hat U^{-1}\hat U}_{\hat I}|\gamma\rangle}_{1}+2\big(\hat I-2|\gamma\rangle\underbrace{\langle\gamma|\big)\hat U^{-1}|\tau\rangle}_{U^*_{\tau\gamma}}\underbrace{\langle\tau|\hat U|\gamma\rangle}_{U_{\tau\gamma}}$$

$$=-|\gamma\rangle+2|\gamma\rangle-4|U_{\tau\gamma}|^2|\gamma\rangle+2U_{\tau\gamma}\hat U^{-1}|\tau\rangle$$

$$=\left(1-4|U_{\tau\gamma}|^2\right)|\gamma\rangle+2U_{\tau\gamma}\underbrace{\hat U^{-1}|\tau\rangle}$$

initial state  target state

$$\hat Q\left(\hat U^{-1}|\tau\rangle\right)=-\hat I_\gamma\hat U^{-1}\hat I_\tau\hat U\left(\hat U^{-1}|\tau\rangle\right)$$

$$=-\hat I_\gamma\hat U^{-1}\hat I_\tau|\tau\rangle \longleftarrow \hat I_\tau|\tau\rangle=-|\tau\rangle$$

$$=\left(\hat I-2|\gamma\rangle\langle\gamma|\right)\hat U^{-1}|\tau\rangle$$

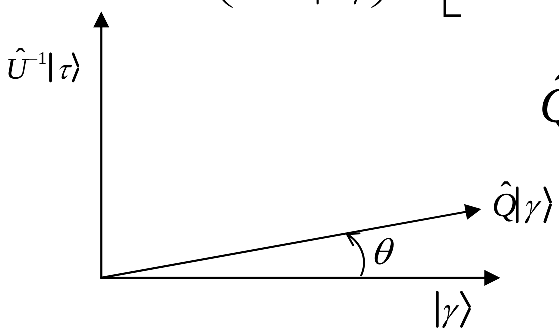
$$=\underbrace{\hat U^{-1}|\tau\rangle}-2U^*_{\tau\gamma}|\gamma\rangle$$

target state  initial state

$$\Downarrow$$

The rotation operator $\hat Q$ preserves the 2-D vector space spanned by $|\gamma\rangle$ and $\hat U^{-1}|\tau\rangle$, which are nearly orthogonal. Any linear superposition of $|\gamma\rangle$ and $\hat U^{-1}|\tau\rangle$ is transformed into another superposition of the same two vectors by $\hat Q$.

$$\hat Q\begin{pmatrix}|\gamma\rangle\\ \hat U^{-1}|\tau\rangle\end{pmatrix}=\begin{bmatrix}1-4|U_{\tau\gamma}|^2 & 2U_{\tau\gamma}\\ -2U^*_{\tau\gamma} & 1\end{bmatrix}\begin{pmatrix}|\gamma\rangle\\ \hat U^{-1}|\tau\rangle\end{pmatrix}$$




$$\hat Q|\gamma\rangle=\left(1-4|U_{\tau\gamma}|^2\right)|\gamma\rangle+\underbrace{2U_{\tau\gamma}}_{\sin\theta}\left(\hat U^{-1}|\tau\rangle\right)$$

$$\Downarrow$$

$\hat Q$ rotates any vector by $\theta\approx 2U_{\tau\gamma}$

The number of sequential applications of $\hat{Q}$ required to transform $|\gamma\rangle$ to $\hat{U}^{-1}|\tau\rangle$ :

initial state    target state

$$N \sim \frac{(\pi/2)}{2|U_{\tau\gamma}|} \sim \frac{\pi}{4}\sqrt{2^n} \sim \sqrt{2^n} \quad \text{(steps)}$$

$|U_{\tau\gamma}| \approx 1/\sqrt{2^n}$ (If a unitary operator $\hat{U}$ spans all the candidate states with equal probability amplitude)

The process should be truncated at an optimum # of rotations, $N \sim \sqrt{2^n}$

## 2.2.2. Implementation by Walsh-Hadamard transform

initial state $|\gamma\rangle = |0\rangle = |0\rangle_1 |0\rangle_2 \cdots |0\rangle_n$

unitary operator $\hat{U} = \hat{H}$ (W-H transform) $\Rightarrow$ $U_{\tau\gamma} = \dfrac{1}{\sqrt{2^n}}$

$$\hat{Q} = -\hat{I}_0 \hat{H} \hat{I}_\tau \hat{H}$$

sequential application of $\hat{Q} \cdots \left(-\hat{I}_0 \hat{H} \hat{I}_\tau \hat{H}\right)\left(-\hat{I}_0 \hat{H} \hat{I}_\tau \hat{H}\right)\left(-\hat{I}_0 \hat{H} \hat{I}_\tau \hat{H}\right)\cdots$

New interpretation

| |
|---|
| repetition of $-\hat{H}\hat{I}_0\hat{H}$ and $\hat{I}_\tau$ after the first W-H gate |

- Inversion about average $-\hat{H}\hat{I}_0\hat{H}$

$$-\hat{H}\hat{I}_0\hat{H}|y\rangle = -\hat{H}\left(\hat{I} - 2|0\rangle\langle 0|\right)\hat{H}|y\rangle$$

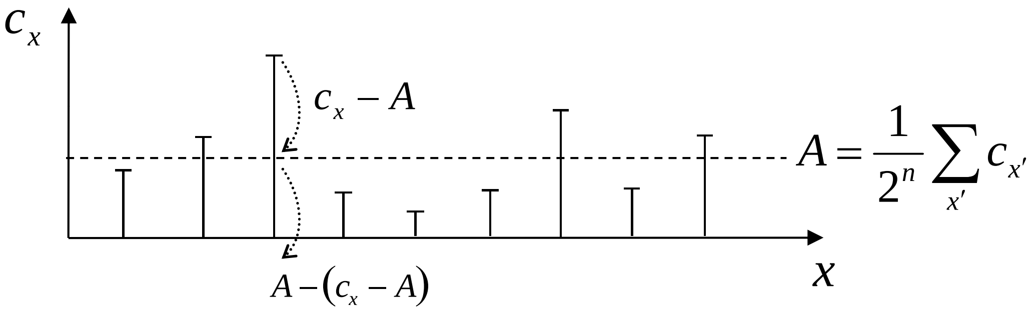
If $|y\rangle = \sum_x c_x |x\rangle$

$$= -|y\rangle + 2\hat{H}|0\rangle\left(\langle 0|\hat{H}|y\rangle\right)$$

$$\hat{H}|0\rangle = \frac{1}{\sqrt{2^n}}\sum_x |x\rangle \qquad \langle 0|\hat{H}|y\rangle = \frac{1}{\sqrt{2^n}}\sum_{x'}\langle x'|y\rangle = \frac{1}{\sqrt{2^n}}\sum_{x'} c_{x'}$$

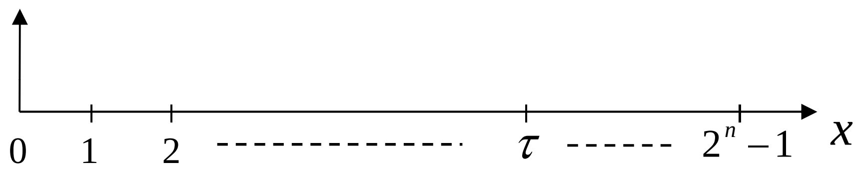
$$= \sum_x \left[ -c_x + 2\underbrace{\left( \frac{1}{2^n} \sum_{x'} c_{x'} \right)}_{\text{A = average of all probability amplitudes}} \right] |x\rangle$$

$$\overbrace{A-(c_x - A)} \Rightarrow \boxed{\text{inversion about average}}$$

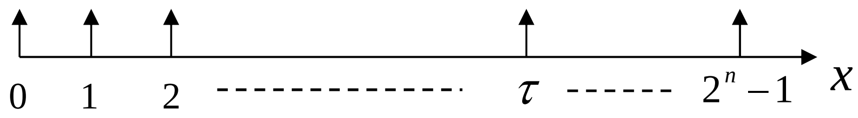



**flow of the Grover algorithm**

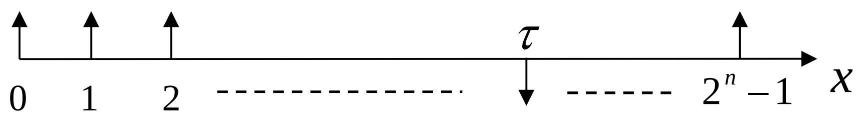
(1) initial state $|\gamma\rangle = |0\rangle$



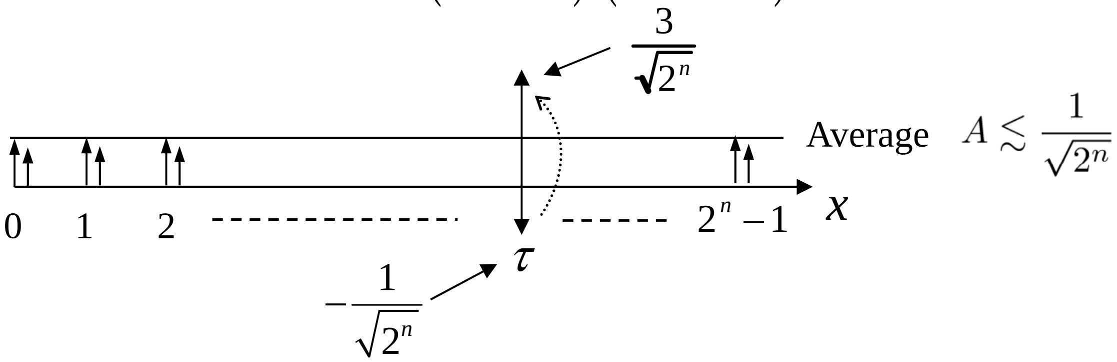

(2) Walsh-Hadamard transform $\hat{H}|0\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle$




(3) inversion of the target $\hat{I}_\tau \hat{H}|0\rangle = \frac{1}{\sqrt{2^n}} \sum_x \left(\hat{I} - 2|\tau\rangle\langle\tau|\right)|x\rangle$

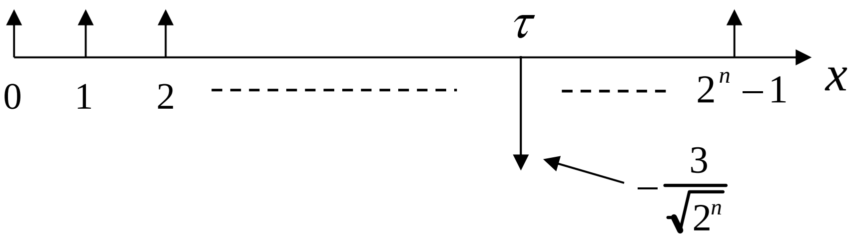


(4) inversion about average $-\left(\hat{H}\hat{I}_0\hat{H}\right)\left(\hat{I}_\tau\hat{H}\,|0\rangle\right)$

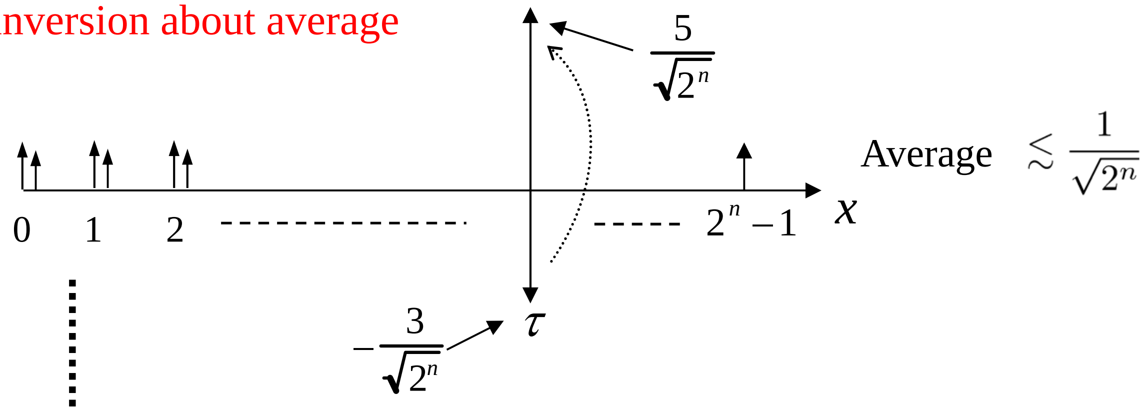



The increase in the probability amplitude of $|\tau\rangle$ is compensated for by the minute decrease of the probability amplitudes of all the other states $|x \neq \tau\rangle$ , since A is slightly smaller than $\frac{1}{\sqrt{2^n}}$ .

(5) inversion of the target




(6) inversion about average




repeat the process $N \sim \sqrt{2^n}$ times

$|\gamma\rangle = |0\rangle \quad \Rightarrow \quad |\tau\rangle$

(initial state) (target state)

- How quickly the probability of finding the solution increases?

| Grover iteration | Probability amplitude | Probability |
|---|---|---|
| 1st | $3/\sqrt{2^n}$ | $9/2^n$ |
| 2nd | $5/\sqrt{2^n}$ | $25/2^n$ |
| 3rd | $7/\sqrt{2^n}$ | $49/2^n$ |
| ⋮ | | |
| k-th | $(2k+1)/\sqrt{2^n}$ | $\sim 4k^2/2^n$ |

In order to achieve the probability close to one, we need $k \sim O\left(\sqrt{2^n}\right)$ Grover iterations.

Example: Four folders $|00\rangle$ $|01\rangle$ $|10\rangle$ $|11\rangle$

$n = 2$ bit Grover problem  target state

$$\hat{H}|00\rangle = \frac{1}{\sqrt{4}}\left[|00\rangle + |01\rangle + \underline{|10\rangle} + |11\rangle\right]$$

$$\xrightarrow{\hat{I}_\tau} \frac{1}{2}\left[|00\rangle + |01\rangle - \underline{|10\rangle} + |11\rangle\right]$$

$$\xrightarrow{-\hat{H}\hat{I}_0\hat{H}} \left(\frac{1}{2}-\frac{1}{2}\right)|00\rangle + \left(\frac{1}{2}-\frac{1}{2}\right)|01\rangle + \left(\frac{1}{2}+\frac{1}{2}\right)\underline{|10\rangle} + \left(\frac{1}{2}-\frac{1}{2}\right)|11\rangle$$

$$= \underline{|01\rangle}$$

$2A - c_x$

target state !

Average

$$A = \left(\frac{1}{2}+\frac{1}{2}-\frac{1}{2}+\frac{1}{2}\right)\Big/4$$

$$= \frac{1}{4}$$